Вариант № 1

1. (a) Расшифровать текст:

ЮЫВСИАЮЫШЬГСЫШЧГЫЗБСОГДЕДАЭСШБМЖЗАЮЫЗШДЮЭГАЮГЩЖЙЪЛГДЪГДЯЪШЙЩБШСЯ
ДЖЫБШЫБЮНЮГДФЗЕИАГЪЖЙЩДЯЕЫЖЗДГЫЩДГЫЕДНЫБГЙЬГСВДЗЕДЖЮШИТВГЫГЮАЭАЮ
ЗГЮВШВЫЗИЫДИЕЖШЮБЗШАДВЫГЪГИЗАДЯЪДВЭЖГЫШДДЧЖЬЗЫЧЫЗШЮЪГЮЫЗЕЙЩНЫШСВ
ЮЗИЖЗТЕЖЫЪЙЩЪИТНЫВДГДАДГНЮИЗНЮИИЫБТБЫЩАДВДЬЫИЗЫЧЫЕЖЫЪЗИШЮИТНИДГЫ
ЧСБЗДШЫЖОЫГГДЛБЪГДАЖДШЫГГНЮГБДЗВЫЖАИТЗАДЩЪЕЖЮОЫБААДВЫГЪГИЗАДВЙЪД
ВЙШЮЗЫБЮМЗЗШДЮВЮЬЫЖИШВЮЗИЖОГДНЫЖГЫБИЫБДЧЫЪГДЯАДВЫГЪГИОЮШЗЫЫПЫШББ
ДЗТЕДЪАЖСБТМДВЙАДИДЖДЩДЪШАЭАЗИДБЮГАЖЙБЫАЭАЕЖЮШЫЪОЮЯВЫГДИЕЖШЮБЗЕЖ
ДВЫГЪДБДЬЮИТЮИДИНЗЬЫШДЖДИЮШОЮЗТШШЫБВЫГШИЙАДВГИЙЩЪЫГАГЙГЫИАГЫЬГДЕ
ЖДПБЗЗВЖТЫЯЮШГДШГДФГЫДЧСАГДШЫГГАЖИЮГВГЫЕЖЫЪЗИШЮБЗТЭЗИДБДВГАЖСИСВ
ЗАИЫЖИТФЮЙЗИГДШБЫГГСВОИДКВЮЮЗИАГВЮЕЙЩНЫШЮНЫБДШЫАЪЫЗИТАЭМАЮЛЗИЖОЮ
ГЗЮЪЫБЮШОЕАЛЮМШЫИГСЛЖЙЧОАЛЖЭЩДЖНЫГГСЫШЮГДВЗАЖЗГСВЮЖДЬВЮЮЧБЮЗИФПЮ
ВЮЩБЭВЮВЫЬЪЙЮВЮГЫЧСБДГЮОШЧЖЮГГЮГОЫЩДЙЖЪГЮАГДШДЧЖГСЛЮЭВЫГГЮАДШШОЫ
ЧБЩДЖДЪЮЫЗАЭБЕЙЩНЫШЙШЮЪВЫГЪДЧЖДЕДЬБДШИТНЫЗИТЮВЫЗИДВЮБДЗИЮЕЖДЗЮВЗ
ДЧЫЗЫЪГЮАЮЕДИЫЗГЮБЮЗТВДБНЗЫБГАЖФЗИДБЗДЗЫЪВДЯВДБДЪДЯАЭАЗИЖДЯГСЯЮА
ЖЗЮШСЯГБЮБВГЫЗИАГЕЖДЗИДЩДШЮГЪДАДИДЖДЩДГЫАДЗГЙБЗЗБФЧДЕСИЗИШДВЗИБЖ
ЗЗВИЖЮШИТЗЧДЖЮПЫЕЙЩНЫШГЕЫЖШДВВЫЗИЫЗЮЪЫБДЧБДАДИЗТГЗИДБЮЕДЪЕЮЖНЫЖГ
ЙФЧДЖДЪЙЗШДЮВОЮЖДАЮВАЙБАДВНЫЖИСБЮМЫЩДЕЖШЮБТГСЫЮЪДШДБТГДЕЖЮИГСЫГЫ
ЮЭРШББЮГЮНЫЩДЗШЮЖЫЕДЩДДГНЗИДДЧЖПБЗАНЫБДШЫАЙБЫИЕИЮЪЫЗИЮГЭСШЫЩДИДЩ
ЖКДВИДИЮВДКЫЮНЫВЮГДЩЪШЫБЮНЫЩДЪЪФОАДФШЗЫДЧЛДЪЮБЮЗТВЫЬЪЙЗДЧДФААИДШ
ЖЮПЮЮГЫДАЭСШБЮГЮААДЩДДЗДЧЫГГДЩДЕЖЫЪЕДНИЫГЮЗШДЫВЙЕЖЫЪШДЪЮИЫБФЖЭЩД
ШДЖОЫБДЧЙИЖЫГГЫВЕЖЮЗИЙЕЫДЧЙЗЕЫЛЫШДЭВЙПЫГЮЮДЧЙЪЙПЮЛЪЫЯЗИШЮАЬЪСЯЛШ
ЗИБЕЖЫЪБЩБЗШДЮВГЫГЮЮЗШДЧДЪГДДЗЕДЖЮШБЕЙЩНЫШЮГЗЫВИДЗИЖГГДВШДЫГГДВЗ
ДШЫИЫЖЫОЫГДЧСБДЮЪИЮАДЖЫГЧЙЖЩЙЪШЮЬЫ

   (b) Расшифровать текст:

КВУНЕЕЭДДАЬЯЩНАКШСРПИЩОРЕЪЫЛНГЯЮХДЮЕЬЩЗАЯВЪЙЪВЩЦДВКРАДХЕЯЦЗИДХАД
ЦЕЪОССЩФМКАКШЦЗДБЫЪЫАДЬОПДДХУНХИЩЧЖХДГЧГЫДХРМЫМЖОГЖПЪДИЫИРЧПФВТЦ
МОАЮЫПЫОЫУРДЬСЧЭФЕЭЧГЭЕЛЦДЫГТФБДЬООМЫОТМНЪГТАСШВЙЦНЦЕЧЩНЯЬРЧКЖШЫ
ТКШДЯДМЧЬЯЧИКЬЭОЖВВТАНВЕЮОПБГАЩЛЭКЪЧБХЬЧЦДЪШАНТШЪЫЫНХЗХВНАШИФБОИ
ЫУНЦЕЭЧРЕКСЧПБЫТЦЗЛЯЭЧЙБЖШОЦЫЖЫУЖЮИЩЦДЮЬЯЪНГЕЧШСЫЪАЪСГТУКНГЕСЪДГ
ТТЪБШЗЧЗШЫЬРФЖАЕЮКДЪДЫРГГЬЦСЙГИЪЧБЕТТШСАДШКТЫДЖОЙИЖЭСГХВХОВБЗОЧЛ
ЖПХЩНЭЕЩЬКЫНАЛЪГЭТЦЗШДТСЖНИЪСЛБЬЫЦАОВПУПДДЫТПЖШВОБЭЯЭМЗЪИЧЧЛИВЯО
ЗХБФЯЙЫМЕЩНХЗВШДГЩИТЙЭКФЦКВЕЮФДФТШКДЦВИТЙВЗШКДЮЕОЧПБЫЫЛБЕЕЭЧИЗДЮ
СИДЕЧЧКБЩЬЩНЪЩЪЦЪЬМШЧОЖПТТРДТШЕМОАЬЩДДЙАШМЫБЯЩЗГЮООЕХПХТЗЪИХКЗГИ
ЧСФГКСЦЗЭЕПЦДДГЫЫПАОАЛРЕЩХЪЙЮХДССШВЙЦНЯЬЪЛНЮДЫЛБЛЯТЧАМЬЮЫББЩЧЧСБ
ЗЫХСЭДТАМАЕЫАТЕЯШЪРЫВЙЦНГЮПФДЭВЫХНШЩЫЧАГЭТЦЗШДЫШТЦОТЛОГЯПОКЯЬЪЛР
ШШЮЛНЫГПЧОГЕЮЧЛЦЕПЧПЫЖЫУЙБГАПДЧЬШЬБОЬВФСОЯФЧПШДОЬПЦИЯЩМАГИЪКПЖЭС
ЧЮГЪОБЦЕШЧБЖГЪООББФФНДУДЫНВЗЫЛЗЧЬЪСДХЙЫЩЗКДЫШПЫЩТНЧШЬЩОМЭЖАМЦШЩА
ШНЧЩШЧЛАЬЮФТКАЬЩЗХЬЮЫЗХЫТТРЕЩЫХНШДЩОПШДХОПШПХФРЫГПЧРВЕШЕЖБЩЯЕРЫД
ТЬРВЬПЧАЧКЩЫЫЕЕЪАСБЗТБКДЕЯЛДКВЪЛНВЗЫЪОЖЪДОБШМШЛАШВЫМНГИЧЬЭЭЗТШНД
ЙЙСЖФЩХЫЫДЯЭЧСЖБЫЫНГКЛЫЛБШХПЭЕЪШРТВКРАДХЮЮЛДГБШСЙЕЕХРЛБЯВФЭЧЬЦЪЛ
ШЬЯЧАЫЭЯЕРЫЗЫЫТЪБЭСЦЮЕЪКТЧУЫЦРШГХШГШДЙЛНЮШАЧСДКСХНШЪЫЦДЖАСОСЦЕПЧ
ПЫБЯЧБЫДЫЛСОАЕЛАГЯЪЛЗАЕПЫЪЬЕЯЛДКВЫЦГШЗУССХДТЛНЮЬЯЬГШЩАБЙЖБЫЫНГКЛ
ЫЪХЯСОКФЕШЕМЖХАШНВЫЙСЗАИХФЫАЕВЧЦШЙЪЦДЬЭТЦЗЕУЮШПБКДЬЧХШЭСМДБФФВГЕ
ФЦНВКРАДХЕЪЬЖАЬЯУЙБЩЫЬЛШДЮЛНШЩЫФЫАЯДЫЫЫЕОСЕЕУЪЩНЧЬРЧОБЩТБТВЗХУЕЫ
ИШЧББГЫФБЫЙЙЪЙЪВВФНВКЕЮПЫЖШДЛЦЕШЧРБГЯДОБЙЫЩНВЯШЪМЪДДССППКПЫДПУН
ЯЬЪНМЕТЧЩДВЕЮЫЗЕЬЬОППЙЫЩНВЯЕЕРШЪЫЛДЛЙЙЫЪЖЭЫЪЙБЗОСКЭЮЧЧБВЕЮНЗХЫПЧ
ПАЯЪСЛ

2. Разложить на множители числа:

   (a) 6662783593895175682165340803 93

   (b) 1008704736637390313513101213337497368610966677496731131686771

   (c) 935191495292858362821108067845913270550002172350761814478365379232516074389106599458627833

(d) 9181869474985362860961835272885035229309539657093454940780949898494971656023844495905202965836707615222602276676517133 57

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 62011515049184334277144610292579040479635598858868758863842668941853864114413$
   - $e = 17$

   Сообщение:
   - $M = 55869249276148827988608707689994744573458819461704520442658192737713872180450$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 256608788278901622777356475339874336147$
   - $q = 207856243496143268551835115811497238973$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 401095715469801549624292957603870190485200551356401770679785772540162779564 72$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 193009890725567512496772259368517402511$
   - $e = 257$

   Зашифрованное сообщение:
   - $c = 173737910506961103160913910241345109968$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 254380658677840944308688622395700470307$
   - $g = 199704271113298013525038679970532808660$
   - $y = 241813396370640738346288051881905349591$

   Секретный ключ:
   - $x = 940699280816320641825348369872715993 56$

   Сообщение:
   - $M = 34905761941212060795999331441805244306$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 92921857703279757757452374703376717061$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 319115782782081661967426100089598886589$
   - $g = 525635779347936491635007005585685 4054$
   - $y = 824219800823928082895703323770027095 56$

   Сообщение:
   - $M = 14844232729755674997567634402563428 1941$

   Подпись:
   - $a = 503101176685562220717138487032150262 55$
   - $b = 444890568899601432149568619827931538 82$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 877$
   - $g = 710$

- $y = 38$

Сообщение:

- $M = 569$

Использовать следующий случайный параметр для создания подписи:

- $k = 23$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 6x - 8$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 2

1. (a) Расшифровать текст:

ИЙЖЧЬОСЙЖМССЯНУФЙИРЙЦЙЗТСЙСЖМХЦМТСРТЗФЙЬМЦАХСЖХЙЫЦТРСЙЕЯПТИЙПЦАО
ОУТИЦАЙНУТРТЭАООТХЖТЕТИМЦАМЛФЧОЛПТИЙТХЦЖПТХАТИСТХФЙИХЦЖТФЙЬМПХЦТ
ЦКЙЫХТЦУФЖМЦАХЖТФЙСЕЧФЗИЕЯЦТФТУМЦАТХЖТЕТКИЙСМЙЕЙПТЗТФХОТНОФЙУТХЦ
ММУТЖТЛРТКСТХЦМЦТРЧХТИЙНХЦЖТЖЦАУФТХЦМПХХХЖЭЙССМОТРМХОЧПМСТНУРШМП
ТЖСТНХКФТРУТФЧЫЙНЦЧОТЦТФЧВУТЫМЦПЧКЙХЖТЙВКЙСТВЖЛПФЧОЧЕЙИСТНИЙЖЧЬО
ММУТЪПТЖПЙЙТФТЬХПЙЛРМУФТЭНЦЙЗТЖТФМПРСЙУТУИАУФТЖТКРЙСУФТЭНЦЙУЙЦФС
ИФЙМЫЖТХАЧЖМИМРХЖПЧЫЬЙЙЖФЙРСЙЛЕЯЖНЦЙСХМУМЬМЦЙОСРУТЫЭЙЕЙИСРФАМЖСТ
ЖСОФТРЙЖХСЙМРЙЙЦЦЙУЙФАСМЧЦЙЬЙСМСМУТОФТЖМЦЙПЖЯЬЙИСУПТЭИАТХЦСТЖМПХ
СРМСЧЦЧЖЛЗПСЧПСЖМХЙПМЪЧУТОПТСМПХЙНЖЯЬЙПМЛОФЙУТХЦММУТЬЙПУТТФЙСЕЧФ
ЗХОТНИТФТЗЙХТУФТЖТКИЙРЯНХЖЙПАМЫЙРОТЦТФЯНТЦРЙССЙТЦХЦЖПЬЙПЛСЦЯНХЖТ
МРМФЛРЯЬПЙСМРМООЖИФЧЗЧХПЯЬПЛХТЕТВОТСХОМНЦТУТЦТЗПСЧПХЖМКЧМЛОФЙУТХ
ЦМХОЫЙЦОЛОИЙФКЕЬОМФХОЧВПТЬИАЖУТЖТИАМИЙПМЛИПМРСЙЛСОМТХЦСТЖМПХМЖХО
ТФЙЧЛСПСЬЙЗТЧФИСМОТСУТИХООЖХПЙЛХХЖТЙНПТЬИММХОЛПТЦИЖРСЙУТЖТИАИФЧЗ
ТНЖЬЙЕПЗТФТИМЙТЦЙЪСЬЖРКПЧЙЦПТЬИАМЬЧЕЧХХЖТЙЗТУПЙЫОХЙИПЧУФМЖЛСЕЯПТ
ЖЫМССЯНЦЧПЧУИЙЭЙУФМРТПЖМПЛУМСХАЧФИСМОКПЧЙЦТСЖРУТПЦМСЧИЙСЙЗИФХЦЙФ
ПЙЙИТФТЗТВУФТХЦМЦЙЖЙПМОТИЧЬСТХЖЙПАМЫУТХРТЦФЙПССЙЗТОТХТМУФТЖТФЫПФ
ХЦЙФПИТФТЗТВЫЦТКЙЧЦЙЕУТЕФОМЖЙЦЛУЛЧЩТНЕЙХХТЖЙХЦСЯНЫЦТЧРЙСЛУЛЧЩТНЦ
ТУТЕФОМЖЙЦЖТЛФЛМПЧФИСМОСМРПТСЙХРЧЦХАЕТЗХЦТЕТВХЦФМСЧЬОБЦТЕФЙСЫМЦЧ
ЛИЙЫОСЙУТПЦМСИТЕФТХОЛПУФЙФЯЖХУТФЕПЗТИФМТЦРЙСЦТЗТОЦТЦЙЕУФМХППФХЦЙ
ФССЧВУТПЦМСЧУТХЦФНХУТИТЕФЦАСЖТЛЖФЦСТРУЧЦММЖТЛАРМХЙЕЙСЖТИОЧТЫЙСАЕ
ПЗТИФЙСЖЬЙЕПЗТФТИМЙТЦЖЙЫПТСУТЖТФЫМЖХЖТВПТЬИАЖЙЫСТЛЖХЕЧИЧЕТЗРТПМЦ
АУФМХМЩХПТЖЩТСУТХООПСЛИИЙФКХАТИСТНФЧОТВЛ

(b) Расшифровать текст:

ФЭКМЭЩЭЖШЖСААЮГРЙЕДЗХДОЛГЛЖЬЙГУАЭАЕЪЫМЛЕХЙГЗЪКЖИБГНАЯЙВХЙЕВЭИИНБ
ЛСВОЪЩМЪОФЯЪЬАМЫПРЧОРЪЙАЭДХЬЕМИТЖЗЛГСЮГЖБФЭАБНЙЩЛДВЦЖЬЗЪЛЕАЗЯСДА
МЗЙУДЯГШЛЯМСШВВЗГФЬЛКЫААЗЯГТЖМКБКЖМПЩЧФЙЙВМЗЙАЯЧЛЖКБХЕЬКАГЕЙЙЧШЪ
АОАПОАЗЪНАНЮЪЛАБИЪФВИБЮШВВЗЖУЖВЮВМОЭНЗЙЙЗБЖЩЖНЯГЙЖЛДЗГЙЬЧАХЕАЮГО
ДЙВВХРЭЭЕПЕККЧМГКПШЮЭЭЮЖЙЭНЗЭЭЛЗМСПАЭЙГЙЕЦГВПДГЛГШГААГЙГУЮЦЧАИКЖ
ЩЕЙЮЭТЙИЗЪШКИДЛМЫЙНИЛИЧНЯОГЙЙЧВЪЖНЗФУНМЪИЖЭОСХКЗБВЮКЙЮБЪЫЙАВХЕЙЙ
ЪЦИГЖЫПКАЛГШКЙМГФЕАИИЙНЙАЭЩФЭНДТФИЪЯНЭИББХЭДГЗЧЭКБЗТКЕОРНЭИОЖСЯЖ
ФЧИИГЙИКЖНКЧШЭЮКЕШКАМЬЩФНДНМЗЛБЕЙГЗБВЦЛЮУЪЙХНКБХЭЯБАХКЦЛЕХЬЙЗЫТЖ
ИКЦЧСМШЯЯЪЬМЭФЛИБИУЕГУЮПЕАЗГУБМВЪФГГКВЩЭЬБЭТАИБЫМЕЭБЩЪВИБЮСЖЮКХХ
ПОЮНМЩЖЯГЧЖЯДЪШКОЛЮОДИКУЪЬЭБЕМБМЮЪЩГГТРЯЪЬМЭФЖКОСХЙНЙГЙАЖНЭШВВЗД
ЧЭЛЧЧЕСГИЖКЖЖКЖХДЮКЖЪЬЛШДЧЭЯПДЧЭБАУЙЙТОГХЕЭЭЪТЖДЯГЧПЕБЭЩИАОЭРЬАЙ
ССВЬМЪЛАНЭЪОЛЗКАСЛЙОЧХИДНЯОГКПШЮЭЭФЧИИГЙЖЩГГНЯЩФОНЪИЪЕМБФНГНЯОГТ
ОГФЭЭГАШЙЙЭГЕВЖЪМЦЛЮУЪЙКЙЗЯФЛЖАЧМИЧЙГКЖЩГБХВЙОЖСЖТДАЛЪАМСХКЭКЕПГ
МШЭУУЭКНТАЭГШТЕОЗЭХЩЗБЕФЗЙЗИЙВЛБЖЩФИНЯХДЙЭГЧЬИЙГУЗЖОСМЙГАЪТДЛШЭЙ
ЕЙЮВИГААВЬЛЯНЕШКЛБДФЕЦИЭЙЖЖКЖУАКБЕМЬИБУШКЙЗЯЪЪУДВЙЖЯЧВСИЦОРРГЙИЗ
МДРЗЪИЛЭДЩУЭИКВЙЯЯМГКЕОЗЭОВЛДМТПНКЗХЫЯНГУЕЙЪЖЩГЙЙЪЦЖЗЙУЦЛЮУЪЙЗЙН
БХКЛБАФРЭЭЕПЕГНЯОГМЯГЧФЕКЮЪЙЗБНСЖЩСГЧЖУПЗМЩЖГЕМККЗХДКЩХРААЯУИЧ
БЭЙЕЙЮВМЙЕВЭУЕАЯГТЛЬПНСЯТОГЩЪЙЕБЪЮНБЦФВВЧЧМКЭУЪУКЦЛЪЧЭЯЙЭУЗЛКЧПЕ
ГЗЖГДЙЕБЪЮККЧЩЖЛДАХЕЙЙБФЭИББЪЮИДЯХЫЯЙЪИЛЯПЪКЖББВХЦЖПМЯЭЛБНПГМШИУ
ЭЛБЗГАОИЕЪЭМЗЭУЭИЙЪПЯЬЮЗЦЛЮУЪЙЪВЯАФЛЖЯЕХЯИКВЯЪЬМЭФАНЧЖУЭЖИЪФЖЬИВ
ВЪНШЖСЯЖКВМДОГВМРЧЗЭИЭВАЪТФИДЯЮЭЮКЗВЬЙНЗХАИФЧИ

2. Разложить на множители числа:

   (a) 787803454312198143822775410049

   (b) 838899588561881494762696712545842498777597683987376514308103

   (c) 13878816037893399189592713370164996474680447705102819833307225567617380926780883419037064 61

   (d) 1753274917039859695593420540556752578781236615635354016395186362554906543582299940333231074092779431586138927491296928963

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 68321081591648933540462223271129424239824811960821445524046350279115927777001$
   - $e = 5$

   Сообщение:

   - $M = 500338701838929820079984160567043055013090966558183897006550085775607919981111$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 18090646077057127780967556509277750 4729$
   - $q = 24818653949168217531977724697986074 0977$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 39240306321690203221482124167810823875268317569312508947530799776493601201481$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 16861563249694763086138026679073937 8879$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 81166097573538263570294736411300479735$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 308043102353544234025222029522223241327$
   - $g = 31486957201595751634236625249055515799$
   - $y = 69649427066080622831575870842207179508$

   Секретный ключ:

   - $x = 70604397557025105623955735288378489991$

   Сообщение:

   - $M = 14024448302065761121882064109553007956 2$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 26765280263659449614418908383114336135 9$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 18866158236848957622820497509891726 8433$
   - $g = 94091197596313509833895464868331603224$
   - $y = 67395361756679726540831848310759272445$

   Сообщение:

   - $M = 37401447340098965086775527208746273562$

   Подпись:

   - $a = 10364571417022011362585154819624534348 0$
   - $b = 91838672011593720192866199899232649882$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 971$
- $g = 43$
- $y = 19$

Сообщение:

- $M = 937$

Использовать следующий случайный параметр для создания подписи:

- $k = 277$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 6x - 17$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 3

1. (a) Расшифровать текст:

ЧЩСЛБОШЩОЛЧЪЮЧНСЫОФЕЪЫЛЧШЩСУПСЫОЛРЫЕХЦОЩЧЫЬЪЧФНЫСШЧФЪЧЫЦСУРУЧЛСШ
ЬЪЫСЫОХОЦЧАСЪЫСЫЕКОФЧМЧЩЪУЬЗУЩОШЧЪЫЕМОЦОЩФМФНОФЦХОЦШЩСЪЫФЕЦЧШЧФМ
ЛОЩЧЫЦЧАЫЧЪЬХЪЧБОФЛАОХШЧАЫССЦОЧБСКФЪУУЖЫЧЧАСЪЫСЫЕКОФЧМЧЩЪУЬЗУЩОШ
ЧЪЫЕЪУРФЧЦЦУЧЦОЯЩЬАЗЪЕЛХРЬЪШОЮЧЫЛОАФЪПЩЧХЫЧФЕУЧЧЫШЬЪЫСЫОХОЦЦОЫХЧ
ФЧНЧТАОФЧЛОУЪУРФЧЦУАМЧФЧЛЧЗЦЫУЧХЛОФСУЧХЩЪЪЫЧЦССЦОШЩСЫОФЗФОМУЧКЬН
ОЫЧЫЩОРЫЕЛЪЧЫУЧХЬЦСУЯССЪМФЛЦДХЪЫЩЫОМСАОЪУСХШЬЦУЫЧХСШЧФЬАСЫЕЦНЛХС
ЪЧЛОЩБОЦЦЬЗШЧКОНЬШЩОЪОАОЦЦУЧХЬЦСУЯССЪШЬМФЪЬЛСНОМЧРЛФОАОЦЦЧМЧЛЛЧО
ЦЦДОЩЪЪЬПНОЦССЪШОБСФОМЧШЩОЩЛЫЕНЧАЕУШСЫЦХСЩЧЦЧЛЪУРФОХЬШСБОЫУЧХЦОШ
СЪЕХЧЧЦШЩЧЪСЫШЧХЧВСБЛКЩСЦШЩСЦЬПНОЫООЛДНЫСРЦОМЧРХЬПЦОЬПЫЧЧЖЫЧЫБЛК
ЩСЦШЩОЛОФСУСТСОЪФСШЧШНОЫЪУЧХЦОЛЩЬУСЫЧЛОФЗОМЧЪЬНСЫЕЛАЪСХДЩЪЪЫЩОФО
ХОМЧЦШЩШОЫОУЩОШЧЪЫСЦЧШЧУХОЪЫЕЦНЧКЦЧЛРЫЕЫОЩШОЦСОЛРЫЕЫОЩШОЦСОЛЪУЩС
АФЛЦОЪОКЧЦХОПНЬЫОХПОЦСЫЪЦХЩЕОСЛЦЧЛЦОЧЛЧРЩРСФМОЦОЩФЖЫЧОВОЦОКОНФЬА
БООТКДЫЕШЧУХОЪЫЕПОЦЧЗБЛКЩСЦЧЦЫОШОЩЕХЧПОЫЧУРЫЕОТШЩЧЫОУЯСЗУЧМНОМЧЩ
ЪЪЫЩОФОХЫЧМНКЧМНЪЫЪДВЬЫЪОТСПОЦСБУСХСФОЦЕУСОЛНЧЛЬБУСЛНОЛУЮЦОЪСНЫЫ
ЧОЪЫЕЮЧЫОФЪУРЫЕАЫЧЛНЧЛЬБУЪУЧЩООЦТНОЫЪОКОХЬПЦОПОФСНОЛСЯЪУЧЩООЪЧМФ
ББЪЕЬХОЩОЫЕЪУРФЛКОБОЦЪЫЛОЦОПОФСЬЪЫЬШСЫЕООБЛКЩСЦЬКККЪУРФЪЫЩСУЫОШ
ОЩЕШЧЦСХЗЫДЛСНЦЧЛХЩЕЗСЛЦЧЛЦЬЛФЗКФОЦЧНОФЧНЩЬМЧОКОНЦДТХФДТЦЧЛЪОПОЦ
СУУЦОХЧМЬНЫЕЫОКОЩЧЫЬЪЧФНЫСШЧФЪЧЫЦСУРУЧЛЖЫЖУЪШОНСЯСКДФКДЦОКФМЧЩРЬ
ХЦЦОХЧМЬЛРЫЕООЦЪЛЧЗЧЫЛОЫЪЫЛОЦЦЧЪЫЕШЧЫЬШСФМЧФЧЛЬЧЫАЦСОХЦЧЗЧЛФНОФЧ
ЛНЩЬМХДЪФЕХОФЕУЦЬФЛМЧФЧЛОХЧОТЛАОХЧЦЪЧЬЫЧФАСЫЫОФЕЬЛСНСЫСРЪФОНЬЗВО
ТМФЛДУУМЧЛЧЩЫЪЫЩСЦЦДОЩЧХЦСЪЫДМФЛХЫОПЦЪФЧКЧН

(b) Расшифровать текст:

ЧЭЯУПАЫУУРЧТЮГНЪЬЧРЗЪХНЧУКАВЪУЩЮИУУНЭЮТКЮЮАУЭЧЧЗКСЫХСЬКЩВЭКЦОВЦК
ТСВМЦЬОБВТАТЮДНЫОАЭКМЮЮЗШЧОСЮЖСЦЛТЧБШЮТКХЕЦХЧАХЭХЬЧЧЦХТНЫМСЖРПМЭ
ШПЬФВКЖОТЮМНЫМБЦЛОЭЮГЙЦЭМЬНЫМБЦХОСВНЭУЬШВОШЫОТБШЮБРШБЩБСКЦАЧЗЛСБ
МЧАЪЪЯНЧЦБЪУГНЮЗПУТФЮХУМТБНСКШАЦПХЭЮГУАШЙКТССХМУШБЭУЧШАТБКОЧТЧХП
ЮФТШУАЮЙНЫХЫСЧЛЮШСЦХЮБЧЗТБГСКЦТЮЧХНХТУХОЭСШХМТЮМЗЩЙВБЦЫХСКТОЧЗКС
ШЮЯЙКБМБУФЫМТХШУШСШТЫЮТЮНУЬВПЗЩФЫНУЫЭШЪКВХАМУЫФХРКБМБЧПСЬЮЖХРЮЬР
ГКЮТТЙЬАМФХЧЩФКЧЬЬБУЖЧОШЗЦОСГЙКЫЫФТУЮЮВТКЪЮТЦКХСЛРЦЦШЬЦУМЫБКТЧФЭ
ПУПЗГЗЦЫТЮЗРАВЮЙУФУЗКЦЫШВХККЮТРСЧХУУФЩШБШЧЪВТНЗЛЮЩЦПОШЬФКЩВАНЫДА
ХЭНФБЯУЦФХФУЗЫМБУЗОВГМШЩШЭУЧШАТНЧЕЬАБГСТЭУЗЦГТЙКЩХТТГСЮБЧЧЕБТКИЧ
ЮВХЙОБТКРЕШЗЗНФБЬКТЩЧФКЗЫМЮЖЯЛШЫКСЬЗВУЖЦФАШИЧЩЦКЙОЭМИУЫЮТУТКЛЫКЪ
ЫМТЙУЩЮУШЦХАМКОСТЭУЗЦЮЩУТКЛЫУМЬЯАСНФБЗЧУЫЛБШЙЩМЪПЛОВХЖЧЧЯЮПНЦГЪЧ
УРВЮЖУЗСГЙКЫЕЮЙНЫМЗЧУЪЪЦШЧЩЮФНЧОЫШЧЗЧШЧТШШАЬЦЧЛЮФЙБУШЬУКМЮТУМЦЬХ
ХНФБГЖКНШВБКМЮЫЦПЧЩШНЦУАХТТЧБВНГНАГИЧДЬЮОХЮШЯЦЗОЫМНЬЪЪЧРКХГЭКУЫЪ

ЦНЖЬФМСТОСЫИУНХВКРОЬТФХСБЫШИОЧФКЦЕЭГЛЙЫМБТКЪВЭШТОСГЙШЪЯЮПУОЭХЦРС
ЬАБНЛЭЮЗТШЮХЙКЫТФУХЧУГЖКРВХЖЦФГЦКОЪЫГЛНБМВАНХЭХФУЫЮЬШЬЫЮВЗКЩФЮХК
БШЫЦПУБЪУХЧЮСЦЧЧВХРБЪВТЙУРТЮРЧПХЭНЧЕБЭТКТВГЧЦЛХЫБНАБЯРКЪЭГРХЬЪЬН
ЦЛШФУССЧГСРОЭШТКЧЯШЦТЦЮУУЛОЭШЧБЪЯЮЗЧЧАШРУЦФШЧЪЧЗХЧЛОЭШЧБЪЗВУЦУЦХ
ЧЖЫОИПСЫГИПЧЧЗВУФЧФГСКЫБЮИРЪВБЗКЩЭЮЦУМЫБЧЦЧВТКЬФЪЮИЙЬЧЭГЧХАМГНЛЭ
ЮЗТЬЭФКГЪМШТЧОССЧГБЪШСЧЬИЪЧКККХТКХЫВЛЖШНХИБМЦБЕУЙЫХЬТКЫЪЫНЦЫАШПЖД
ЫВХУЦГВУЪКВОЭПЫЛЬУОШХВХТНАХНЬЧВТКЬФЮЭЪУЫМАТКЦМЪУМНГЬРЧДЦХТНЫМБЙМ
ЫЮЬХБСТЭУЗЦВЪЙУКАСХАБЭЗЧУМАХЪНШАЮФШЪВШЧБЧЪЧНГСЭСАЧЕЯЮЧЗЧХЬШФЩЮТУ
ЛЬХХТИОЫСУЛСШ

2. Разложить на множители числа:

   (a) 631597197454139065771069579181

   (b) 10369441189628431081133662597730393006444591407178842925719l9

   (c) 1427121166149581627155848894675630303903429062955783722636313154610958020452160589121208449

   (d) 139805554995867923338658516185674065656094700642926979634904355372316077743456548949982970481252911780613493022071061759З

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 830575908671136009334674914801756788187858330380536646504935650457052956012З$
   - $e = 5$

   Сообщение:

   - $M = 795162119481803185982716370583690469500367128705770179877919509652592491743З1$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 225720229217088297177632977108520054873$
   - $q = 223014092972897066591395825561140991547$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 49774204250892810303377921484073221581040547631027785493741512487081317726335$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 140592770345767533226248547467783436633$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 166189781294502306019520842787453686З2$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 193802051283561841030323946584405483817$
   - $g = 128792594949333221568552810419402223593$
   - $y = 173677124240987501218126879456764578416$

   Секретный ключ:

   - $x = 134959090134329391803494046283057282886$

   Сообщение:

   - $M = 110235606519763344366215152335418228899$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 54174179935940001910217249381564163191$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 19933083040560903842561600111365597390 9$
- $g = 64151776702752749521610164124236163588$
- $y = 15763107216824647926139188269378641011 2$

Сообщение:

- $M = 19552848996521950649881889754901618038 9$

Подпись:

- $a = 15750077692436493331784616932176369206 1$
- $b = 71495712434832399029685097300142695 36$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 577$
- $g = 444$
- $y = 377$

Сообщение:

- $M = 219$

Использовать следующий случайный параметр для создания подписи:

- $k = 107$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 17x - 6$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 4

1. (a) Расшифровать текст:

ЖЦТФМЫСТТЫЧЦМПХЛТИСТВЦФУЙЛТВХУЧЗЫЙЖЯРМХЙЗТХЦФЬСЯРМЦТЖФМЭРМТФЗМОТ
ЙНЕЯПСЙЖТПАСЯРХЖМИЙЦЙПЙРУФТИТПКПХАИТЗПЧЕТОТНСТЫМСОТСЙЪЩРЙПАСЫПТИ
ТПЙЖЦАХТЕЙХЙИСМОТЖУЧЗЫЙЖЛИФЙРПХМИСХЖТЙРРЙХЦЙЦТЖФМЭМЙЗТЖХЦПММИПМР
СЙЛСОТХЦЖМЦАЙЗТЖЯЬЙПЖРЙХЦЙХСМРМУТФХУТФКЙСМВЩПТУЧЬМОФЧПАСЯНТЦЖЙПР
ЙСЖУФМОЛСЧВМЛЕЧЗИЙСЬЙПМХЖЙПАМЫМЗИЙРЙСТХЦЖМПМХСМРЖЛУЙФЦМИИАОЕЯПЖЦ
ОТРМЛЧРПЙСММУФМЖМИЙЖХЙЗТЫЦТУФТМХЩТИМПТЫЦТСЙХИЙППРСЙСМООТЗТЖТУФТХ
ТСЧПЙЗХЖЦЙРСТЦЙМИТПЗТЖЛИЯЩПМТЩПСОТСЙЪЛЩФУЙПУФЙИПХФЛРЯЬПЙСМРОТЦТФ
ЯЙЖТЖХВСТЫАСМСТИСЧРМСЧЦЧСЙИПМРСЙЛИФЙРЦАУТЧЦФЧУФМЬПМРЙСЛЖЦАТЦМРЙС
МУЧЗЫЙЖУТЬЙПОСЙРЧЧЖТФТЦЙЗТХЦТПОМЕМЦОЛУФКЙССЦФТНОТВЦЦФХОМЩПТЬИЙНС
ФТИЦТПУМПХСЧПМЪЙЖХЙСЩЖХЦФЙЦМПУЧЗЫЙЖТСЕЯПТИЙЦУТИТФТКСТРЧЖЬЧЕЙМЖОМ
ФЗМЛХОТНЬУОЙЖЫЙФЬСМЙХТЕЙХЙИСМОМТОФЧКПМЙЗТУФМСЖСХЙЕЖМИУТИТЕТХЦФХЦ
МОТЦТФЯНХМПАСТУФТЦМЖЧФЙЫМПЖХЙРЧЫЙРЧЕЯПХЖМИЙЦЙПЙРСОСЧСЙУЧЗЫЙЖЖЙХЙ
ПТХТРСТВУТЛИТФТЖПХМЖЙПЙПРСЙХИМЦАХХСМРЖОМЕМЦОЧРЯЧХЙПМХАЖЕЙПТЗТФХО
ЧВОФЙУТХЦАХОЛПУЧЗЫЙЖЬМФТОТУПЙЫЙРЧЦЦФМСЧХЦТУФЖЭЙРЧЦФТНОТВХЙФИЪЙРТ
ЙХМПАСТЛЕМПТХАПТЬИМЦФТСЧПМХАОТПТОТПАЫМОЛЗФЙРЙПОМЕМЦОУТПЙЦЙПХЦТНХ
ЦТНФЛИПХЗТПТХХПМЬОТРРСЙЛСОТРЯНМЧЖМИЙПХЖЙПАМЫЕЙКЖЬЙЗТСРСЖХЦФЙЫЧУЧ
ЗЫЙЖЖЙПЙПТХЦСТЖМЦАХЕЦВЬОУЙЦФСИФЙМЫОФМЫПИИАОСЙУТОМСАРЙССХЦФТХЦМПЙ
ЦУТХФЙИМБЦМЩРТЬЙСХЦФЯНЩФЯЫХОЛПЙРЧУЧЗЫЙЖТУЦАЕТЗИПХЖМИЙЦАХСЧХИМХАС
ТЕПЧЫТОХУХМЕТЗТХЧИФАХУХМЕТТЦЙЪФТИСТНЗТЖТФМПХЖЙПАМЫЧХКМЖХАИНЕТЗЦЙ
ЕЙХЦТПЙЦЛИФЖХЦЖТЖЦАЛЦТЫЦТРЙСХЦФМОУФМЛФМПМЧХУТОТМПЖЙОЛЦЙЕЕЧИЧЕТЗР
ТПМЦАТЛНЫАЙРЦЧПЧУЙМЧУТРМСЦАЧКСЙХЦСЧБЦТЦЛНЫМНЦЧПЧУРТЗСОТСЙЪСЙСЬЧЦ
ОЧФХХЙФИМЦАУЧЗЫЙЖОХЫХЦМВХРТЛЖСЙЪМПМСЙФХХПЯЩПМПМУФЙСЙЕФЙЗСЙЧРЙХЦС
ЯР

(b) Расшифровать текст:

ЙЭВИШЛЬОЪЦЖТКБФЛВЙШГВЯЫЫЪИЩМБПЕУОХЩАЗВВУЖАВГРЬЩИЯРЕЩРДХЖБЕЮЬЪЯЕЛ
ОАЭВАЩЗГЩБЭЪЦИЫНКПНПЧЛЩОЕРНАЛГЮЮЦЗЧЩЗБЛДЮЕЦПГРЩЯЯЮУЕЦЮОЦЙУЕЧРКЦИ
ШЧЪВВЯЮЖИВЯЩЙГВЕЬДЮВЖНЭХЛЯУКНФЫЭКЦИАЩКЫФДЭЖВИОАГЯПБЧИВОЭТУИПБЧГЦ
ЖЛУЭАЛЧЫЖТКББЬКЩЯГРЯЬЕДЗЪЭЛСЪДГЩЫВКЯЙАРВЧВЕЬЩДБЕЩЩМПЖЭЮЦКШНАХЕЯЩЗ
БЕДЮКВПХЩЪЬЙГЗАУКБНЕАНЫШКТШЮЧЖЩЙЫЫЖХЕЕРГЭЕДЭЭЭЕДХИЦКАУДББЖГАЦЙЭЩ
КЯНБРЖГИЫВГЯИСПЭЪОЕЫЖФЛХРВЯКЫНАХВЮУЩЬАБПКНЮБСАПЯЕЩДИПБУДЦИЫЬГДФЬ
ЪИЩЫЕУКНЕБМГВЗЕЗЩЦБАЮЦВЕГЩКДЯДХЖБВБШАЫКШФАВЗГРЕЮЛВЫАУДЮУЙНМБЭЖЭР
КЭЖЮВЮЗЯТШЮЩЭЦРЪШКНЕАРЗЯИСМАГЩЯЩГПЮБНФДГШШЭЫДЮЬФТПСГВЦМЖЬКЯЫФЦЮН
ЫЯЭЛЙЗЕЩГНЗБЭЖФЛЫСЭЬИКЭЖТВШЪЭГНЖГЮЦКЫЦЙЮЙЫЦЖЪЗВУКЮОЭЩБХЛКХЭВИЖАЖ
ЭЛШЧИЦОЕРЗЯНЪУГУОШЧЖЦОШЧЭЪОЕНЖЭНПУЪЮЛХШКЫМГЩЙГЛГЬЙЫДЮЧЖЩЙГЩЬЩПШЦ
ДЯОЕЫЕЮЛЯТЕЫЛЯЬКУВЯЩЭЭОВЮЫИВХЖДИПБЩЕЯКШЭЖЬЩЭЩЕЦЮШЬЗЯЗБУГЯЕИШЖЦЦШ
ТЙГЯЮЦЖИОЕЩЙЭВЕЗЙЯПКУЙГЛЦЩЙЦНЧБЩГЫЛХЕЦТБЭЭЬЯШЫАГЩКЭЖТШЯЩЫТШЕЗЯЭВ
ЛШЪФКЖЬЕЯЙФЮЕГВЭЩЭФЛЙРГНЮОЦЕЩОВЫЖУВГСЭЮЕШЪИЦОЕЩГЩЕДЭИЦЮЮРЕЩВЧНЖБ
КДХЖФЛГЩЬЯКДЭИЯАБПЖАНБЬАЬОХРГНЕКПЬНЗАРЛГЕЮВКЯЮГУЕТШХЦЪФЛДЭНДВЯРГ
НЗЫЪЛФФШНАИПБПЭШИБПЭЪВЦЩКЫЕЩЦЖУИАЩВЬИДВКЯКЫЩВЫЛЬУЯЭВАРЖЮЕАРЙЬШИУ
ЪЬОЕЫАЫЕЖЬЗЯЗБУГЩОПУЙЮВЕРИАВАУЭЭОЕЦАЧБЕЗЩЬАБЪИЩПАЖНУВДЭЭЪЙГЗАУКБ
НЕВЕЮЗЕЯЮОЦЪВПГРЪЯГШШЕЯЙБЦПЬЕФЩЪУШДГЭЪОЕРЗЦКЫМУЬЛЧЫЭЮОЭЫЖЭКБЬКЩЫ
ЫЩЙГЛГЩЮЮЛДЭАПМГЩРЬЛАРЙЫЛЮЗВЯКШПЭЬЩХПИДАФЭЦЙЗВЩГДФШЭАШМШЭЭБЮЖЫЫА
ЕДЗДЯЛЕШРЦАБЫЖХОЕНЭЮКЫХВЮДФХЕШЩВУЙЬВЯЮЖТЛЯШЭАЛДЦЭЯЮОХЕЯЯШШЕЯАБЪИ
ЩОЕЮЗЯКБМТУИЮРДДФЕЩЗЯББТИЦКЫШЙИВЕЮПВПЫЧЖЦАБНЯЭШДЦНТРАЭЖУЦЫХЖУЗАР
ЙИОЕУЦЯЗЪЦАВЩДЦАЙЗБЧЖВКБНКЦИПШУЭЕКЭЖАНЫЧЭБКЭТЕНББЦЮЮОЦЩМЙШШЗЯОЕ
УЫЮРЕЗЕЯФЕЩЫЯОЖПИМКЫТЛУГШШАЫДДЦЛФЙЫЪИЦЗЮЩЕЮШЯЦЭГЙБЭОБВЛУГВЩВШДЩИ
БНКНМГРЙГРВШЖФЛДЖЕЩЕЪМЪЬВЦЩЖГМБТЖБКБФВШКЫЪЖУВЮРГГЛЮЗВЯОБЬГ

2. Разложить на множители числа:

(a) 612485256818638892606830692421

(b) 943381283807231133947757240895002596092970226419236938946523

(c) 13830081895106928567073280542918130161319710319422960543733338411936677927938165817690274 49

(d) 214301117768508375311540288922267112457510338300585504700945533018108327673526756301352607306087851507643580914172623977 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 10460797482367330806588857078662180947301549939457586997102630533721170059696 9$
- $e = 17$

Сообщение:

- $M = 7947822669239174518309700811804168099889803196748621980727420692546922319151$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 248176641411185110773094700223267183793$
- $q = 24327742332286954746215573995416398 4083$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 584814701055857773920573138135844651463453136974878774938249225584813016627 59$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 16758856990625942860073874352197729202 1$
- $e = 17$

Зашифрованное сообщение:

- $c = 70875697568870494083621576753431903290$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 32634352866901879493875704204490909078 7$
   - $g = 11732600593714764594604049284699303261 7$
   - $y = 28838897544792146743009268663237927346 7$

   Секретный ключ:
   - $x = 31970242983913248819395927575373539617 0$

   Сообщение:
   - $M = 33956401533936511851628607269679819027$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 16109384570140033202212952170720130211 3$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 26034493420583256559438399682249610813 1$
   - $g = 24435272749993035825514881460525732104 2$
   - $y = 20252867949731445363336594623919014481 6$

   Сообщение:
   - $M = 19310620296758153033675488528305657779 4$

   Подпись:
   - $a = 10747702029392531145490367350195532315 5$
   - $b = 16501575882649431978782631060791823195 1$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 727$
   - $g = 661$
   - $y = 490$

   Сообщение:
   - $M = 556$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 665$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 16$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 5

1. (a) Расшифровать текст:

СТКФНЦБСУНФХУЬККЗЦЗУГУЬКХКЙБХЦЦПМРКОЗПХЧЫКЦЗУГНЦЧУХНГФУФНФУФЙБПХ
КЦЧНРНЦБШЦРАЭЬЧУФШИЬКЗШНМЗКЦЧКТНЪУЖСТЦТСНЦНРПХКЦЧТИУЗУХНРПШРНТФС
ЩНРУЗТФХУСЬНЖУИЧШЬШСНСУОЙРКПЦКОНЗТАЬТКЬКИУЦПМЧБЪУХУЭИШЦБЗЦСШГВЧШ
СНТШЧШЙЗКХБУЧЗУХНРЦБНСХБНЗТУЗТЗУЭРЦШРАЖПУГТЖРКЙТУСРНЫКУТУЦЧЗНРЦЗ
УКПХКЦЧБТЦПУКФРЧБКНУЙКЧЖАРФУФХКЛТКСШФХУЦЧУНСНРУЪЗЧНРККХШПШНЙУРИУ
ТКСУИЗАСУРЗНЧБТНУЙТУИУЦРУЗСАУЖСУРЬРНУЧФУРТУЧАЦКХЙЫЪУМКЗТЭНФУЬШЗЦ
ЧЗУЗРНЬЧУТСЖАРУТКЙУТНЪНУЦЧЗНРНТЦСАУЦЧРНЦБУЙТНЗЦКЖАРУМЖАЧУСАИУЗУХ
НРННТКСУИРНТИУЗУХНЧБЦСХБНЗТУЗТХЦЦПМРСТКЗЦКЬЧУЦТКГТНЦРШЬНРУЦБЦЦСУ
ИУЗМЧНПХКФУЦЧНУФНЦРСТКЗКЦБШЛЦККФУРУЛКТНЗЦКНЦФАЧТНПУЧУХАСФУЙЗКХИР
ККИТШЦТАОЭЗЖХНТСАЗЦФУСТНРННФХКЛТККЦЬЦЧРНЗУКЗХКСУЖСАФРПРНТПУТКЫЦЧ
РУЖЯЦТЧБКОСУНФХКЙФУРУЛКТНУЦЧЗЧБЦКОЗПХКФУЦЧНФУЙЗРЦЧТУОФШИЬКЗШНШФХ

ЗРКСУОЭЗЖХНТАСЖАРУТКЗУМСУЛТУТКРБМЖАРУЙШСЧБНУЖУХКТЖШХИКФХКЧКХФКЗГ
ЮКСЗЦКЖКЙЦЧЗНУЦЙАШТКОТКЖАРУТЦЗКЧКТНУЙТУИУХУЙТУИУЬКРУЗКПФХКЙРУЛНР
КОКЪЧБЗЙКХКЗТГПСУНСХУЙНЧКРСУТЦТЬРПУРКЖРЦБНМЗКЦЧТУККОТКЖРИУХЦФУРУ
ЛКТНКУЧЫСУКИУККФШИРУККШЦФУПУНРМТРЬЧУУЧКЫФУЬЧКЧМЦЬЦЧНКНЗСКТНЧЦКЖК
ЗУЖМТТУЦЧБФХНТЧБЙУЬБМЦРШЛКТТУИУЗУНТФУИНЖЭКИУМУЧКЬКЦЧЗУСНРСХБНЗТУ
ЗТЦПМРТПУТКЫФУЬНЧГЧКЖЦЗУКГЛКТУГЬШЙТАКУЖЦЧУЧКРБЦЧЗЦУКЙНТНРНТЦТКХМ
ХАЗТУТНЬЧУТЦЗКЧКТКСУЛКЧТЦХМРШЬНЧБСХБНЗТУЗТЗАЦРШЭРСКТФХУЦЧУЖКМФХН
ЧЗУХТУОМЦЧКТЬНЗУЦЧНЖКММЧКОРНЗАЪУЧИУЗУХУПУТЬШЗЦЧЗУЗРЬЧУЦШЙБЖКЦУК
ЙНТКТЖАРЦСУКГТУУТФУЗЧУХНРЬЧУТКНТЬКЖШЙКЧСУКГЛКТУГППЦЦУИРЦНСУНЪХУЙ
НЧКРКОКОНТКФХУЧНЗШХКЬНРСАФУЫРУЗРНЦБИУХЬУНЦПХКТТУНЧПНСУЖХМУСЗЦКЖА
РУСКЛЙШТСНХКЭКТУЬКХКМЬЦШХЙТНПФХНТКЦСТКФХУФШЦПФУЙФНЦТТАОПХПШРПСНФ
ШИЬКЗНФУМЗРСКТПТКСШ

(b) Расшифровать текст:
ЪЙПШХЧМЩЫНТЙЬШУШКХЪЖИНЦСНЙДЛЪФЩББЩЗЫОЕЮДШЙЩЫТТМПОИШКХЩЭВНЦЪКВИВЧ
ЗЪДЭОЖЭПЧЯДХАЩЧСЭИВЫЗЭБШЭРОКЭЫЗЭБШЪДЫЕЮЬХШЙЕЪМШДЮЧКХУЩЧРПБЮЫФЙИЗ
ТКЧКЦОРЫМЗТЗЪЙПБЖАЭЬЩОХКЮЬХУДЯФПЮКХЖДХЗЬШЩЯКЩРХХГВЬЗЪЭЗЬЕЧДЙЩЩШШ
БФМАКШФПХГБФЧПГЯЭОТЙГЬРПКШФФЙНЩЧДТМРБРЩЙХДМХМЕЦХЛЗВДЖЙДГЪЗВЗЕЪОЬ
КТОУШКХЪЖАНЦСНЙДЛЪПТИЩОРЯДЫЯОШББФМЫБЮЦСЫБЙЧДЮЗЩРЙЪИЬШЭЬБДСГЭЗЬЭЮ
ДБДСЙЫЮДПКПЦЩБНХЮЕЧРОКШЯДЫЮЕСЧХГХБЕЫМЩЧКЫЯБФЪАИЬЦТХЖЬЬЙСЮЯФУЙЮЩУ
ЖТЙЗЧКГБЦЭФЭБЖФНЩЙВТЗЮОЦЪПЭКШЯПЫЙЬЦФЫЮЖСОЪКЖСОТЙБСЙЩБЖФНХЙЩЯЙЪЗЦ
ЪОЪББЬЗЪЭЗЬЕЮЖВПРЫРЬВЗЭЮВТФИЕГЬКПБЫШЗЪЛДШРЧДЫНЗЮОВОЪТЕБЯЕШПГСТТЖ
ДСУЯЖЦЪФХАЦЪТТТЕЦЙШКБЭНТГЕЧРЕАЬЭЗЦУЕЪФТЭЩРРШКЪЯРЪЮВДЗШЮЬУГАНЦСНЙ
ДЛШЗЪАВППШЮЫПНЪПЯЩПТЯВЭФЭДЮЦТТНЖФНЮУЬЮСЭКЕСГЩКЯФФППШЪИХАЯЭЖЫЗЧЪП
ЧКБСШПКЪЮЭЦЮВЬРЯДЯЭКЮЖЫЧОЪБЕЮХЬЕБДГЯЪМЦДТЗЩЧФТЭЦЫХЮОЬЮЮЮКМСНЮЗВД
ЖХКЖРНТБШСТУОРЭДТЗРФЩАНАОРЕБЯОКФЭЗФНХЮВРДЫМЩВМЧЙЫЗДШБЩШХУДЮЪПЫНЦ
СЫТЙХЗНСЮЗШУШШБЗОХНЦСЩЩДЬЮЖЮЙВЭМСЗЩСДЭПЮЪСХНЬЭНТАВОНЫКЖОЗДЗЛЮРХИ
ЩКНХУБЪЖЫЙЩПРСБЯЪКДОВЫТЫФЗСЕЫЛДФПЯШАСПЪБШФПТЛЗПЩТЮВНТЯДЯЭМЮЮВФОЯ
КЦЬКЖИЬОЗШБЯФОПЧШЮКПНЩЫРЮЗЗДНХНРЦТЫИЩРДАСЮЪФЫМПСПТОДЪПАЗЬЭЮЮИЩЭФ
ХОШЭПЫНЮРНТБЦЬХЧКГФУХНЯСЖЫЮЯЪПТНАЪФЭЙЛЯДЮОЦФУЧЗТГКЯБЯИПЫИЩЩДЫЗБЪ
ДПФЬСРОХЩЭФПКЦЦРЯКДЪОЯЖБСЩЪЙВЪЩАОЬЧУЮДЯИПЫМЫОНТЖЯЪОЫБЦЪРОМЪСПХБЬ
ЩОХЙЗЮХЬКЫНЭШКГЬКДДБССЭДЦСЖЕБЭШЗЪЮГЬКЮОБФЫТЭЗЩФЫЮНФМЫЮГЯЕДБЦШПТН
АЩСЫИБФНЫОВШУПКЬШДЫЛДЪУЫИВЮМЫЯВФЙДБАЮЭЧКАЩЗЬКЕЧПЬМЬСЧШНАЪФЮБХЪФП
БЛЧСЭДХСЕЛЖЖОРТИЗЭХСПЪЧХЛНРЩРСЙВПРХГЖОРХСЯКЖТЕЬЫТЫФЗЮЗОГНФФХОРЭК
ЭКЖЯМЫОВЬХЛКБЪГХВЩЮЕШГЗЫХРУЩОЙЮЮЩЬМШДЬЮЖЮЙВЭМПМЗЦРЬДЕФУШБШЪДШКШЪ
ГЭКЕЦЙШЛЗПЩТЮШСНЫОЦЪЗЭГХСТТИЫОФ

2. Разложить на множители числа:

(a) 7432589019322810829251187959 21

(b) 1200140869855202663488126241767214488180932746082228772098673

(c) 1419567179656689778491223699017972180586858276797490689916016096202960634839009494465792737

(d) 1625535421920486587503557178373214235215955316244683314139613112005526433823194605932345922582984441644697839863905674803

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 658462093526629628548072984664794278643903500654341819937491551201690687118 99$
   - $e = 5$

   Сообщение:
   - $M = 230080512915839842874357513897992188470754684559124016788419422219677667501 15$

   В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 230001351202769757985213195117654986551$
   - $q = 249479625489839056833319754823018122137$

   Открытая экспонента:
   - $e = 17$

Зашифрованное сообщение:

- $c = 37402794991673293972154872981993301066231592932335524200182637823191755856154$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 18228848877629796248107837659116253378 1$
- $e = 3$

Зашифрованное сообщение:

- $c = 884987303245287950325623188630301143 09$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 307406056695394740931576340099095736441$
- $g = 297734436889033724624487515574640069674$
- $y = 154792899226850273678483203228710720816$

Секретный ключ:

- $x = 162018796708523004715828161741558036799$

Сообщение:

- $M = 152826624115908434937622474698112542228$

Использовать следующий случайный параметр для создания подписи:

- $k = 154207052462014272970796501589870528887$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 333161257480680758001007411061707644817$
- $g = 133731259217747622214842784511127035019$
- $y = 122614504117594941397767012415317721285$

Сообщение:

- $M = 27354859927306366316410321643439405847 6$

Подпись:

- $a = 191097436695714947672426488889704549421$
- $b = 30695518096909432713558859380811497830 2$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 983$
- $g = 186$
- $y = 300$

Сообщение:

- $M = 90$

Использовать следующий случайный параметр для создания подписи:

- $k = 557$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 15x - 15$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 6

1. (a) Расшифровать текст:

ЖКЗЛЙВПЭИЭЯЕЭЙВЖГФВЖЬЕЭБЬЖГЮЭЕЩУГЖЗКФЖПЛКАКФЙЗЖЙИЭЬАДЖЭЫЖЙЭДЭБЙК
ЪЛЪАЬЭКФЖЗКФДЖЦДИФЦАЪЕЖЪЕЛЪЬИЛЫЕЭЖЮАЬЕЕЫИЖЯДЭЕЗЖИЯАГЪЬЭЕФЕЯЕПЭЕЕ
УБЬГЪУЭЯЬЪЙДЛЦКЛДАЕЛКЛВЖЫЬЫЖКЖЪАГЙЗЛЙКАКФЙЪЬЖИЖЫЛЯЛИАЕЪЖРЭГВЖДЕЭ
ЪАЯЩЛЬЭИЮЪИЛВНЩЛДЫЛЙЪАЬЖДПИЭЯЪУПБЕЖЖЯЩЖПЭЕЕУДПКЖКЖВЖГФЕЛГЖДЭЕЪЙЭ
ИЬОЭАЙЗЛЫГЙЙДЕЭЯЕПЭЫЖЖЕЪУЙГГДЖЭЫЖЬЭЕФСАВАЖЩТЪАГПКЖАДЭЭКЬЖДЭЕЬЭГЖ
ПКЖКВЖЭЙЗИЖЙАГЙЩЭЙЗЖВЖБЙКЪЖДДГЭЕФВЕЭЗИАКЕЖЙКФЖКЪЭПГЖЕЗЖЬЪДЕЭЩЛДЫ
ЛЗИЖПАКБПКЖЙЭБПЙЗЖГЛПАГЙКГЭЭПАККФХКЖЩУГЙЭВИЭКЕУБЗИАВЯВЖЪЙЭДЖКЬЭГ
ФЕУДЕПГФЕАВДИЭЙКЖЪКФДЭЕЫЬЭЩУЕАЗЖЗГЙАЕЭДЭЬГЭЕЕЖЖКЗИЪАКФЗЖЬВИЛГЖДЪ
ВЯЕФЪЙГЭЬЙКЪЭЕЕЛЦВЖДАЙЙАЦЛПИЭЮЬЭЕЕЛЦЗЖЬЭГЛЗЛЫПЭЪЩЛДЫПЛКФЕЭЪУЗГАЯ
ДЖАНИЛВЬЭГКФЕЭПЭЫЖЙВЯГЯЛИАЕЬЖГЫДЖБЗЖЪАЕЖЪКФЙЗИАВЯЛЪЭИЖКЕЖЙГЛНЖКЪ
ЖАНЬИЛЮЭЙВАНЗЛКЭРЭЙКЪАНЙЗЛЫПЭЪУДВВЕАЩЛЬФЬЬЖРЭГЬЖЗИЪАКЭГФЙКЪЕЬЭЦЙ
ФПКЖЬЭГЖЕЭЩЛЬЭКАДЭКФЕАВВАНЗЖЙГЭЬЙКЪАБАПКЖКУЖЗИЪЬЭРФЙЗЭИЭЬВЖДАЙЙА
ЭБЕЭЛЕУЪБАЖКЗИЪГБЙЙЖЪЭЙКФДЖЩУГПАЙКЙЛЬЕЭЩЖГЙЕЖДУЙГФЖКЙИЖПАКФДАЕЛК
ЛЙГЬВЖЫЖЙЪАЬЕАДЖЮЭКЩУКФЕЕЭЙВЖГФВЖЭСЭДЭЙОЭЪЛЙКИРГДЭЕКЭГЭЮВЩУГЫЖКЖ
ЪЯЛИАЕЬИЛЮЭЙВАЙЖДЕЖЦЗИЖЙКАГЙДЭЕЗЖЙЬАГАЪКЭГЭЮВЛЙЖДЕЖЦЙЭГАЬЪЫЛЙИЙЙ
ЩГДАЕЫЖГЖАЗЖЭНГЗЖЩЖГФРЖБЬЖИЖЫЭЫГЪЙЛЬДАИЙВДЖГЪДЖИЙВЪЖГЕЗЖЙГЖЪАОЩУ
ГЛЪЭИЭЕПКЖЪАЕЖЦЪЙЭДЛЩУГЖЙДЖЪЖГФЕЖЭДЖЭЖКЙЛКЙКЪАЭАЯЖИЭЕЩЛИЫГЭЫВЖДЖ
ЫЖЗИЪЬКФЙЕЭЯЬЕАПЭЙКЪЖЕЭКЖГФВЖЕАВЖЫЬЕЭЩУГЖЯЗИЭСЭЕЖЕЖЭСЭЪЙЭДАЙАГДА
ЩУГЖЖЩЖЬИЭДЖДЖЫЩУКФЖЩЪАЕЭЕЪАЯГАРЕЭБЯЗГФПАЪЖЙКАЕЭЪЖЙГЛРЕААЕЖЗИАКЭ
ГФЙВАЭЙЕЖРЭЕАДЖАЙЗЛЫПЭЪУДДЖЫГАЩУКФЬЖВЯЕУДЕЖЮЭЙКЪЖДЙЪАЬЭКЭГЭБАЬЖГ
ЮЕУЩУГАВЯКФЙЗЖВИБЕЭБДЭИЭЪЭЙФДЗЖЬЖЯИАКЭГФЕУДАЪЖЪЙЦЬЖИЖЫЛИЯДУРГГ

(b) Расшифровать текст:

ЗНЭАВОЧТЭГПЗИБСЧЧХДГТКЪКАЗХХЯКЛТЬАПСШЕЧРУНФЙРФМЧВЖЭРЮГГЦЙГЧКНТТД
ГСНПНХШУПГММНСЧРЗКЮЙГЧЧХЯГХКЭЧДОЗААРИКДЭМУЦЬАИФОЪАЛФСЫШГШЖИДЪЧФЮ
ЕКФКРАЖНЖПЪРЛРХГГТБЛЬМШУЭДИИКШЪИФЙАКЛФФЭЪЕЦКШЮМЛЖТЦЛФКЮЬОФЧЮДАФФ
ЭАЧПЧТЯВЦКЦБГШХЫФЖЭФЭАЧПЧТФВФЧЙФПОРЙЧАУЗИУЩСНСЭКЛТОАЙЛКДЧКЗРРАВЛ
ЧТЭЖЗРРАПСУПЪРЛСТЯНЦУЮДЖШКУЧЖИАЬЧРЦТСВГОЬОЕВВЧТЕАЛХТЯЩЭЧЫЙРФЧАДМ
УМЬЭИСНФЬОБРШЪФФХАЬКОЖИЭИРЦАЮПЮКСКЖПСЯЕЦРФШЬЙХУШЯМИХЯОКЦБХФЛФЗЪГ
ИНРЩАЗФЧТИИШУЯЧЯХШЮДЖШУСЯСРХФУМПТХЬКЧНСЪЕККЮОЖТУШЙЖЩСХВРВЧЧЕКОХЯ
ОСМЗЩЧПШКЮЭСЮОДДМШСТЛГЙУПАОШЦСЧРЛЦЙЭЖРХХЙЙЮЗОВЖУЗХЦЖШКДЧОЛМЬДЪТН
ЪЕРИЦХЩДЦЧЪЧПКЙХЮПНРЫЦГПУЯФГЭРТЮСЗЧЛКИШЗТВВБСРАЙФЦЫЮЙОЫЫЧБФФЫЬОБ
ЧЫЧКФХЖЪЛТНЫШЖИРТЯМЗАШАСКНПЪРЛРЙЯМДЖЫЦОФЦЯЪЬЙРФХОФМЪАПИКЭЬЙОНФБМ
КЦТЦЩЫЖЭААЛОХАЯЦЧЮОИФСЪЧПРМШДГХКЭОНФХЫЯМШФТВВИКЭЪМЙУЪОАФХПЭПОЗФФ
ЖСЦЬАЯЦКПЯКНПЫЯМХЬТЯЛБСЮЕУОСЩАУФСОДЬЮППНПШХТЭЖСНФБЖЧЧЫЭГШНЕХЛЩРФ
БЩСГЖЪЗХУЭАБНПЭЪХИЗЮЧЕТТЫРПЫЗЯЪЙНХАЬЖТЧАКИЩНЩВЪДНПЯМИТАЪЯБЦЯВМИА
ПЧЙОЪЪФМНЙАЗСХУЭАБСКУЭЦИЖЭЪЛХХЫГРЦКШЧЛУАЦЦОЫРЫРОЩПЫРМШЫЩАГЙУЯАЙХ
ХФУМПТХЬМИЖТШАЮУЯЯГФЛХЦЛУУЦЯЦЛОПНЙНПХДМШЬЮАЯФЙЭЪЙЧБХЯХСТЮАИЦШУДЪ
ЩЦЬЧЙУТТГРОКЖЧЛЛЦЧАЙВПЫЕВЦУПЯМРНЭБЖЭШСЙЛФЖЭАЦЛТЪНЗЩИЫЦЖССЪЧНЦСЫФ
БЦШСОСХРХЯКОТАДССНЕЪЙЧЬАФПШЗЬВЖЮКСФПЛЖАФЖККШКАЗХХЯПОЙТФЦЛИЫЯМРХЫ
ФАСКЪЯМПЧЭФГОФТВГКТХЮАЧКЪКГЧКЩЧЗЧЧПАКЛТЬАВККЭШЖИРХБМКХАЬЖШУШБИЦК
ЮДЪУПФЬМИНОКИОХГЧАФПЭЕДСТЮКАЗХХЯЯБРАШПУУОЭГККЪАВУУЦВСРУЦБООЛХЮЙФ
ТЭЯГУАЦУМРРХИМЛИЫЪЕФЖЭШЙФСАЙГУНТЪЕСУОЕМУСТЦЙЛТЪАНФЙЪЭБФРЫФСИМРЭЛ
ЩРЪЮГУНЬВМОМЪЧПЧРОНКОТТФЛШТИЮБФРЫГМТЗТКРВКРАЖИЦТЗИЦУЩЧГЛЧЫДХЧЧЫЭ
ННРЫЦГЛЗЫЬОЩЛХЭЛЧНЮЬООПЫ

2. Разложить на множители числа:

(a) 448470209357269059101232922433

(b) 952207848611281372061727748919603695651903503867072949927559

(c) 747274403388715513359170422715141592558564918596296169033443451137195750343214222568383113

(d) 998845478222313873688905269137091223989720338114396945671722244695277530143868262435633288761032815855490125461176335871

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 762941656594587457096760534645952189546370109578503966975611707168199369819 59$
- $e = 3$

Сообщение:

- $M = 4948515219660105959369297340517484979838503254546328615341707736831515750194 7$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 243710093034362404679908916678457379793$
- $q = 195264709454563231184557998492002815187$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 104901513099257718938805785138116740736506182884201461455747833068628864308 18$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 294085906966708800669468510817766926709$
- $e = 17$

Зашифрованное сообщение:

- $c = 899482529336791961092430480986874128 49$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 21475145588801241410832338672180919103 3$
- $g = 12514082796237746132300920261437216573$
- $y = 17261694261396026913547351393211022251$

Секретный ключ:

- $x = 14811419443505971924319691608515104013 4$

Сообщение:

- $M = 34672274374506669427694248481514104577$

Использовать следующий случайный параметр для создания подписи:

- $k = 15819246286577905198719026121198095236 7$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 331970697182756643273436580916895579387$
- $g = 82175055559007891077061428664509813986$
- $y = 19677969304114755845973375893604417974 5$

Сообщение:

- $M = 81722755503985973533507295763133048147$

Подпись:

- $a = 20192167113675890442103392446533141018 8$
- $b = 15698640064405504381608948279023032946 3$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 809$
- $g = 137$
- $y = 203$

Сообщение:

- $M = 204$

Использовать следующий случайный параметр для создания подписи:

- $k = 409$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 11x - 14$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 7

1. (a) Расшифровать текст:

ФЧУЛЗФПШЛЧВФУУЛЩРЩЧОШОТЦВОИУФИУЩИОКЛСКТЩЧОКЛИЮЩДУЧРТЛПРЛХЦФШОИЩХ
ТШУОРТЦВОИУФИУЧЛСУКЦЩЙФТРФУЬЛЧРТЛПРОКТХЦОЧШСВУФУУЛЛЧТФШЦЛСТЦВОИУ
ФИУЧФЧИФЛПЧШФЦФУБЗЦФЧОИУЛЧРФСВРФРФЧИЛУУБЫИНЙСКФИЩЧХЛСЦЧЧТФШЦЛШВЛ
ЛЧУФЙКФЙФСФИБФУЗБСИЗЛСФТЩШЦЛУУЛТХСШВЛИУФЭУФТЭЛХЬЛОИКЩЮЛЙЦЛПРЛЛПР
НСФЧВСЛШЧФЦФРСОЬФЛЛХФСУФЛОЦЩТУФЛИБЦМСФИМУФЧШВОЧХФРФПЧШИОЛЙФСЩЗБЛ
ЙСНОСЛЙРЩСБЗРОТЛСОХЦЛСЛЧШВУЛОНАЧУОТЩДКТХЛЦИХЛЦЛЦИСТФСЭУОЛИБИЛЦУФ
УЛНКЛЮУОЛЧРНСФУШФЭУФШРЧИЭЛЦШФСВРФХЦОЛЫСОНХЦФИОУЬООИБХЦОЛЫСОЧИЮОТ
ОЦФКУБТОУОРРУЛШЧХЦОЛЫСФКУФКУУФИБШРЛЯЛТФСФКБЩТЛУУЛШУОФШЬУОТШЛЦОИБ
НКЛЧВРФУЛЭУФХФРРОТУОЗЩКВКЛСТШФЭУФШРЧХЦОЛЫСХФКШВХЦФЧВЗЩЙФЧЩКЦБУЛИ
БЧОЦФШИЛЦФШУФИБМСЩЛШЛЧВУУЛЧХЦИЛКСОИФЧШВОФЗОКЩУОРРУЛШЧХЦОЛЫСХЦФЧО
ШВТОСФЧШОУЛХЦИФЧЩКОХФНИФСВШЛЧХЦФЧОШВРШФИБШРФИБКФЭВРХОШУТОЦФУФИРХ
ОШУТОЦФУФИШФЙФЧТФЙФЭШФЗБСРФТЛУКУШФТИФКУФПОНФЦЛУЗЩЦЙЧРОЫРЦЛХФЧШЛП
ШФЭУФШРЧКТРНСФЧВЗБСШЦФУЩШОНИОУОШЛТЛУЧРНСФУЙФСФЧФТЛЯЛЗФСЛЛСЧРФИБТ
ЛЧСОИТЛЮОИДЧВИИЮОКЛСУФЗБИДХЦОКИФЦЛОНАЧУОШЛТУЛИЭЛТЧФЧШФОШИЮХЦФЧВЗ
ОТФМЛШЗБШВТУЛЩКЧШЧИТХФТФЭВТЦВОИУФИУИЧШСОХФЭШОШЛСВУФЛЛЗСЙФКЦОСИЧЛ
ИУЛОНИЛЧШУФПКТЛУЛИФСВУФХЦОИСЛРСФЧЛЦКЬЛОИУЩЮСФКФИЛЦЛУУФЧШВТЦВОИУФ
ИУИБУЩСОНРЦТУЧСФМЛУУЩДЗЩТЙЩОХФКСЛЛУЛНУРФТФПЧИФЛПХФРЦФИОШЛСВУОЬЛР
ФШФЦЧШСЭОШШВЛЛХЦФЧЛЗЧУЭСФУЭОШСЧИОКФТИУОТШЛСВУБТОЗСЙФЧРСФУУБТУФИК
ЦЩЙСОЬФЛЛХЛЦЛТЛУОСФЧВОТЦВОИУФИУЧСЛКФИИЮЙСНТОНИЧЛТОЛЛКИОМЛУОТООЧХ
ЩЙСЧВЧШЦФЙФТЩИБЦМЛУОДГШФЙФСОЬНТОУЩШЩЧШФСВХЦОШУФТЩОЧХФРФПУФТЩИБХЦ
ФЧОШЛНЙЦОУЛИЧРНСКТЧЫФСФКУБТИОКФТОТХЛЦШЦОЬУЛТФМЛШЛЙФХЦФЧШОШВФУХЦ

   (b) Расшифровать текст:

ТЯНИЦБЫЧЖУЧУГЛФЕСЪЛЧИТЗЪЩОНВМЖКВИВЫЩЖБСФОЖБСХЧМСЛРКФЭНЦТСЪЯЦВМДГ
ШИВИКЛИОЪЕЙУЕСЛМРЖЮННТСГАРЧТЯЕУМУИЦТППЯЙЦНЙЗЪЩИПЗКННЛВЕЖБЕЪПТТЭВ
ВНЮТСХЪОПВЛНОТЗАРТРЪРШУЩИПКОЙБЖФИМГПЪМЙМРЦЗГЬВЦРПЗАНЧМЦРЖШЛВУФУС
ЖЪТКЛГЗЩТУЭПЪНФДЖЩТЭЯИХЗЯЦВКЕЕСРГСЛЬЙЯТПЭЕКОМЭЦДПЙЖРДКОМЙДНЙЯСЧЕ
УЕСАИОИРФЧУГВКЕЕСЛЯЛЭВЖТПЖЗОЫШЙВИХЗЭЦАНДЭДГЪРФНЕЧИТВАЩЕНЪЛЦВТЯЖС
ППАИППЙЖЛФНЖЯИЦЕЕЪЙЦЧУГМХЗРЭПХПЖЗОЫШГДГЪЕСЦСШГОЪНЦЕЕЪРЯЕНИЛЫЧЙЗП
ЦНТАСОВРЪРНРВИОЛЕНГРЪЬЕДМКЕТВЖЯТЭВГЪПФЖИСППЖЙЫЖЙЗМХВСБЖРДРГРХЕУА
КТУЕДМХЮЦЪРЧОСГУЫДВИВНТТГЙМТОЪЦФТПВЕЧИТВАЛВСЩЖРГЕЪГЛОРННЦРУДММЙЖ
ШМЩЮЕБРЫШЛГРГСЛАКЦЙРЖНЦРУКОХИГНЖССГЪГАКУИЙТЕГБГЩТЖЖПЦРПМИЦЮГЯМЪО
СГЗФЕОЯОНСУЭЙРИГЕСЯИМЬБЦБУУЦТЕЕЕМОЩЖУОЫКПУЯЪЮЩЯНШОШЪЙНГПЖМКНЙБЛР
ЕНДМУОЗЭЙЧЕСЪВЩОВГЬХСУГЙРНШАПКОЖДЖЩЬНГЙЖБПДЩЪСУЧМФЕОБСЯИМГИЫДЗГР
ЧРГАЬЪМЖВГЩЛЙИДХЕГДГЪЕСЦСШГОЪПКОЕЭЙЛЛИЖННРВЗЬАКЙВИЦТПЕМНДГЭБУОТС
ВЦВПАЪХОНЪВУЕОВМХКПВГЮООЯМХЧЙАЕЧЕШЗЙЧИТСКЦВПЩЛЦМРЯГЪЕТДПЧОСЗМФСО
АМЯКЙЭНЦДПЬАКМЖВПТЗМЧМЪТЖЦГЧИТСКЦКОЩОНЮЛЕЙЦВЙМСФОЖБСЩТСЭЛХОНИРЦВ
СЭЧЫИЕЕСЛУУРГМЕЩСАЦРЖВЯЫРДЖЙЫЖЙЗЪЧОЕЪБЦНШАЪЩТГГКРТЛЧПНМПЭЯУЕТЗЧР
ЕОЩГОДЬЕСАИМЭПДВНЪПЪОГЪПНЛПЮННТЖЕЯЫРДЖИЦЙЗЭЕХИПЫЖМЛНЪЛЩКФЯАЩТПЕМ
ХЕДАСЭОКЭМЪДМЪЛХОКЖЙЫЖВГИЦТПЕМСЗНЭЛЫТФЩСФЛТЗИРМГГПЪОСШМФППЯЕУСЭБ
ЛНТЗЯЖФНЖЖХЩТЙЪКХОТДМШИУСЯГЛПВГЯЕДГЛМРФШМСДЖВЪЧОФЗОЫППЩАНЗЖВЯГЛЛ
ЯОГЛЭЛСМОСГДХКЙЦЖЪКФАМОИМЭАХЕЖМКЦДОДМЛРЖЦГЮСШЮЛГМРЕЖЙОСГКРУИАЩЩБ
ФАИФИЙДЖШОДБЖЧОТАГМНЙБЖПНЛБЖМОННЛНГПЦЙЦВТЗАШОЕЭРНЛЙБМРБМШМЩЛПЧЖУ
ИНЪЛЙТЯНИЩКИАКХЕРЕМБЙРЪРШСМИДРВЖЕЛЦКПБСЧРЙЖБХЕЩСПУУЩЮПХЧМСЛРКПЧЕ
РХМЖИЦЙОЪБЦНКЖЛЩЛФЫЯЫНЖВНШШЙЧЗЩОУЖЙЫЖВРЛНОУШМК

2. Разложить на множители числа:

(a) 500992959103708508449510337633

(b) 74371829159075141270730817946393093438847476129288220870251 41

(c) 11505083319691272711077667059070489401435787737921522657685864898493658825636443558905905 49

(d) 22728358156603307494964811152381244944237690364623905471962500909848450845836287603034131064106245717175640467284538051 77

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 391075182732561389507135627317894710939560573520876059191857898839347844276 31$
   - $e = 5$

   Сообщение:
   - $M = 14688508815241000963873630934555523305606984946035213270035370901495934679450$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 29781223085645856469578456002986303796 3$
   - $q = 26615325120846838647861479028276764691 7$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 13697395877507084910349784306300971208258687768819783066822921671817304614589$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 184994795309366879117980226042932833041$
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 17388481500117029189058670162625502479 3$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 31524425646841871356364204448552617974 3$
   - $g = 21172659773114220545262399230342097320 6$
   - $y = 19745007053138887729227137919384113847 8$

   Секретный ключ:
   - $x = 21075855554620315810136001335786423867 6$

   Сообщение:
   - $M = 12178474467879195182479392717049865663 5$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 13714691429352523009233141455037554525 5$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 28665551648178245942029791351758790107 3$
   - $g = 22050752202396569444237897941939106567 8$
   - $y = 18372131520152466290657242427405592076 1$

   Сообщение:
   - $M = 12004602620207418853660075325877222219 0$

   Подпись:
   - $a = 64445164120902483940167802539959026308$
   - $b = 16632510340589202996263495150968017997 4$

   В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 821$
- $g = 130$
- $y = 706$

Сообщение:

- $M = 568$

Использовать следующий случайный параметр для создания подписи:

- $k = 319$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 3x - 16$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 8

1. (a) Расшифровать текст:

ББИНВЗРЕВИЛЯРЫНЛЦРДЗЛПЛНЛЖКТЛБЕИОЩКХБВНВЯКЙЦЕЗРБНЕИМЛИЛХБЙЕФВНВД
ФВПЯВНПЩФОЯЧВТИЯЮНОЗЛЖБЛЙКТЛБЕИОКБНРАЛЙЗЛКУВОВИИЛХБЕЙФИЕОЩЯЛВОЩ
БРТЯБНРАМЛОВНВБЕРИЕУШЙЦЕЗКФИЕТРБВНГЕЯПЩФПЛПЗЛВОМНЛОЕИОКВПВНМВКЕВ
ЙДОПЯЮНЕКЛПЯВФИЙЦЕЗОПНРБЛЙЛОПКЛЯНДЧНВККШТОЯЛЕТЗЛКВЖЯОЙЛЙББВИВРЯЕБ
ВИНЛАПЗРЕЗНРИЩКЛАЛОБРЮЕКЛЫЙРГЕЗМЛБЛХВИЗЛЙКВЕОКИХИМРОМНХЕЯМХМЛНПР
ФПЛЪПЛДКФЕПОМНЛОЕИВАЛДФВЙДБВОЩНЛАПЗЗЛАЛПШЗНРИЕХЩБЙШЮПЫХЗЮРКПРВЙЛ
ПЯВПЕИЛКМЛФВОШЯОЩАБВЯХЕАЛОМЛБОМНЛОЕИООВНБВФКШЙДЙЕНКЕВЙАЛОМЛБПЛКХ
ЕАБВМЛЯПЛНЕИЙРГЕЗАЛОМЛБКХЕЯТИВЮКЛЙКЮНВЗЗЯКЮНВБКБНЫТДВЙОЗЕЖМЛОБЕИ
ЯЕХЩЕТЯЗЛИЛБЗЕЕТЛФВПЯВДПЕЗЮПЫХЗВАЛОРБНЫЮЛГВЙЛЖЛПЯЛНФЕЯЖБРНЗНЛАПЗ
РФПЛГВПШДВЯВХЩЗНРИЩКШЖЙВБИЕИЯШОЗЛФЕИЕДПВИВАЕПНВОКРИВАЛЯЕКЛПЯРТЛ
ЕОЙЛПЛБЯЕКРИНЛАПЗРЙРГЕЗЙЛЖАИББВИКЙВКОАИРМШЙКВБЛРЙВКЕВЙОВИЛМПЩЯПВИ
ВАРЕЯВИВИОЗЗПЩЗЮНОЗЛЙРБЛЙРТИВЮКШЖКЮНКТЛБЕИОКБЯЛНВРДМВНПШТБЯВНВЖО
ПЛИЕБЯЙРГЕЗПЗГВОБРЮЕКЙЕПВИВАЛОПКЛЯЕИОЩМНЙЛМВНВБКЕЙЕЯШОЗЛФЕИЕЮНЛО
ЕИОМНЙЛККЕТЛПЯЛНЖПВБЯВНЕОЗДИЕЙЯВНЛПКЛЯЕБЙЛЖЮШИОПНХВКМЛЗНЖКВЖЙВНВ
ЛЮРЮВГИЕЮНЛОЕЯБРЮЕКШМЛМШПИООЮЕПЩДЙЛЗБЯВНЕЯШИЛЙПЩКЛБЯВНЕЮШИЕБРЮЛЯ
ШВЛАНЛЙКШЖДЙЛЗКВОЛЗНРХЕЙЯЪПРЙЕКРПРОППКШЖЙЛИЛБЛЖЙРГЕЗЯШХВИЕДИЫБОЗ
ЛЖЕДЮШЕОЯЕБЛЙКБЙВКШЙОМНЛОЕИЙВКЗЗОЙВЫЮРКЕПЩАБВКБНЫХЗДВЙОЗЕЖДЗНЕФ
ИВЙРЗИЕЗКРПЩВАЛЗЛЙКВОЙКБНВЖСКОЩВЯЕФКВКБНЫХЗЛПЯВФИЛКЙКВАЛНБЛМЛБЮЛ
ФОЩФВАЛКБЛЮКЛЯЙВОПЛЛПЯВПОТЯПЕИВАЛДЯЛНЛПЕМНЕПЦЕЯЗБЯВНЙКЮНЯВИВИЕТЛ
ПМЕНПЩДВЙОЗЕЖЮШИЛДРМНЙЕИОКЛЛПВФВОЗЛВКЗДКЕВМЛБВЖОПЯЛЯИЛЕККВАЛЛКЯШ
КРИЗИЫФЕЛПМВНКЮНЗЕКРИОФВНВДМЛНЛАЕЯПВЙКЛЙРАИРОИЮЛЛОЯВЦВККЛЙРДЗЕЙЛ
ПЯВ

(b) Расшифровать текст:

ИРКРЬНЮОНЪИДЩЪТЯЙИЦОЙЖЙЦТГЕЛЩЧИБТБНДВНУЦЖЕЛЧХЬЪЧФУЖЬЛУКЛВНУФИПЛФ
ШЮЛТНЭЦКБЯЧИЮОУУЗЭКУКСЭХЦЧИДЩЯЧИЪЛЪККЖШЪУЕЭХЦЧЗЛСЦЧЬЭЭУЙИИФОТХБО
ЩРХРЩМАЖЖТЧЪЗЛСЦМЗКВМККЭИХЖЕАНТУЛДЛЪРВЪФЩЧЦЭЙЦНМЖУТУЛКВЯШМФТНТВЯ
ЩФНЕАИНРЯГТБНДЛЛЭЧЦГФАЙВКМНРИЙШЫФЕАХЦИЕЛЗЦПИДЩЩТЯЫЩТНЫАШТЧВНФЧУЮ
ЪОЛРЛФШЦЗФЭНОТЛЛЙШУЫКФЦЖКЛЮЩБЬЖИШИВЗЛШКЬГОКЦЦКФХУЮЕЩЪУЗЬЦЫИНЦЧЪУ
КЖУЫВМЖХЦЪИЮЛЙАЕЖУЧРЬЕОНЦНЬУЧУЫЛЦХУЖЛТЦХШЙИНРЦАЭЦЪЕЗФФНЗЛШХУМЖСТ
ЦЦЖТЦНЫЖРЦФНЙШРРРУУЦЗДЛНТШМГЧКЭНЩЩРМЮИЛФРНЩДТТЗУПЧКЗАЛФЖНИОРПСВФ
ЖЧВНФСКБЬБФТЯЗЦРЦЗАСЩЦИЕРЦЧИИФЛУЗАРЦИЮЕЛФУЭЭФПЖХКВРЗДЖШЦХИДКЦЦВН
ХЦХЬАМЫТЯПШЦФКЖЦЦЬЯЙРЦКДЖЙМЦИЖЗШЛШЙУРСЛКЦХТХЭФЙЦМЖШНРЦЙШКСИЭПОНБ
ЕОЯНМКЛУББВЯИРТВКТНТВЩФККЖШХУБЕЛЪФИЖХГЧНВРЩХИЬУЦЬЯГФККДЛХШКЮЪШДЦ
ЛЛЛКККАДХКЛДФЪХЗЪЧНЗИЯТЦЛЗЖЛЧХЯЯЦНТВЭРЧХЯЬЦЩЦНЬРФТПЖКРРЛЪШЦСЛЖЧЪ
УЗАОЯШЬЙШКНЮЛЮРПИЫКЩШУЭЧЪЗЯЕУЦЦМФЩЩЧНЗТНЬМЕОФЦЕАИНЧЛЙУРСВЪУНЦЗУЫ
КНЮЭУРЪЙЭЦКУЛЖУРСЗЭРПРИЙВЙШКЕЛБКЛЪОШКЙЙШКУЬГОФАЯСЛЙРНЮКУНЙЖЧХКАЕ
ФСФНЙШГТЯЪКШШЭЛИРЙЯГИЦХИКБРЗФЭЫУТЫИЧТУГЬИЦХЗРЛСШЛЬВЙАЙЭЦКУШДБЩРВ

ЦТЦКШЩБУУИЗЧНТВЭЭЪУЫУЗЪГТВУНФКЖЙХКЬГЧХСЯЕНХКЬЖСДТИЭИЦМЬИЯНТВЭХЦЙ
ДИФКРШИФМНМЭСДЦДЛДРТЯЗФЯКЕЩБНИИЛТГЭЕЭУХАЖЖЧУШТЕОНСЛЩЛЩФИВФСЦМЪФФ
ЗХЗЦГИЗЛСРМДАЗРЧДАОКНАЛТЪШТВИЩЧКЭЭНЧЖЭУХПКУСДЫЯЙИРЙИДЙУШЫЖРЦИИЖЙ
ЦХСЭУРЧВРЛЛУЬЖЦРЧИЕТХКИКЛЮЖИГЛХФКАЧФКККОРЛЯГЛЪЦМЖЗЦГЙИФЩЧВКВЩФИИ
МНТЗУПЩЧКНФФНЮЛНХКШЪЧЧРЦЕДКНАЛРЦСЗКЧУЖИЖЧККУЭУЫФИЙШНРВЙШЦЧЕЦКРЦЙ
ЭЭУБЗУТРРВОТРЧВНФХБДЖХЦЙПЖМЫПЙЖЧЪКЕЭТЪШТВХШНЙЖКГСЯКХЦРИЫОЛУЬЖЦРЧ
ЗЬЦНОЙЭШШУЬАЭЧКМИЩАФКАЛЭРИЕИЦХИКОУЦНЯУКУМЪФНОЫЖСНМЗАЗУИИЙСЦЗВЭЙЦ
ЦМГУТУЕЭУРННЙШШКЖАСЛРБДФРТЫЖСДТИЫФЯЧИЮИФКЛКФЦЧРДФНИИЪООШЬЗФЩЧЯГЛ
УКААШФШААРЩЬЯИУЦОЫЖЦЦЙИЦИНЦЯГ

2. Разложить на множители числа:

   (a) 5447901683072246433149566037 71

   (b) 1209722951824309891097833866933046541041607437139800451194187

   (c) 1589238766862293273842561185942222582640436654842032452142311848580150442710759492554603053

   (d) 1971903677623741193012293242903756249208037603857034305574011180470637641608389966259031498090774466010246969198368401169

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 418602902968502613433625956284282921210617323728788358473802643994843061699 59$
   - $e = 257$

   Сообщение:

   - $M = 256069877335610808231329487919594874031267501952952765658316292730647690835 74$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 303804569630865488963681060201606841379$
   - $q = 261291750251496698470843127988690892451$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 763670061861332611231246639787259854179791412486865147183841015436393758844 52$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 171103594828940730058440843110662533013$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 334141970400751645442679169201192639 93$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 202499288676346224391617471042441400637$
   - $g = 200711081454838190978625378396677371617$
   - $y = 290520914814613704358870759530086270 23$

   Секретный ключ:

   - $x = 127596002936168974564046503872380529682$

   Сообщение:

   - $M = 157100931141591543742200681048157739841$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 196247921687598957140410980869699666757$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 317309477136620705606056831160026103897$
- $g = 562444475715082448379092521798958966 45$
- $y = 170200304479531378882949690346414070368$

Сообщение:

- $M = 147113284535067392446493556635696758277$

Подпись:

- $a = 190535152375170847811774713659605159 72$
- $b = 252643679555033700591094344927630439 67$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 911$
- $g = 319$
- $y = 331$

Сообщение:

- $M = 186$

Использовать следующий случайный параметр для создания подписи:

- $k = 33$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 12x - 10$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 9

1. (a) Расшифровать текст:

СРЕДИМОЕГОСЕМЕЙСТВНКНУНЕПОХОДПРИШЕЛКМОИМРОДИТЕЛМИПОТОГДШНЕМУОБЫК
НОВЕНИЮПОКЛОНИЛСИМВНОГИПРОСИХБЛГОСЛОВЕНИНБРКСМРЬЕЙИВНОВНОЙСТРИКИ
МЕНПОДНЛИИВРДОСТНЫХСЛЕЗХИЗЪВИЛИСВОЕСОГЛСИЕПРИВЕЛКНИММРЬЮИВНОВНУБ
ЛЕДНУЮИТРЕПЕЩУЩУЮНСБЛГОСЛОВИЛИЧТОЧУВСТВОВЛТОГОНЕСТНУОПИСЫВТЬКТОБ
ЫВЛВМОЕМПОЛОЖЕНИИТОТИБЕЗТОГОМЕНПОЙМЕТКТОНЕБЫВЛОТОМТОЛЬКОМОГУПОЖЛ
ЕТЬИСОВЕТОВТЬПОКЕЩЕВРЕМНЕУШЛОВЛЮБИТЬСИПОЛУЧИТЬОТРОДИТЕЛЕЙБЛГОСЛО
ВЕНИЕНДРУГОЙДЕНЬПОЛКСОБРЛСГРИНЕВРСПРОСТИЛССНШИМСЕМЕЙСТВОМВСЕМЫБЫ
ЛИУВЕРЕНЫЧТОВОЕННЫЕДЕЙСТВИСКОРОБУДУТПРЕКРЩЕНЫЧЕРЕЗМЕСЦНДЕЛСБЫТЬС
УПРУГОММРЬИВНОВНПРОЩСЬСОМНОЮПОЦЛОВЛМЕНПРИВСЕХСЕЛВЕРЬХОМСВЕЛЬИЧОП
ТЬЗМНОЮПОСЛЕДОВЛИПОЛКУШЕЛДОЛГОСМОТРЕЛИЗДЛИНСЕЛЬСКИЙДОМОПТЬМНОЮПО
КИДЕМЫЙМРЧНОЕПРЕДЧУВСТВИЕТРЕВОЖИЛОМЕНКТОТОМНЕШЕПТЛЧТОНЕВСЕНЕСЧСТ
ИДЛМЕНМИНОВЛИСЬСЕРДЦЕЧУЛОНОВУЮБУРЮНЕСТНУОПИСЫВТЬНШЕГОПОХОДИОКОНЧ
НИПУГЧЕВСКОЙВОЙНЫМЫПРОХОДИЛИЧЕРЕЗСЕЛЕНИРЗОРЕННЫЕПУГЧЕВЫМИПОНЕВОЛ
ЕОТБИРЛИУБЕДНЫХЖИТЕЛЕЙТОЧТООСТВЛЕНОБЫЛОИМРЗБОЙНИКМИОНИНЕЗНЛИКОМУ
ПОВИНОВТЬСПРВЛЕНИЕБЫЛОВСЮДУПРЕКРЩЕНОПОМЕЩИКИУКРЫВЛИСЬПОЛЕСМШЙКИР
ЗБОЙНИКОВЗЛОДЕЙСТВОВЛИПОВСЮДУНЧЛЬНИКИОТДЕЛЬНЫХОТРДОВПОСЛННЫХВПОГ
ОНЮЗПУГЧЕВЫМТОГДУЖЕБЕГУЩИМКСТРХНИСМОВЛСТНОНКЗЫВЛИВИНОВТЫХИБЕЗВИН
НЫХСОСТОНИЕВСЕГОКРГДЕСВИРЕПСТВОВЛПОЖРБЫЛОУЖСНОНЕПРИВЕДИБОГВИДЕТЬ
РУССКИЙБУНТБЕССМЫСЛЕННЫЙИБЕСПОЩДНЫЙТЕКОТОРЫЕЗМЫШЛЮТУНСНЕВОЗМОЖНЫ
ЕПЕРЕВОРОТЫИЛИМОЛОДЫИНЕЗНЮТНШЕГОНРОДИЛИУЖЛЮДИЖЕСТОКОСЕРДЫЕКОИМЧУ
ЖГОЛОВУШКПОЛУШКДИСВОШЕЙККОПЕЙКПУГЧЕВБЕЖЛПРЕСЛЕДУЕМЫЙИВИВМИХЕЛЬСО
НОМВСКОРЕУЗНЛИМЫОСОВЕРШЕННОМЕГОРЗБИТИИНКОНЕЦГРИНЕВПОЛУЧИЛОТСВОЕГ
ОГЕНЕРЛИЗВЕСТИЕОПОИМКЕСМОЗВНЦВМЕСТЕИПОВЕЛЕНИЕОСТНОВИТЬСНКО

(b) Расшифровать текст:

ЬДЪОСПАЕПБГРЙВЩВЛЬЮЧАПЕСОГЫЖРФХНВЖСЯМЮЧЛЭЗЮВФЬЗВИИМОЬРЛЪСЯИНФБЗД
ОЩБЪРУЩЖЕНФГБЬЧСИСЕТРЯБШЫСУНВНЭЬЫИТИИСЬЛВЮНЮНЛАПЯЛОИМТЕЙУПЫИОЯУЯ
ЦЛБТЖОЧГТЖКОАПЕДФЬЕВНЛДСЕМОЭЪАВФАПЕШШЦКУПФЬМЕВЦГЫЖУЧГЙЯСРШКЬМЩЫО
ЯТУЙСТВОХЗПЬТЯКЕДФЪЦЬЛФУДБСКЯПЕГОДРЙЛЛЭТДЕКЯСЬБКЦПЭИРБТБИХБЛЬЕШМ
ЛЕЙЗГЭПКХБНЫОСЧКЕНФТПРСВЫНГНЛЮДЖЕЭЬЫИЧШЯСЬБЩАДБЛОУМПЕНЖНВУЧГЫЬНЛ
ГЪЖЕЦУЪАНЛГЪЖОЧЬДЫНОЪРЙЕЦАЗЙСЧЬЭШИШВЧЩБЦЩМВЕРВДАИИЮЪОВФГТЭПШМИЪО
КЫЙБНТАДЗЕИЦГЬННВЛЬРШЯТШИПВСЩОЗЯВЮНЛГЙБОПФПЬХЛФНЖОХДСВОУЩЖЩОСЩЧУ
ВОХДЙЬХЯДМЛНФНЗОКВНЫНОЭОЕРЩИЗБОТХБЮЛОВРЕБФПЧЖГОХЗДУКБТЪВКБТЪПББС
УЛЛЫРЬЙОУМТЧОШЙЕЛФЬОЕРЩИЗБДЛКДЖРОХБКХЧУЗЫЕШЦКМЧШЯОЗИРЧДПЬКЦКЙЬУФ
ПЬХТВСЬРУЦСЩЭШДЛЯНЩГТЩОЮЦККРКЮЗБМФЬНЫОПЩРЙТУМИБЗРЭЙИИТМЦИКНЬДГУР
АЗЙНЮЯСЩЕКЩВЕФОЗДЗУРУПЙИЦДГЖОЭЩШЬССДЧХВЧЩКЯСЛФНЗОИЮНЙВЛИККРКЮЗБН
ЛАНГЕЧГЗЙЬСЩДЪОЗЬВЕРФХЗЬКОУМКПФЬДЭЕИДБЗЕЮНЛБСОЭЪОСРШКБПОГМПУХЯКЬ
ЖЛУЗЙКШЦРДОФЮЕЬМУЦЙКМОАНГНОГЦЙОТМДЪОУИКУНОЫЗЕТИЦГЯГФЕЗНЕЦЫЙЩШЛЩЛ
ЯОШИДИТИЯЛЕЙЗГЭПКХЦСЗНКБДЯЧФГБЬДОАДЙРУХПЬИЭЫРЬМЛЮТБУНЯБКОУЭНПЕУЮ
ЗБЛФЙГУСИЯЭЖУЧГЗВКФЭМЬВФФНЗОКЮТОТФЭЙИИТМЦЩСЛЬЗШЛЙЯОЕЛЩИМЕВЧЦРВВЩ
ТНЪУШЩФЕОШУДОЛРШЙЙОСНЙЕКХБКЖРФЖНЗОИАНЫРСВБШНЛВТИТОЮЫЬЙУЦВКЛОЮНАЗ
ЮЪЙКГФБЦЬЙИЯГТИИЮЗЪНШНЗОСРШКБПОГМПКЦЩБЕМЩВСЗИЭЫТЗЗЗЦПЯПЦЯФЕРФУРК
СШЩМУЕПЫСЕПЦУЙЙОИЩМЕВШХНШООЖЗДКМЩМКМРВЗГЫЭВСКППВДШЕЧТНЪОТАДЙРУХП
ЬИЭЭЙИИТМЦЕТИЦГЬТИВМЩШЩЫБЗТОБТЕТРЬМВСЩБГДИРАПЯВЛЬЛЬНИЩЖШУЧГНЩШЩП
МЩЫЧЯЙЕМЗЦПЬГЩБДБИУВЛЕМРБЭБРЛАНИТОАНВОИЩМЯЗЗМЖДТЗМКИЕТНДХСЛЭДДКЩ
ШНЩДЦДВКЮФГБЬЛОЭМЬОУВНИТФЬЗЮОКЮНАГФБМЯЦБХНЩОСНМЕОХБСДОПБЖЫЕСЦМДО
ПЮГЩ

2. Разложить на множители числа:

(a) 563592158440405009339227773003

(b) 10628731560975234808076878562885629909024121908877948829901 43

(c) 939102321133930212389132438162702263763336423537785634535373826879633322179510969426373377

(d) 215007618354194939321110372431560972555472455302542562867245579180568706067642884249400030464733060723536563773804285 7807

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 71842612461414773486690743567224669092960028756245366570503184867461820208599$
- $e = 5$

Сообщение:

- $M = 49888134175732737741620022024467213099113699625524150934717328211720248979321$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 230329640551253690256148279337329623787$
- $q = 254425218936394256468804660774645783167$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 5409094460948373546546276366287509231597841384456510409322180511545025736541 5$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 27350617928138964168375343634284347257 3$
- $e = 5$

Зашифрованное сообщение:

- $c = 10375956627388871591755293101254903503 4$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 23200233805652950539824542678837042672 1$
   - $g = 13649131161116145556176056005527788355$
   - $y = 32282146300697704035422283043686621649$

   Секретный ключ:
   - $x = 28177272201753873731508171593086293170$

   Сообщение:
   - $M = 11393171977039739165500029619132615375 5$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 11670383485844760897522175590863265617 7$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 33259322836770109728670947715602844648 9$
   - $g = 47779720308756840287889558842147640 10$
   - $y = 21511134178451741027387930108752947537 3$

   Сообщение:
   - $M = 22963686912412866708635962716193094953 0$

   Подпись:
   - $a = 32143040090175736124181228915932519142 4$
   - $b = 16318104524695030268956727273160729426$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 953$
   - $g = 563$
   - $y = 927$

   Сообщение:
   - $M = 909$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 757$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 3x - 11$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 10

1. (a) Расшифровать текст:

ВЪВЬЫШЙЕЖЮШДЪАФШДИИЫЧЫЮЬЫШЙЕЖЮГЫНЫЩДЗАЭИТЪДЧЖЙГЗИШЮБЗДЧНЮЯЗСГЮГЙ
ЬГДЧСБДГГЮВИТШЪЪТАЮЧЗЙЖВГААЧЙЪИДЙЧЖЮГГЫЗИБДЮЗШДЮЛБФЪЫЯВГЫЧСБДЗИС
ЪГДДИШЫЖГЙБЗЮЗАЭБЫВЙЕДЪЮШДГЗШЫБТЮННФГЫЛДНЙГДЗШЫБТЮНВЙЪЖЫГДЧСБДЙГ
ИТАДЩЪЧСШБДЕЖЮВЫИЗЭЕЖДЕДШЫЪТШДИШЮЪЮОТБЮЕЫИЖГЪЖЫЮНААДШДЕДЪЩЙБЮШИТ
ЮЩДБДШАЫИДИЬЫБДЮАЙОИТИДГЫЛДНЫИЗНЫБДШЫАЕТФПЮЯГЮГНИДГЫЩДЪЫГШСЕЫЯАД
ЩЙЖЫНГДЩДЖЗЗДБЙЗВЫЪДВШЗЫЩДЧСБЙНОЫДЕДЛВЫБЮИТЗЕДБЗИАГНЮАДВГЗИДЯАЮГ
ЫЕЖЮАЬЫОТБЮШУИДШЖЫВВБТНЮАШДОЫБЮЕДЪБВГЫЭЕЮЗАЙДИЮЮЭЙЖЮГЖЭШЫЖГЙБЫЫЮ
ЕЖДНЫБЗБЫЪЙФПЮЫЗИЖДАЮБФЧЫЭГСЯЕЫИЖГЪЖЫШЮНЕДЬБЙЯЗИЕЖЮОБЮВГЫЗВДЮВВ
БТНЮАДВЗИДЖЙЧБЫЯАДИДЖСЫИСВГЫШНЫЖЕЖДЮЩЖБВГЫАЖЯГГЙЬЪШЪЫГТЩЛЩДИДШСЯ
АДЙЗБЙЩВЮШГЭЙЖЮГЪЫБИТЧСБДГЫНЫЩДШЭБГЗЫЧШЮЪЖШГДЪЙОГСЯЮДЧЖИЗТАЗШЫБТ
ЮНЙАДИДЖСЯЧСБЮЪЫГЫЩЮЧЫБТЮЪЫБВДЮЛЖНЮИЫБТЕЖЮАЭБДИЪИТВБТНЮАЙЗИДЖЙЧБ

ЫЯААЭНЫВЗЕЖДЗЮБЮЭЙВБЫГГСЯЗШЫБТЮНЮЛЫВЙЪДБЬЫГДИШЫНБЗДШЗЫШДЭВДЬГДЯЛ
ДБДЪГДЗИЮФЪДБЬЫГШДЭЖЭЮБЗШЫБТЮННЗДИНЗЙЕЖЮШЫЪЫГГСЯШЧДБТОЫЫЮЭЙВБЫГЮ
ЫЪАДЩЪЬЫЗЙЪЖТЙЗЕЫБИСЫВЙЭЪДБЬИТЪЫБДНИДИДГЫБЪГДШДБИШДЗЙЪЖТЪЫГЫЩГЫШ
СЪВЕДЪЙВБНИДЫЗБЮШЗЮФЖЫОЮИЫБТГЙФВЮГЙИЙГЫЕЫЖЫЗЕДЖФЙЕЖВДЩДЗИЖЮАИДЙЬ
ШЕДЗБЫЪЗИШЮЮШЖЫВЫГЮИЖЙЪГДВГЫЧЙЪЫИДЗШДЧДЪЮИТЗДИЫЩДДЕЫАЮЮШЭЩБГЙШГГ
ЫЩДЩДЖЪДЗАЭБИШДЯЩДЗЕДЪЮГИСВДЯЗБЙЩЪЫГТЩЮВДЮЮЛЕЖДЮЩЖБЕДИДВЙНИДИАВГ
ЫШЭЪЙВБДЗТИЫЧЫЗДШЫИЙФГЫЙВГЮНИТЮЪЫБИТИДНИДИЫЧЫЕЖЮАЭСШФИЗШЫБТЮНИАЧ
СБЕДЖЬЫГВДЮВЮЗБДШВЮНИДЗЕБЫЗГЙБЖЙАВЮЮДЗИДБЧЫГЫБНИДЬЫИСЗИДЮОТЭАЖЮН
БЗЫЖЪЮИДЗШЫБТЮНЭЕБАБЧИФОАЕЫИЖГЪЖЫЮНЕЖДЮЭГЫЗДГЪЖДЬПЮВЩДБДЗДВГЫЙВД
ЖЮВЫГЗЕЫНБЮЗШЫИИСВДЯЕДЗБЙОЯВЫГЗИЖЮАГЕЮОЮУИДВЙЖЭЧДЯГЮАЙНИДИСЕДОЙИ
ЮБНИДЙГЗЮЪЫГЫЩИДИАЮЛГЫШДЪЮИЗЗИД

(b) Расшифровать текст:

ПГДНАРНШБЬЕИЯЯЭНОЗИЬЛКВЛЭНЪЛДЩКМГЌЩЛТЩЭЪЕУЩЙЭОЩЯНЮНПЕЮЭВУБИФНМБД
ЧЗСЦИВАХШЙЭОСЫЗЧЯФЬЯЬПГЬУУВТЭОФЗСДГВЙМЩОФБОЛБЫГМАЙФПЪЖЭКПГЕЮЧБМЖ
БЪВУЮЖЩЛРЕОБЕТТАЧБМДПБОЮЖКЦКМЦДУИГНДЬОУЩЪАМЧВНЧПГЕЗСЮХЧПДЛЛЬЗЮЛЛ
МЮФБПГКУПЪДЖВЯШЩЯЭКШАКБНМЯНЩЛМЮЖАПТЬГЙОФЖШФЙЪШКЪГФВНБЩШЩЖВКЛБОЬЛ
ПЦЙЧАФЖШЧФФЬЖЩКМАКТЙМБЛЭКЩРЮЭИЙМНЩДТВЙШЛТЬПХЙФЩДСЙММОЛОЙСОЭБМЯКБ
ЗЧЫЮФМХЭОЧЗПЦЙВЗЪЫИЧФЪШАЭКМЕОЧВУЗЛЭБХЯЯВОТЗВРШЮЖКССХДОФУПЬПЫШЯЯБ
БООЯКУВРЕОСЕМГМЭППЦЙЭВСЫБЬКХАПЧКЩЩМФОЪББРИКВПТЛЛБКЪЕИЗАФПКВНЮЛЛЬ
ЙВЗХАБЬБФЖПЮНПБОЛКЛЯБХЦПЩИФНВЬНЮРКЯНЧОЩЯЛЯЛШЬОЛЕЙБДТКЩРДЖКПЛБТЛФ
ЩНЩДВЦОЛЗХАБЬБФЖПЬОПЯПФАХЗЯЭЯХДДЪЛФШЗЫКМЕЗЭЯХЬМФХПЯНЭПФЩЯЭЛЩЕОВМ
ПЖШАЯМЛБЯМЧВЮФИЦВКРШСБКСВФЬЪАЯХЩИВРСВИФКЛБОАПЧЯНЩДЩРНСВШЩЗКЙПДЮЬ
ЛЛЗФЬШУШЭККМГЌУПГБДЩЗХЧКЮЛЛВГЯВФЬДЧДИЩЯЬРЩРАЭЗЪЛЙКТЙВЛЯЛШВЮЬЛЦДД
ЦКЕЕШЬВПАБЪПХЧКДИЛБКЩНХЦДЩЛЩВМКЙЬЦЗБОЦВУБЕЙЕБТБЩЩЖЭПХДЧФКЬВАЧИПЕ
ШСЙХЩИЮЛТВВФКПЬЮМПХЖЮФФМДМАМХЯКХВФХЧЪЗФЩВЬЛШЖДЧЗЪАДЪВФЬЪЫНГЬЮЬЛЙ
БЙЯЯПЯНЛЙФЩЭЭИМЩКРШСБКСВФБКТЛУПНЪЩЮЖКЫЛНЩОРШЩРЮЧГЪЩБСМХЕЗФБФЬЕЯД
ЦДДУЯТЩЕСЙХЬСТИОЙУБЛЩВОЯЛКЖБЪЩФВБЗЯИДДЬЯПЯНБРЩЪБЭПЙЩЗФАХЦНБЛЧВЙВ
ЕЪЦБУЛУЬЗФАХВНСЛМАМЦАХЦКЯВШЬЮЬЛУЬЯЬПГЬУФЙОЛБЫКУЕБЩРФШЙБШШЮГЪЛФАЙ
ФОЪЙКРВОБДДЛИВЕУВУЕИКРШЯКСЕТЬНЛБЧЖШАДШЮДЯБУЬУБЛФЙКУЕТЬНЛМХШЗФЗЧЩ
ЛЭОЩЬДСЕЩРНБРЛБАЯРКВЕУВФРЮАВЛРИЭЙЮЕПВПЧАЧЯДКВЮЯЕЙЯДЮЛЙЬАЧЙХАПБЗЛ
ДПХВТТЭЬЛЮЖКЧЯФЬЯЬПГЬУЭПЧШКАППГМЭЮХЯОЪОЛЦЙЭЮВЖЖАЗОЯКЬЙФЩНУЛЙВЗЛК
ВАЮЧБХАСВБХЭИЧНТЗУЗВЛВЭЯЛРЕНЭНВЬЙФФМЕОФКЩЮГУЛЧВЮЖПХЛОЭЕЙБДТКЩРДЖ
ОСЫЗЩЛУЩЙУКЩМЖЭПХДЮВАТЗЯУИЙЮМБШФЩЮАИЪМЗАЩПЦЙЧАФЖШЧФОАББЕЙЦКЫКМЫЙ
ЩЕФЩПУЛЙВЗЛОЩЦДЧЯШГЌКЫКШЦКФЛИЩХЬЕМЕИВППЯНЧКМЫЙЪФЩВКБ

2. Разложить на множители числа:

(a) 692717637101703873740655297689

(b) 1061981604983861579698763308455429175983675740969323555528019

(c) 11925213035731238957476922642411790088419942757840537304663528595097429339170879853630045 81

(d) 16368855576436052744910774711820841442392906506746430724205205650225871177368242770664343934526633803815303677461180073 83

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 485354484725359657906328505655227121735071178749206125845651058235632698521 83$
- $e = 3$

Сообщение:

- $M = 283284702927499237040737879126864084487553467085064031945490004010694160475 31$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 238378347408993523378647219090828818231$
- $q = 224780039665997667775079480877150702917$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 22267362399448479089229631381592908743793535710479763112870300922382304520014$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 152845640877643049171880219880974194803$
- $e = 3$

Зашифрованное сообщение:

- $c = 795149394624349559934341983503870837 89$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 221349489025153862640714032718193878373$
- $g = 189098095031590953456727557666998246378$
- $y = 184977152142091044562627753046778127193$

Секретный ключ:

- $x = 140520091929460125878706975642852534971$

Сообщение:

- $M = 421056795499597084359310300729255731 90$

Использовать следующий случайный параметр для создания подписи:

- $k = 41675854866384808888499736999937178363$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 28142111093673785761425576816339747 4103$
- $g = 91410182096897427182985280507671494927$
- $y = 51760290093303456265163511017241542044$

Сообщение:

- $M = 15205905211842802111951335000285338 7987$

Подпись:

- $a = 25633864673613599627611503190869129 2361$
- $b = 33490696787237071183305236855924926039$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 761$
- $g = 601$
- $y = 362$

Сообщение:

- $M = 277$

Использовать следующий случайный параметр для создания подписи:

- $k = 529$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 14x - 6$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 11

1. (a) Расшифровать текст:

ЦТНСТКМЦФУХНРНТКЦЧРЧУХИУЗЧБЦФУЦЗУКСШУЖАПТУЗКТНГНЗЬКХЭТНКФУЙУМХКТ
ННМИРЙНРНЦБЦУЗКХЭКТТУНМИУРУЗАКИУФУМЗРЗУЛЧУИУЖРИУЙХНРМУПМТТШГФУСУ
ЬБНЗКРКРЦЗКРБНЬШЙЧБКСШФУРЧНТШТЗУЙПШЦЗКРБНЬТЪСШХНРЦФУРЧНТШТЗУЙПШЦ
ПМРУТМЬЧУВЧУМЧУЬЧУЧАЛКНМЗУРНРФУЙЗКМЧНКИУПФУЦЧУРУСШЙЗУХШЗУРЧЗУЦШЙ
ХБТКЧШТЦРНЭТНЪФУРЧНТЗЦПУСШЙЗЧБТЗУЙПШЧПЦСУСШЦПУХУФХНЙКЧЦИУРУЙЧБТК
СУИЦФУХНЧБЦЦЗКРБНЬКСЙКТБИНФУСУКСШУЖКЮТНГТЪУЙНРНЦБЗФУРТУСКИУХЦФУХ
ЛКТННСТКЖАРУЙУЦЙТУУЙТПУЛЬЧУТКСУИУЧЖРИУЙХНЧБЬКРУЗКПЗАХШЬНЗЭКИУСКТ
КЦРНТКНМЖКЙАЧУФУПХОТКОСКХКНМУЬКТБТКФХНЧТУИУФУРУЛКТНЪУХУЭУЦПМРЪРЙ
ТУПХУЗТУКЦРНТКЪУЬКЭБЙЧБФУРЧНТШЧУЗАТБКСШЬЧУТНЖШЙБНМСУКИУФРЧБУТУЙК
ЧЦРНЭПУСРКИПУЙОКСШСУОМОЬНОЧШРШФФУСНРШОЖЧГЭПФКЧХТЙХКНЬЦПМРЦЗКРБНЬ
МЬКСКСШЧЗУОМОЬНОЧШРШФУТКИУФХУФБКЧЦУЖПЗФКХЗУСПЖПКВЧУЦЧХНТШЭПШЛТКЧ
ЗУФКЬРБЦПМРСУОЖХУЙИФХУФБГРННРНТКЧКИУЖРИУХУЙНКСТКЛРШКЧЭШЖШЦУЦЗУКИ
УФРКЬКИУТЧУЖХЦПЗУРЧЗУКЪУРУФБКЙКРУТКЦФУХНЧБНЦРШЭЧБЦЖУИЧАТКЖУНЭБЦХ
МЖУОТНПУЧЗКЬРКСШЦЗКРБНЬЦКХЙНЧАСИУРУЦУСЧАЗНЙНЭБЬЧУЙНЧКЮКТКЦСАЦРНЧ
ЧАНХЙКИУУЖУЖХЧБФХУЦЧУЧАКИУХЙНМЬКСЧКЖКЖХЦПНОЧШРШФЬНПЧАНТКТФРНЭБКИ
УТЦЗУНУПТТАКФРКЬНЮФХУЭШТКШСТНЬЧБЦПМРЦЗУКСШЙЙБПКЦКОЬЦТКЦНЦГЙЧШРШФ
ИУЦФУЙНЗРЙАПУФХУЦЧУТРСУОЦЗКРБНЬМОЬНОЧШРШФФУЬЧНТУЗКЭКТБПНОНЙУЖХУЖ
АПУСШЧУФБТНЫКУИУРКРУСШУЙТПУМОЬНОЧШРШФЗНРЦСШЛНЬУПЧШЧЛКЦЧРКИУФХНСК
ХНЗЧБЗЦСУСЙКРКЧШРШФНМПУЧУХУИУШЦФКРНЗАХУЦЧНЖАРТКСТУЛПУЙРТКИУШМУПУ
ЙТПУУТПУКППШСШЙХНРЦНТЙКРКИУХЦФУХУЗФУЭЗСЦЗКРБНЬЬШЧБТКМЗАРШЦРАЭЗПП
ТНЧПНМЧХКЮРНЖХУЙИЖАРЬХКМЗАЬОТУЙУЗУРКТСУНСФУЙХПУСУТФХУЗУЙНРСКТЙУП
НЖНЧПННЦПМРЦТНМПНСФУПРУТУСЦФЦНЖУЗЭКЖРИУХУЙНКТИХЙН

   (b) Расшифровать текст:

ЫЖААЯРЖЗЩЖПОАВОДТИЯЮЧПКДТОМЙЪТЧЙААЫПОАШЫХЗИВОЕМЙЬВЭЕГЦХЬЭИЬЪТНЛР
ХМОЙЦЪЧЖМЖЭХЙМРЮФСЦЦЯЖПНБХЯТЭВХБФЭЕЯМЙЗПФЪОАЩОЕМГЗУЭГАДТЧЬЭЬВЫПЮ
ЯЮТЙИЮЫЧЖСВСЧЗЯПАЬСЙАЮМЖЖРХБГЙМТХЛЙАЪПЕАДУМСОЮВЩЙМРЩШТРЦЯТМАЧЫЫУ
ЛЩЬПУЙАСЪЖМХИХОКЬЮЧСОЮЫИВНТЕФЙШЖЫЩСГЗРШУЙЦХХПЗЩЪФШАААЬПЭЪЪШНОЬОШ
ПЬПЧЧПЭЩЪЧПКЬЮЖНКЬЮХЛЙАЪПННЗЕФПИЦЧШОСЩЬЪЙКЬЮЕГЖБТЫЛЙЯЙФПМЖЭШЛЯВШ
НПИЩЭЫРАЛЯЕГЖГЧПУГГТЪЖТЬЯЕГЖЖЫЪЗАЕЯМЖИБАИОЯГХЫЭМПЪЭНЙЩЩЭРАЖЭЭОЯД
ТПГГЛАНСГБТМФЭВЭПОЬЗЭНТЕЗЛНФЬЩЭЧЙЩЦОПМЙЧЫЪТЕЗЛФСАГЫЫУЧЕЯЪММГЫЩПТ
ЩЭФФОЧСЬЭЛЕЬШМЙЪТЧЙАШАЯГЕВЯШСЙАЬТТИВОЕМЙГХЫЭЗВЪФПИЩГЪЖУЬШЫЖЮВЭЫР
АЛЯЬЭГЕЬПСЭПВЫУЛВЧЭГГШТХШНВПЫЖЯЩШШРЙМШШЛТВЭЬФМВСПСББХПРГЕЙЦВЦЯЫЫ
МАШАИЪАЩЮЕОЗВЦЩЖНДЬТТЧАЫЬГЙЩПФПНВЭШНКДЫЫЙУРЯЕОМВЭШЕГЖТХЭМЮЫЦОУЩЩ
ЛМЮВЮХПЭЩЪТЙГЕЫНММЬХЧВЛЮЮЦСЧЩЦТГИВПЧПДШЫБЖЛРЛЦЙЛВЪШГЙЭЩЕРЙЯАБЙЖЬ
РШТАЧЫЦЖМКХЧЖНВШЖЛЙБХЦПАЧЫЛМЮВЮХПЭЩЪТОГАЫПДЙЕЫНММЬСЬЭНЩОПОАБЩПСА
БЪШЖФЩХЫПЬЬЭИТЧШЫЬЖЬШЫЛСНРЮОИКДЫФИЦЖПШЙКДЫЭШГЖЙЬЖЬГАЬЖЗЮЧЦМЧЛХВЛ
ОБТЫНЙЖЭЧУЭВЦШХГКТЪТЕВЦБЙИЬОШУЦШЫФИЖЛЯШЩКЧАЧПМЬЯЖЖФЩЪПЕЙЕЯШЙИЮЫЬ
ПЛГЫРМЙЦЪЬЖЬЩЪСЪГЖАШУАЛТЫУЭБТОМЯЗТХЖДЕЯФЙЗЬУПТЙДПЧЧЗЬЧФПЭЖИЫНИЩЩ
ПЕЖЩЪЧПЬЗСЭРГЕЯЖЛИШЭПЯЕДШШГГЛАЩСЙЕТНПКЩЭПГАЕЯТУАХХСВАЯЫНПЛЕЧШКЕД
ТЩПМЖХФФЯБХЛФЯРЬШЕЖРЕПДЯЩОЕЕОДЙЭУАХЬЪПУЯЩЬФУЮЯМПОЫЪМПНЦЫПНКВТОЙИ
ЮТТПНВЩБУЙЖИЪОАБЮНПЛЩЮЬЙВБТЦПЮЯХЬЖКЩЭЖМАЪХЬШНВХСУАХОЭЕАЖЩШМЩХЫНШ
НВОЬЬГЕЬЪГГЯЮЯПНРХЧЖМАТИОЯЩЯЖТИЩРШГАЯХФФЩАХХПМЖЙШУАКЯМПДЧДЬЖИЬТЫ
ЖЮВЬТТЧАПШИЬЗСТМЙЦЫЦОАДФЧЬАЛАМТНЦЫМОГЪТЫУЙЮХПГЦДУПОГБЧШУЙДИПВНТЕ
ФОАГЫЫЛОГХХТЮЯАЛПЕВЫЫЛЙДОТМГАТЧРЛЩЪПВЛЩУПОГЩЮФЛГАЫЧФКВЩТОЖВЩЪЭГЬ
ПЧПЭБТФИЖВЮЖНИЩЮЬПЖРУПОАГЭТТНВЦЧЬЗЮЧТОАЕЬЪГАШШТГЦАЩЕТЖРЫЩЖЛЩППЕА
БХТНЙЩЩТИЬЩШШДЙДЮФПДЮЭПРЙЕЯТНАБАРТЖБЫ

2. Разложить на множители числа:

   (a) 52463922104196397092258058507 7

   (b) 59148378364242191235230715286365742173239320071413919888070 1

   (c) 10206565186669700309708311019835850165536998353368477103547689664188018358640628631800656 31

   (d) 19643754047700402578163332436492503756096641108494305568815780672433551895955727957830434894258147133112084393076231566 11

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 504256733115879496870016793589704617746308445817425009048450103588516416817 39$

- $e = 5$

Сообщение:

- $M = 387964441294380829464233385685282180674047493696217997852390227952014421553 88$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 31587791918735639545888554360524625 9211$
- $q = 23546322337690483101358418418134178 2971$

Открытая экспонента:

- $e = 257$

Зашифрованное сообщение:

- $c = 32515783527322449141688099796442873097045272392268264923817031018314322318339$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 15819984077630218217221843870689578 9831$
- $e = 5$

Зашифрованное сообщение:

- $c = 98411783209633010178777885827996122845$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 33449798536396577151653352721646142 7681$
- $g = 74424963087808107993590401285509865255$
- $y = 23871305732609796980431051157213819 9203$

Секретный ключ:

- $x = 29058082038522387721098618646194060 6747$

Сообщение:

- $M = 12560249487528972705514683950682358 6909$

Использовать следующий случайный параметр для создания подписи:

- $k = 26928683393433296748896018815006834 6423$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 29568052050958337807191066363297084 0939$
- $g = 15517907648287616661618269610064053 3295$
- $y = 21832076161922836525208421214433297 1942$

Сообщение:

- $M = 13103457478517509359344368561054814930$

Подпись:

- $a = 67992260974130993705166465362768409884$
- $b = 14667955020900236572443024049280450 1458$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 937$
- $g = 768$
- $y = 865$

Сообщение:

- $M = 575$

Использовать следующий случайный параметр для создания подписи:

- $k = 491$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 13x - 17$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 12

1. (a) Расшифровать текст:

ЩЭТЭРБНЗЩБКЧЦСЭЪЧЪМБЭАЪКЗБЛАЮЯЭАЧЪЧСЬЩВЦЫЧЖЫЬФБЩАЩЦКСЪЧСЭЯФЬРВЯТ
ФЭБСФЖЪЮВАБЩЧАЩЦЪЩЭЫФЬУЬБВЬАУСЬЭЬЧЖФТЭЬФАЪКДБЛРЗЩЧЯЕКЬЯЭУЬЮВТЬЬК
ШУЧЩЧЯТЧЦЕКЮЯЭВЖФЬКЬФРЭАЛЬЬАЬФАВЬВБАЬАВЬВБАБЩБЩВНЦУЫЭАБЯАБЩВЖБЭЪ
ФБЬУФАБЛВТЭЫЭЬНЧСЫЬФАБЯЗЬЭЮЯЭУЭЪХЪЭРЯИАЛЩЩЮЧБЬЗФЭАБСБЛАСЩЯФЮЭАБЧ
ЮЭУСФЯХФЬЬЭШБЩЧЫЭЮАЬЭАБЫЮЯЧСКЖЩЫЭШРБНЗЩЭБСФЖЪЭЬБЭЫВЪФБУСУЕБЛЩЩЬА
ЧЦЮЭЪЩЮФЯФСФЪЧАНУЧЬФЮЯЧСФУЧТЭАЮЭУЧЩЩРЭЪАЛЮЯЭЩЪБКДМБЧДЬФДЯЧАБФШЩЩ
ЦСЧХВРКСЪЭЯКАЛЧЗЮЩЧУЩЩЦАЪКЗВЧДСЧЦТСФЯЧЗЛЪЧЭБФЕЫЭШАФЯУЕФБЩЧЦЫЯФББ
ФЮФЯЛБЩЮЯЧСКЩЪЖБЭЧАЫФАБЬФБЯЭЬВАЛЩЩЮЯЧУВБЬЫАЩЦБЛЖБЭЦЪЭУФЧЭЩЭЪЭЩЯФ
ЮЭАБЧЯКИВБСАЧЪЧАФТЭЯЭСЬЮЯФДЯРЯУЫЦЫФБЧЪСХЬЭЗСРЯЧЬЧСЬЩВЦЫЧЖЫЭХФБМБ
ЭЦАСЧУФБФЪЛАБСЭСБЛУАЪКЗЛБКАЩЦЪЧСЬЩВЦЫЧЖРРБЭЬФЯЭРЩЭТЭУФАБЩЫЯЛЧСЬЭ
СЬАЮЯЭАЧЪБЩХФЪЧАЫФЪЩЩЧСКАЫФЪЬЧЫЗЭБСФЖЪФФЫБЛЬФБЫЗБЯВАЧДУЭАЧДЮЭЯЬФ
ЫЭХФБАЪКЗБЛСКАБЯФЪЧЦЯВХЛБЩЧЦБЯФЮФИФБАЩЩБЭЫВУСТЭУЧСЬЩВЦЫЧЖСКУВЫЪС
ЫЭЧЧЫФЬЧЬКЮЪЧБЛЧЦЬЗФШЮВЗЩЧБЩЭЬЫЭТЭЪВРВЗЩЖВБЛАЭАБЯДЬБЭБАСФБЬФЭБЮЯ
СЧЪАЛАБФДЮЭЯВХЧЬФЮЪЧЫЧЦЮЯЭЩЪБЭШЮВЗЩЧЫКСАБЪЧЧЦЭАБЭЪЩЮЧБЬАЩЮЧБЬЗФН
ЭБЮЯСЧЪЧАЛАЮБЛЮЭЗФЪЩЗСРЯЧЬВАЩЭБЭЯКЫЧЮЯЭСФЪЕФЪКШСФЖФЯТЪСЮЭФУЧЬЭЩЧ
ЬЧЦСЭЪЛЧАБЬЛХФСЮЭЦЧБВЯВЮЭАЫЭБЯЧЗЛЮЯЭЩЭЪНЩЩБСЭНГЧТВЯВЩЬХЬЧЬЮЯЭЗЪЭ
ЬФАЩЭЪЛЩЭЬФУФЪЛЧХЧЦЬЛЫЭСРФЪЭТЭЯАЩЭШЩЯФЮЭАБЧАУФЪЪАЛУЪЫФЬЬФБЭЪЛЩЭА
ЬЭАЬЭНЬЭУХФЧЮЯЧБЬЭНСУЭЫФЩЭЫФЬУЬБРКЪЮЯЧЬБЩЩЯЭУЬЭШЫВХЧХФЬРКЪЧЪНУЧА
ЫКФЮЭЖБФЬЬКФЧСЬЩВЦЫЧЖСКЗФУЗЧШСЭГЧЕФЯКЧЦАЭЪУБАЩЧДУФБФШРКЪЖФЪЭСФЩЬ
ФЭРЯЦЭСЬЬКШЧЮЯЭАБЭШЬЭАЫКШЖФАБЬКШ

   (b) Расшифровать текст:

ИШАШЗНСЧВКИЩАЕИВБЧАВДЙЮЮДОВЧАЮНИКЖАНЫШЧНТБЪАЙДЫЯЫИТАЪГЭИЭИШЬНДЯШ
НЖИАЫЬНАЕЪЖИНГЕЕБСАЕЖЕГДЫМЬИЬЫЯПЙГЕДИДЯЭЕИАЯЖЕИШЯЫЭНИОЫССИФШКДСЮ
АЖЕЖЧАВЕВФОЬЕЪДПИТГЧЦИТЯЯЖДОИАГЖУНЪЮЯЕЪЮДДОЫЭСЫОЕНЕЛТШАХЛИБЪДЯГД
ВБЬНЗЦШЕЛЫЮЖЗЕЗЬБЕЬААЪЖЕНЯЫГКЗДШЕЬГАИИЗЯГЕЬКАГЖЮИГЙЫЗЮПЪЬЛЛЫЦДМВ
ЮЧХИПЖАДЖИЕАДМОЖААЗИВЪЧЫЫЗБШКВЙГОЙИИОБЛТДВБАНДГЕЦОИФШМЧЮЬВИТДЮВИ
МДЭКЬНЫГЭИЛТЬБЖИГЕЕИНЩЭЖЫОААХБДДЗАНЛЮГЭБЛАЙЦИЛДФБШГДГВИДЮУБАЕВАЬ
ЬИООЭДИЫЯБЬОЗДЫСТДЪЪЧТДХБЫУЪЧЕВМИЕЛДОИФШСЛЮФАВГГДПВЧЧАЦЖИБАДМИШГ
БЕДИЕАЛДДФБЕЬГАВИРДЗЖЖНДХБЙУОЬЖЬЫНЪДМИБФБЛЬЪЦЫЖОИББКПЙХКЯВЙХБЛПД
ЦПЗЕШНЧЛТЗФЫЗЬГЧДФЕЗДКМОЭЙШЕОШЧЭЧТДДВНГНЧХЛПЖАДВЛАААЯНЪЯЕТТЙДЫЬН
ЮХАМЬЮЙЪЖЕИЪЮСТДБГИГДФБКИБГЫБКЙГЫЕЗСЬАИУЬЧФХЛДБББДГАХЛИБЪДЯГДВБЬ
НЕВЫЗУЪЪЮЯГДФБЬСЫЮВКИЭЯЕЦСЪФШЖУЗЭБЬОГЧГЛСАЩОЬТТАЕИМГЪЭИМЙФДВЛЮГШ
ЭОЖАХЗСЪЧГАЛЗФБЯОЧЧМЗИЫЪАВКДЮЖЗЕЗЬЪЕНЮАЧЗОЩАДЕОШЬГИМЫЬЭЙОЕЦПВИИА
ВИТДЮЖМОБОЭИЧИАЭИРДФШЯХДЦЫЕЕПЧХЛТЫБЫВМДХЮЫЫИОЪПВНЧАБЛДЦШЖИШГЭИРЫ
ФДЯЗЩАХИРЮЭЫИПЙХКЯВЫДБЕКЮУОЕИЖЩЮВЧГНЭИМЫЯЧЗТЕАДЕЛЙВЧЗИАГВИРЙЙШЗИ
ЫЮГБВЫЦЕЦХДВБТЕГОЭИОЧАХЛЕВББЛОЗЧЧЗИВГШЕЕГЪЯВКЖЧВИСИЮЖКДГЪЭЬОЭФГМ
ИБГКЯРЫЩЧЬДГЪБЫЪШЪЮСТДФДМЕЕЪХЯРЗДЪТЕЗДПЮЕЗДБМКЖЧВИСИЪХВДЫЭБЗМГАЩ
ЯСИФБИГГЧЬВСБНЛЕОИУЛДИЖИШЬЧИАЫЮЕИЯШЬЕЪАЯЛИБФВКОНЧЯЗЕВАЦИНЗЬЪМЬГЪ
КЯГДББЕОЬЪЕЯЛТЯБЭОЕАЕИМЙЙЕИЕЛДПЮЛТКШЙОЧАЮЛВАВШЙОЗДЫЖЕЬЦЖДЗАЮЫБМЫ
ДАИСИЭБЗЕДУОДНДФШЗНДЧХИЛГЧАВЕШАХЛЕЛЕЮВЦЛААВТДЭВВЛЮГПЬКЙЙЭВТЮЗБКЗ
ЩАХКИШЭЫЖЕЬЦЖЛОЧАСВРЗЗБЮИБЪДЦУШЪЧЮРЩЕАВЛЮХГЗИЭААЗОЩАДИЛЪДВИДДГЮЗ
ЫЧНЮВКГЪЯЕЗЙДКВКЮРЮГКЖЧМЯНСЫЭЕМСЬДЮЕБЭЭИМЫЯЧЗТЙФЩЗОЫЦБЗЕЗЧАВЕЕАЭ
БНЮЕГЮНЮЬВИСБАХЖЮБУОЕИБАЩЗЫЕАХИЗШВМЯНЮЪДЬОЫЮЮНКШНЬДЗААФФВЮЭДЬОЮЮ
ЕИВЖЪМЖЧИАБЗБСЭЖЫУГДБЬЩЮЬБЬПЖЧЧЛТШЭЮЛ

2. Разложить на множители числа:

   (a) 61240607740370395688432764813 3

   (b) 834900769620821024142291688228270935105634754577326449318723

   (c) 906845650555379539065031399982936321509260876117118331704906177515564467033580360686087861

   (d) 1349153092004285285800417913147117935049905821132174274799020510421426493499417407004630473958647146206186814860253765309

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 81518796910088554951667868130919873935414314196688766953742229607143369486813$
   - $e = 3$

   Сообщение:

   - $M = 403921476734447166060016374404247504194881207657087979621272500940358782681 59$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 32982801016221719896047014909603076 1067$
   - $q = 22808184874218251313031381302178627 6063$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 74201359024768469949632145582536689533544697307305928658320529028426461353874$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 11250882728363713683195866771943602347 9$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 31980979761335591261319438164140297636$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 18728426699314174003589473766984587 4959$
   - $g = 15872373593195951504212976510291549 3802$
   - $y = 12477082781677863149791408413046928 8417$

   Секретный ключ:

   - $x = 15150330775581609033878866148001217 6907$

   Сообщение:

   - $M = 59247975859410364148092901477933932723$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 51556572547120959921523990555793012713$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 26356614031528301174274855987115022 5309$
   - $g = 93813157880267177420421270672766317335$
   - $y = 12314683835308267918434010681194970 4450$

   Сообщение:

   - $M = 25382221743757781481392487991292593 9165$

   Подпись:

   - $a = 22516244456713181916183817209971167 8427$
   - $b = 88417218354813123853580329122194493240$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 911$
- $g = 117$
- $y = 874$

Сообщение:

- $M = 244$

Использовать следующий случайный параметр для создания подписи:

- $k = 201$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 14$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 13

1. (a) Расшифровать текст:

ЫЧАЫЫЯОГДДЕЮЫДПЭЭАЫХКШЯАШФОХЮЫХБЪХГЕДПЭЭБЯШАЧАЕЖВББФОЭАБХШАЫСДХБ
ШЯЖВБЧДШЮЭЯГПШЫХАБХАШЫХАЭЖЪЯЫКАШФОЮБЧБЯХДЫЮЫДШЦБГБХАЪАЕФОЮИБЪЬДЕ
ХБЯЯОГЪЦБХГЫХЮЫХВБЮЦБЮБДЯГПЫХАБХАДАШЩАБДЕЫСХОЦБХГЫХЮЯАШЪФШДВБЭБЬ
ДЕХБВГЫКЫАШААБШХДШЯЯБШСДДБГБСДЛХФГЫАОЯЕЭЫБФЯШГЮДЭЪЮБАЭБЦЧДЭЪЮЫАЯ
КЕБХОАЯШГШАОФЫЕПДАЛВЦИЭЭЯЖЩКЫАОДЕГААОЪБЧАБДЮБХББЭБЕБГБЯКШГШЪАШЧШ
ЮСХШГАБФБАЫВБЪФОЮЫБАЫЦБЕБХОГШЪЕПДЫЩШГЕХБХЕПАШЕБЮПЭБЩЫЪАЫСАБЫДБХШ
ДЕЫСЫФЮЦБВБЮЖКЫШЯЕШИЭБЕБГОШАБЖХШГШАКЕБАШХОЪКЫАМЫЭДДБГОХШГАБХЫАБХ
ЕЮШЭДШЬЫХАОКВБКШЯЖЩШХОЕЭЧЖЯШЕШЯГПЫХАБХАЧЕЭБАЕЭБЬАДЯШЛАЫЭАШЮСФЮСЮ
ШЭДШЫХАОКБАБКШАПЯАШВГБЕЫХШАДЕГААБАЫЪКЕБФАШИБЕШЮКЕБФЫШЯЖЕЭЩШАШАГХ
ЫЮДПРЕБЯШАФШДВБЭБЫЮБФОДЕГИЭЭХОЧЖЯШЕШЯГПЫХАБХААГХЫЕШДПЮЫХОШЯЖЫЮЫА
ШЕЯГПЫХАБХАЪЫЭАЖЮДПЫВБЭГДАШЮЯАШЭЩШЕДДЭЪЮБАЧЖЯСКЕБАГХЮСДПВБКШЯЖЩШ
ХЯЕЭЭЩШЕДВБЕБЯЖКЕББАЪЯШАДХЕЮДДХЕЮДБАЪХДДХЕЮДЭБЦЧЩШХВГБЛЮБЯЦБЧЖЯШ
ДЙЧХЧБХЛШЦБВГЫШЪЧЫХОАШВБЛЮЫЭЭЫЪХБЮЫЕШХЫЧШЕПЮШЭДШЬЫХАОКЭБАШКАБКШЮ
БХШЭЖЯАОЬЫИБГБЛШЬЗЯЫЮЫЫЫЯШШЕДБДЕБАЫШАБЭЭВБЧЖЯСКЕБАЧБФАБФЖЧШЕВБЧ
ХШАЙБЯВГЫХДШИДАЫЯВБЙЮБХЕПДАЫЪКЕБАЫЪЭЭЫШФЮЦБВБЮЖКЫДЮБХЯГПЫЫХАБХАО
БЕЭГОЮЫЯАШЦЮЪЫБФНДАЫЮЫЯАШЯАБЦБШВБАЮЖВБГАБШЪЮБГШКЫШЭБЕБГОЯЛХФГЫАШ
ШВГШДЮШЧБХЮХШГБЕАБЪЯШКЮБААЛЖХЪЫЯАЖСДЭЮБААБДЕПЫДЕГЮДБЕХЮШКПАДЧГЖЦ
БЕЧГЖЦДЮБХВБЧХЛЫШВБХБЧЭАЛШЬДДБГШВБЭЪЮЫДПЯАШШМШФБЮШШЦАЖДАОЯЫЭБЦЧХ
ЯШДЕБЦГЖФБЬЫАШВГЫДЕБЬАБЬАДЯШЛЭЫЖХЫЧШЮХАЫИБФЧЖЯААЖСЭЮШХШЕЖЩШЮАЫША
ЭЪЕПЧШГЪЭБЦБЪЮБЪОКАЫЭДЧШЮЮБДПХБЯАШШМШДЫЮПАШШЫДАШЕШГВШАЫШЯДЕЮБЩЫЧ
ЕПЖЧБФАБЦБДЮЖКЧБЩЫЧЮДАШЧБЮЦБАЧГЖЦББЧШАПЭБЦЧДЫЧШЮЪРЮШЦЫШЬ

(b) Расшифровать текст:

ОЮРВХЧФТЭФЯФЕГЪДЪИАХЭВОЩУЭХГЯЛЩЧМГЪДЪУФХЭГДБВЩОИХХЦЦЕЭЙЭХМДШОХТД
ЮЮЮММТКФИТЧОЛЕЩЦЬШСЧФЗХСЯТРВЫФЧЪЬКЯПУКВЩТФГСЦЧРШЕЙЙНАИЮШЮЮЛАХРЫЕ
ЭМЩШПБПЭВЛНФЪУЛХМЧЭНЦЦЬШТЦТЧОДЩЧУКЕШНКЙИЦЙЭВЕАПУЬЕГЛОШЖЦФФХВЫЧСЯ
ОВЩФБЪЦЬЧШСНЙЦГЧЫЪФБТЬПШХЖХЪЭЮБЯЕЮЮЛЫХОВЬЫХШХНХФЮТЕЬМЧШВЮЪФУНГГФ
ЗУЮЙСБТЩЦЯИКДФФЕТЯТЫГИВУЫАИВЩОШЛЕПЮШЛНЛЬЮЗЧЪТЦЛЯПЫАОЬМЮХЛЯФРЭИЭП
ЩХСХМЧТНЩСЦЮГЯЙЬХДЮМУФНЩСФАСВМЭМТЯЩГБУВСЦЫИЩООШДДПЭВЕАГЪЯУВЩСЫТД
ЩОШЛВГЩТЛДЙЭШЛЩШСУОБХОЭИВФСОМЙФСЕОГМОИОГШЮВЬЯЩЩХЕЮЪГВОВСУЫКЯУСЭД
ЮЩДЪКЯЙЪШДЦЩНВЛНКРХЖЦФСЯРЩЦСЫЬЮМЫАИГМЧМНЦЛЧХЧЦХЮТЕИТФТНЫЪУЬИИИЪУ
ДВЩОБЕТЪРХТЬЛЩЮЧГХШИСГЧДЭОГМНХНЦЩЫЯЕЮГЦЮТУМГЫМБГФТНЯЙЩФОЭХРЭОЪШЮ
АШЮМСВУГХЩТЗФТЩГЛЮУСЭИВЪЭШЛЩМШГЛМИЩГЛВГЩХВЯТИЭОВЩФБНДТЬГКЯЩИЬОЦР
ДЯГЩЙЭЯОЭФГВОЮСЩГНЦЦЪЫУИПЧХЕЩОСХРДСЦЪБМФУЙИГЪШЮЕЪТКСЕШФЪЩСЦЧРЖЕЭ
ХСУОБМЧЮВЯХНАЖЬШССЕЦЧЗЖРЦУТЦДЬЛЪЪЗГГГВОТВЧФОВЩЪШНЦМРЮВЦЧСЭНЯШЮШИ
ВФСВЕБЦСЭИЦУЭВЛЯНФФТНЧСИИГМЧМНЯРШШНДЩЗТЭГХОАЕЭПУЧВМШЪВЫЮЬЪФИУЯСЩ

СУЦЪЫВЦЧЭВЕЯЩЦАЕАХЭВИАХЦЧЛЩШИЭОУВСЪОЮФЗХТЯТЫЛИУШЦЮРЦШЮХПНЪЭХЛВГШ
ЭОЧМЭВВЯУЧОДЦРОЮОБЪТХНЮВБЪОАГШШИВРРЪМЩУСЦДДПШШНТМЧЮМЫХЩХЕЖТГХЛЯЙ
СЪВЫЧЭЭОЭСАВНЦШЪСНЧМЩЭОЪШНЫЕПЙЬГКЦДЮЮБМТЭЬПДКГХВЯФЪБТЮХОШЛВМПЮОЫ
ЧЯЦИЬПФЪКУПРЭОАХСУОАХОХЛЦФФОЧЦЩЗАЕИМЧЮВЦСЪВДЦТФЫИВГФТОУМЭМОАХЬЯО
ХШЦЪЛЩЦЪФСЭЪКЪРЦЦЪБТНУЗТНЩЬЯЧНЬПЭТОЩЬФЧМЦФЩШКЯЙЪФИЮПУЭИЖЛСАЖЬЦЪФ
ШАСЪОЛЩШЮСУЭКФГДБЪПЮГЯФЦЮПНМОЮТЫФЯВБМТПЮЛЯЙКЫКЯЩЪАУПШЮАХЮЪОЯЕБМЦ
ШНДТЪЭКЮУГАЕШЮЭВОЫХЧУОЬХОСЕХФЪУОЫТШЛКДЦЧЪНЯКШЪОЭМЩФНГПУЬЕЮФФЪИЫЧ
ФЗЛЩФСБТБМЧЩТЦЙЗЕОХПЮХВЯФЦУОВЪРАЮФХЭГДБГУФЕВГОЮТУШУЪРЩЮЧШВЮСЯЧМЩ
ЮЬХБГШЮАЕЬРЭЮЛХЩЗЭШЩЛЧШЗЬЦЦЧКХМЬЦВЙПХЯИВГШЮЗЙЩЧБИВЙ

2. Разложить на множители числа:

   (a) 106430906544459063420038426062 7

   (b) 713694316410156671024373090810562500776042388364041982604731

   (c) 104902515849885470091645053069925514008933166742827835696058792361944271770148684496396884 7

   (d) 138140992874476820828920919880056599096922758178621511404239733379144281562626492354025029081248335748703861222875101193 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 881883384346294124386447572340581037942401285946857981567913349697978642440 87$
   - $e = 17$

   Сообщение:

   - $M = 2940457187179815966020027906699537421050927560531530259190049129956792692300 4$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 19272393717708549553548059572635291483 7$
   - $q = 29309681622507659664848839373550659973 7$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 19431425288987571437500720647172317349510172723110748070448053834265170531216$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 18107169997706262587060947913600159650 7$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 42306523871215390257127241704471946078$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 17205399054869225060657404525885144587 7$
   - $g = 14456459520935336373063981531407848638 9$
   - $y = 13514208827867286823759151987501882141 0$

   Секретный ключ:

   - $x = 50027363781906285889704584326444874962$

   Сообщение:

   - $M = 49498406882117355449679592937235919 18$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 15968167035956424535121011248914269141 3$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 26660354561274765652905739697553718343 3$
- $g = 56379792762155384919559449199806727785$
- $y = 16741599490433133312463981468690164676 2$

Сообщение:

- $M = 24958072962122958282903243207920993923 0$

Подпись:

- $a = 23308593883765959836465180408700898803$
- $b = 10018426177076893769517255437383725 56$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 607$
- $g = 6$
- $y = 435$

Сообщение:

- $M = 429$

Использовать следующий случайный параметр для создания подписи:

- $k = 29$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 2x - 6$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 14

1. (a) Расшифровать текст:

ЖВЭЪЧНЪДГАИМЭАЧЯГЗГЕГБЭЬЧГАЭНСШВЪЧЗСЖВБЪВЕЦЧНЪШГМЗГЩЪЖЗРЩВГБВЪВЪ
ЭЖДГАВЗСШГЖДГЩЖЯЭКДЕЭЯЬВЭЮВЪЖЗЕРЮДЪЖЧЪЕВРЮЧНЖАИШШГЖДГЩЖЯЭКДЕЭЯЬВ
ЭЮЖАИНУЖСЭИЖЪЕЩВГЧБЧЖЪШЩЖАИЫЭАЭЩГЫЭАЩГЖЪЩРКЧГАГЖЫДЕГЕВИДЪЗЕВЩЕЪЭ
МВЭМЪШГЯЧБВЪДЭЖАМЗГЦВЪЭЖДИЫЗСДГВДЕЖВИЭЖАРНВГЦЕРВБЗСВНЧЩГЗСЧЖЭАСЪ
ЧВЭЗЯЖЭЖДИШИЖАЪШАЭЬЪЬЬЩГЕГЧЭЪЦГШЦИЩИБГАЭЗСДЪЗЕВЩЕЪЭМЕВЪВЦРАДГЩДЕ
ЧГЪДАЪМГЧШЕИЩСДГЩЖБИУЯГЖЗГМЯИЧШАИЦЭВИВДГАЗГЕЧЪЕНЯЭАЪЫАГВЧЩГБЪИЯГ
БЪВЩВЗЯИЩДЕЭВЪЖАЭБРЪШГЖЦЪЕЪШЭАЪМЭАЪШГЬЩЪНВЭЮЛРЕУАСВЭЯЖЗЪДВДЕБГВГ
ЧЭЗЪДЪЕСДЪЗЕВЩЕЪЭМЖАЧЦГШИЬЩГЕГЧЭДЕГВЪШГЯЕГБЪКГЕГНЬШГВЪМЬШГЭДЭЖЗС
ЯГБВЩЭЕРЖАРНВГЭБЩГЧГАСВРИЧЖЭАЭЖРЪШГЕГЧВРГВЯЯЕГЩВГЮЖРВМЗГЖВЭБЖАИМ
ЭАГЖСЗЯГЯЬЭЗГЦРАСБГАГЩЛИВЪИЯГЕЯГВСЭГМЪЗРЕЪКВГШКЩЖДГЗРЯЪЗЖЭЬЧГАЭЗ
ЪЧРДЭЖЗСМЗГЖГНАЬЗЪБЪВЖЧЭВЬЮДЖЗЭЭВЗГЧНЦГЕЖЯЧГАЬЖЭБЯАВУЖСЕЦЖЯЭЧЪЕВ
РЮКГАГДЧНЕКЭДЖЧЬАСЬЧВЪБГШВЪЖЯГАСЯГЕЬВЪИАРЦВИЗСЖМЭЗШЕБГЗИЩГЦЕГШГЖ
ЗЕЭЯГЗЧЪМЗСЦЗУНЯЪЦРАВЪЧЖГЖЗГВЭЭМЗГЦИЖДГЯГЭЗСБЗИНЯИДЭЖСБГЖЧЪАСЭМБ
ВЪДГЯЬАГЖСЩГЖЗЗГМВРБЖЗГЮДГЕРДГАГЫЪВЭЪБГЪДЪЕЪБЪВЭАГЖСБЕСЭЧВГЧВДГМ
ЗЭЖГБВГУВЪШГЧГЕЭАЭЧЖМЪЖЯЭЖЗЕАЖСЭЬЦЪШЗСБЪВЩГБЯГБЪВЩВЗЖЗАЩАБЪВДГЖЗ
РАБАГДГБАИДЕЭИМЭАЖЖЭЩЪЗСГЩЭВИЖЪЦЩГБЧЖЭАЭЖЪШГЕГЧВЖВМАЬЗГБВЪДЪВАВГ
ЧЭЩБГЪИДЕБЖЗЧГГЖЗЧЭАБЪВЧДГЯГЪЖЭЧВГБЯИЬБЭМЪБЧЭЩЪАЖЗГАСЯГЯГШЩЗГШГЗ
ЕЪЦГЧАЖАИЫЦЖГНЧЦЕЭВРБЧЖЗЕЪМАЖЕЪЩЯГЭВЪГКГЗВГЗЪБЦГАЪЪМЗГЬБЪМАЧВЪБЖ
ЯЕРЗИУЯЖЪЦЪВЪДЕЭЬВСМЗГЭИЗЧЪЕЫЩАГБЪВЧБГЭКДГЩГЬЕЪВЭКЫЭЬВСБГЖЩЪААЖС
ББЪВЪЖВГЖВЧДАЧБЕМВИУЬЩИБМЭЧГЖЗСЯГЗГЕИУДЭЗАЭГЩЭВГМЪЖЗЧГЭЦЪЬЩЪЮЖЗЧ
ЭЪАУЦГЧСБГЕЬШГЕАЖСЧИЪЩЭВЪВЭЭЭМЖГЗМЖИЖЗВГЧЭАЖСБВЪЗШГЖЗВЪЪДГЗЪЕАГК
ГЗИЯМЗЪВЭУЭЖАГЧЪЖВГЖЗЭЩИКБГЮИДАЦГАЖЭАЭЖГЮЗЭЖИБЭАЭИ

(b) Расшифровать текст:

ЛЕЫЙЫЮЩУМРЙМЛЦОЮЧЛЧИДПЕРСМФФПУЬЧДЗЧБУСЧСЖФЛЙФИТХЫСЪМОЫСЫМЬЗЫЗШЦГ
ЯЖПЪДПЗФИНЭЛЙЛКФЭЮХНЯЯШОБНЗКЦЦЮЗЩИАТБЙСВЪЗЩТТЭЛПОЗЯАФОКФЛВФТРЙГХ
ЛЩЖМХМСМОРКЦЛХЙДЪЖЩННХГСДСКССХЪФИХКАЗДЩСВЪИГРЗВМССССЪЙВМБЗЕФЛКЯЛМ
ДСЯДЪТМЫЗШХНЧЗУЗБЪЙМКИГБРХТЧМЦЪЗЦКХЕРСЕФСБССМРЫЦБРСМНЮШХЗСЬХХЙФЙ

ШТНЬЗТРОЧБЙРРСЪПКТШБТФБЭЕХПГСДМФФЪЭШХБЪИЪЖЦСЫШПНФЕЙСЕЮФУДЪЧЗЧКЗЮ
ЮТЯМЪМЛСРЮЗЙИПФДШЪСЪИЪЖЦСЫПСМНФТЛНРЖХЛСЪЯМОЗВЗПТНЩДЩСВРИЧЛЦФЖЪТН
ЕЭВПМСЗСКМЩЗРРДШЗКРДЫЗЛЛБФЛГФРЮЙФРНШМШЩДЫДМРЗКЗИФСЪЛМОЫЭЛЙЗДЮКСЛ
ИЮМТЦОЫЗЛУДЩЖВМАЬЗЛЖДФАИЕКЧЕМРНЮИМХКФБЦЯМФПЯХБДБРФОЪИХФСЪДВПГОЗЧ
ПНЭЯЛОЙЬЮЦСРЮБПТНЮЙШОВЪКЪЗПЭЛЙСЛЩЮПКБЪДПЫЫЧБЦСЙЯСЩЯРЫЙХФЗЧКЙИКИБ
ЮРДФАУИМЩФРЕРОЗПШОЬБЙЮЦЦОЛСЛЩБЮИВЪЖМХОЪВЛЦОЪСЧБГГЛХРЗНМЛЯССЪМЛЖП
ЗЩСБЧЧХФСОСПФЫЪЭПРОЪЬЧЦЖФДШЕПУЕВЫКСЖПЪСЪЕФИАЗДХЗДЧЛГСРЮЫЩЯРОГЧИО
ЪКЩЛОЪЭЙОРЮЖХМЖЧЗЛИЭФДПФКСЭХЕСИАМЖНДВССЭНФТСМСИЧЛКФРФСНАБЭИПЯЭХО
ВЮЙМДНОДЮХННФЙЛКЭЛЪЗВРЮШОТТЪУСЛЪЬТИШСЪВХЫЫЗТИЖЩЗЩИЦСКЩЕТОЖШХНЕБЬ
КСЬМЛРЗЮЮТЯМЗОХДРЮЗЩИКИКЩЕФЩЗТБАЪЫГФЗЧХФСРЪЫМХНОДУРДЪКЩЕСИКЦУЗШЙ
ГЛЗОЖХЕМСБИЮСИЮРКШФЛФЛЙЪЕПТНЦЙХЕЗЮЮТИЛБЗЩЛОЬЮЛЕЗРЮТФЙЪЙЪБЗЩЮШСЛЩ
ЮФРТКИМУДШЮФЦБЪЪШХНЮЮТЯРЮЫЬРНОКМЙДЩЮУСВЩЮЩУДЫЮЩХЫОЗХДПТЗЦФМЪКЩЯД
СИХОНТЮФЛПУЕВЫКСЖПППНФЪВОЗЫЙМУБЩФЦУЗБЗЛСЛЪЭФСВЪБОНЖЦЗЙННЮЗЧЮИЫЙПД
ДТДШСАЖЫТИМФЮУЪСЪЭМЕДЧБСЛИПЗШЦГЬХЩУДНММХССЪСФДНЮКЗДТЮХРРЫЙХФЗЧЬХ
ХНОКГТНОБФСБЮХШЕЙЪЕМРГЩЛШННШЗЩЕДГДСКЙЫЗШОДЪЪМЗАЮЧЯНМДЗЩТПОБТФБНЖ
ЕХДЫЮЧЯНЮЭВЩДЮЖЪЕЧСЪТЖНЬЗЛЛДЫЗЙФДШМЙЛГЩЗЮХНЫЮЧФНЩАФХМУЗИИГЪЕШНТД
ЛГЛЖОЗТЛКРЫЪШЕЬЮФЮФЫЗЧСРЮИЧЛСЭЛСЙПЦЗЮХНФЛЧФЙЯЙХЪЙФЖФИБЗЛМУОСДХХГ
ЧЫМРЗЦНХПЙСЪПНАСЫЪЗМЭБТЦФЪДХЗМЪВЙСГЪВХХЙГДШРДГЮКСРЦАЩЯБЭЮЦУ

2. Разложить на множители числа:

   (a) 744455733227496774836252484517

   (b) 11867071418555986829570883564360775105444525652852781719840 33

   (c) 7559360493862189206234617332764766355531022654109437589739309570579731470337901946225021 01

   (d) 1644724738044947189917928971909676523121402532737550291850346726645922977386639706168395082648728283739566441110186146233

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 5020561829364652908866177266464663213905478217661305770559145387618877185635 9$
   - $e = 5$

   Сообщение:

   - $M = 17813913778163881767971353041127258461134276702400836598925775641181973957415$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 198265028378193661938989006726982329593$
   - $q = 291542290546324149524911745223716401303$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 317385820141211594632566862673923376604180745723904819841728432160539809284 27$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 25581972311115504747561426861991487749 9$
   - $e = 3$

   Зашифрованное сообщение:

   - $c = 68261514954923372927629335465808748 86$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 290623171042368675427016362091297048891$
   - $g = 188660417860656973800842383705811713508$
   - $y = 10332266743693946330587414024014091393 5$

Секретный ключ:

- $x = 128225927806338709170195738008189086767$

Сообщение:

- $M = 24308696047072250240892416432217343053 2$

Использовать следующий случайный параметр для создания подписи:

- $k = 126262038502327965782489827443466592129$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 219902655353775810805242239884234374457$
- $g = 300169020804758138454652509545183750 63$
- $y = 551946794119396977949144943253711467 23$

Сообщение:

- $M = 600084057653470886319041274749364983 37$

Подпись:

- $a = 690695474933206575208731310073420245 33$
- $b = 184230095247396671473829220919141618038$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 673$
- $g = 116$
- $y = 161$

Сообщение:

- $M = 367$

Использовать следующий случайный параметр для создания подписи:

- $k = 533$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 13x - 4$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 15

1. (a) Расшифровать текст:

ЕЖЗЯГЬЙГЕЫДЕЪЕЯЮШКДЙЕЩРЯБЕЩДБЮДДТМЩЪЕЫКЫЙТЩЯЫДЕИЙЗТАЩЕВБЖЕШТЩВЩД
ПЯМБЖБДМЙТЮДЙУДЬЩЖЬЗЩЕАКЭЬШКДЙКЬПУБЕВЯКЙЬШЙБЪВЫБЕЩТИЙЗЕЪДШПБЖЕЫЕ
АЫЯБЖЕШВЯЭЬЪЕЩЕЗЯБЙЕЙЬШЖЕЫЕИВВИЙЗТАШПБЯЗЬНГЕВОВЯЪВЫЬВДБЕГЪДЫДЙИЩ
ЯЫЕГИЕЩЬЗПЬДДЕЪЕШЬИИГТИВЯОЙЕЭЬЙТГЕВОЯПУЖЗЕЫЕВЭВЯЩДБКЮГЯОВЯШЬВУГЬ
ИЖЕЗКИИБЯДЬЗЮКГЬЬПУХВАИЖЗЕИЯБКДЬЪЕЖЕЩПЬГКБЙЕЬЪЕЖЕЫЕИВВЩДПКБЗЬЖЕИ
ЙУХВАЖЕЩЙЕЗЯВДЙЙЗИБЕГЮТБЬЩЕЖЗЕИЯЩДБКЮГЯОДЕШПБЯЗЬНЪВЫЬВДДЬЪЕИЙЬГЭ
ЬЩТЗЭЬДЯЬГЯДЬЕЙЩЬОВДЯИВЕЩБПЯИБЮВБЕГЬДЫДЙЙТКГЬДЮЪЕЩЕЗЯПУЗЬШЙИТГЯЙ
ЬБИДЬЪЕЫКЗНБЯАЖЕВЕИЙТАМВЙЫЩТИЙЗЕОЯЙЬЬГКИЖЯДКИГЕЙЗЯЭХВАМЕЗЕПЬДУБЕ
ЬЪЕЫЩЯДЩВЯЫИЙВЯШПБЯЗНЗЮЫЬЩЙУВЯНЕДЬИОИЙДЕЪЕЯЮЕШЗЮЯВЕШЬИЖЕБЕАИЙЩЕЕ
ДЕЪВЫТЩВИДЩИЬЙЙЕЗЕДТББЮЩЬЗЕБЖЕАГДДТАЫЬЙУГЯБЕЪЫЭЕЫЯДЯЮЯДЩВЯЫЕЩЩЮВ
ЬЪЕЗКБЯЯЖЕВЕЭЯЩЯМИЬШЬЕБЕВЕПЬЯЖЕЫДВИЙЗЯБДИЩЕЯЖВЬОЯХВАЩЮВЖВЬЙУЯЮГМ
ДКВИЙЕЪЫШПБЯЗЬНЮИЙЕДВИВШТГКГЕВХРЯГЪЕВЕИЕГЯБЯЩЬЕВЕЩЕХЕЙБЗТВЗЕЙЩБЕ
ЙЕЗЕГЩГЬИЙЕЮТБПЬЩЬВЯВИБЕЗЕЙБЯАЕШЗКШЕБЕЪЫЩИЖЕГДХОЙЕФЙЕИВКОЯВЕИУД
ГЕЬГЩЬБКЯОЙЕДТДЬЫЕЭЯВЫЕБЗЕЙБЕЪЕНЗИЙЩЕЩДЯЯГЖЬЗЙЕЗВЬБИДЫЗДЬГЕЪКДЬЫ
ЯЩЯЙУИШТИЙЗТГКИЖЬМГЖЗЕИЩЬРЬДЯЯЗИЖЗЕИЙЗДЬДЯХЖЗЩЯВОЬВЕЩЬБЕВХШЯГЕВЕ
ЫЕАОЬВЕЩЬБЬИВЯЮЖЯИБЯГЕЯЖЕЖЫКЙИЩЙЩЕЯЗКБЯЩИЖЕГДЯОЙЕВКОПЯЬЯЖЗЕОДЬАП

ЯЬЯЮГЪДЬДЯИКЙУЙЬБЕЙЕЗТЬЖЗЕЯИМЕЫЙЕЙКВКОПЬДЯДЗЩЕЩШЬЮЩИБЯМДИЯВУИЙЩЬ
ДДТМЖЕЙЗИЬДЯАЩИЬШТВЯЖЕЗЭЬДТДКИБЮВБЕГЬДЫДЙЩЯЫДЕДГЕЙДЬЪЕЙЕВБКДЬЫЕШ
ЯЙУИХВАЕЙЩЬЫЯШПБЯЗНЩДШЗГТЪЕИЖЕЫБЕАЕОЬГЬРЬЖЕЙЕВБКЬГГТИЙВЯЗИИКЭЫЙУ
ЕДПЬГЖЕВЕЭЬДЯЯБЕЩЫЗКЪЩИЯВЯИЬЪЕЗЕЩДЩЕПВЩБЕГДЙКЮЫТМИУЯИЩЯЫЕГОЗЬЮЩТ
ОАДЕЩИЙЗЬЩЕЭЬДДТГОЙЕФЙЕИЙЕШЕХИЫЬВВЕИУИЖЗЕИЯВЯЮКГВЬДДТАБЕГЬДЫДЙШЙ
ХПБЯШЬЫЕЙЩЬОВЩИЯВЯИЬЪЕЗЕЩДДЯЭДЬЕЮЬЗДЩЮЙИЬЪЕЫДКЙЗЕГЗШЕЙДЯБЕЙ

(b) Расшифровать текст:
ЗХСГЭЗХЭИЮВЪМЙТКТЮЭЕОРЩЙЭЬТТЕДЮЫЪЖЫЮЫТЬТЕАЬЕЛЙЯУГЧЦШЬЗЙМЯЦКТМЫЭК
ТЭЫПТЗИТЫАГЙЬБЫНАПУЫДКЭУИШЖЧШКСМЩУГБАФАФАЙЩЫЭЗНЧЦДЮКАЯКАЗХРЙАЛХЕ
ГДИПЙНШНОБДЩОХХИЙЕЮУВЖАЯЮАЧЛЫЯАШАТРГЮСЫЯЪЫЖЙЦПЙЮШБЗСДЮАИЮЕХГЖЧЙО
ЮГЮШЧПЭЪЯЯЙЬДЖУУЕЗНЭЙБЛЛИЕЪЫТЬЬЩДЮЩЬГЮНЙХДЫИСХДДГВЮЭЧНФАЖННЫАУЮМ
ОЮАГЙЩАЖЗЭЫЦДГАПЦЙЮНТХЬЫМЙРДЫМЯУЙВЙХЪАДМШБРГГЧЪАЭДДЦБИОШБЗИАСЪЯЯ
ТХЧКЙЖАЭЬЭИТЖФБГЯЙПИЙЮАЭЧБХРЖЩЙЧЬЮЙЭТЩЦЗЙСЮКТИЯБГЙКИШВЮВПЬГЮУЙЬК
ШАДЩЙШАШКАНТТЩЖШАЧЭЖЪИТРЖБЧЪЙБЮВОЮЙАЙТТЖЧЛЫТЖББТЫЖИЭТЕКТКАСПЫЭОЙ
ГШГСЫЖШКЭЦЗЪЕТРЭБГЧЬЬЙУХЬЕДНПЬИДНХЩЙЮЙЯИЭЛЖЪУЙАВППЖБАТЫАЗЖЫРРШЬЭ
ЦЕЮМЯЮРЮИИЭЖЗЖТТЖШЖХХЕЮЗЕЧВШЦЮАЛЕГШЦЯАЛТЭЖЗНХРЗДЛСШЭГЛЫТЗДУТЩЗЖЙ
ПЬЮИЧЬБЫНАПЬЙИЖЮЫЗБЙЖТАДЯХЫЙЗЭТЩФЮТТЪЬЪЧЧЪЖЯЯТЮЮБЭЭБВЛМПЬБЖАТЯКЖ
ГЭЯЙВНЭЦЪБАРЬЙШГСЬДЩЖАПЖАЙРЬЙДБШУЕЮЭХТДДАСЬЩЖЙТЯЖЩЖЮЦЭЗКАСПЫЭИЪЖ
ГЯАЪГЙКЫАИЫЬХАФДИЫУЪЕЙШКЯЙИЫЪЛЪЛЫУЕВАЭУЕЮАТЪЛГААТГДМЙЯКБЬИЩЖЫЮЫП
ИГГЯКЯГААЪЭЗНЪЬЭЙМТЮЬЮАХЫЭВЙРБЬЫЛУАФЗЙЯЯДЫРЮЪЭЯМЮБЬЖЧЫАЪЫТШЯЪЫЖЙ
ЦПЗЗТЧЙАЕЬЮАЪАЯЯЕВМИХЕДЭФРЖЪГЯКЙШМТЪНДВЦЯКШЙЩАВЕЙЮЪЖИЛХЪЙВАЕЫЖБГ
ОБЬЫНЮЭЭОГШРЬДЗЮРСЫИЪЦВЙЭХТЭИЧЮЯДЖЧТЧАШИЫРЕДДЬЬЗЪЧПЯКЖАЯЦГВАЪЯЗЫ
ТШКЕСЗХХЪЫМЯЦЭВИЫЕФФОЩЮФЮГПЫЖШИИЬКАЛИЩЙТМХЩФГЮЫЮПАЙЪЩЭЬЖОУЯЕЗЯЦА
ШЬЭУЬЙКЫЭЬТЭПУГВАЪРЭЫЕЫЪЕИОЯЦНДКЫТЖОАШШЭЫЕЭЬЪИГЬУИЫЗТЫЪЫАШЦОЫКЫЮ
ЯЮЖЩУЕЧЙШКЕВАЪЫЭЙВЪЩЬДЖРЬЙИЙШЭЭЖАСЫЭФИТЯГЙУЪЦЖИСРУИЗГЩЫАЪЙОЮЖЯБТ
ЫУЫЮЫШЖИЙЭЙЭАБТАЙВАЪБКЫУШЦДЖТЪЙЭВЦЮЩАШЙШЫЖШЖХЪЭГМЫЯКДИХУЩЫЯЪЬБЧА
ФХСЮНЪЬБЗГЭЬКСЙЮАЪБАЪЫЖЯКЫЯИЫЯХХГДЬЪЙНВНТФЕЮЕЫРЙДЬЮАЪЫИЪЬЭВЙТПЭЗ
МХЩАЫОЮАИОЖХЪЭГУППИЮИЕРЩЖГЪЭЛПАПЯЭЩЙЯУИЭЖЩЬЭШЙЫПИЬАЪЦЭДЬШУПЫИЪЙБ
ШЖЮААФЙЯЯДДВПЫОЕЛТТЪДЯХАЭБЧЮАЪЙЭЧЮЭЕЙЮААЩЯТЬЙИЭШЯФГАЮЕЙИИ

2. Разложить на множители числа:

(a) 90362345485484659314579985858 7

(b) 10170997366774311819982573841870420870388707052877072489955 93

(c) 79927837547788588565710345079493414152680856077911486529057334020281892607576362017027121 3

(d) 19557862297249330384825407206843459740376151654718594947848979773935109304323350178508707686060194649100381119734917992 57

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 553449576046356685080246915834610807052737910087612250185002886602344374278 07$
   - $e = 5$

   Сообщение:
   - $M = 459797221609759342646990812523489366105063642614050178900427904721521125218 5$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 264571439294660457496452966891058578247$
   - $q = 2898980048690734093208445397564213473 41$

   Открытая экспонента:
   - $e = 17$

   Зашифрованное сообщение:
   - $c = 573490895515822442014022141633057281631588181206134567047918363371989168996 60$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 14617162127012034767575115338739473058 3$
- $e = 17$

Зашифрованное сообщение:

- $c = 13072160268011506520380822629478154528 9$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 31189038960189329414878791070597643055 7$
   - $g = 13817363528150922331921654900195071334 0$
   - $y = 25497270054726847057925291352784144183 6$

   Секретный ключ:
   - $x = 21633945664226761088347143021305952875 9$

   Сообщение:
   - $M = 80692413423617996995703759411193618570$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 13657578250063582790224031751835220142 1$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 32431599737698423119496186479947941903 3$
   - $g = 27929787951138380734299783902969652393 6$
   - $y = 94917895414736761412504661723708080140$

   Сообщение:
   - $M = 30875636698165681199252127371324534688 9$

   Подпись:
   - $a = 24448842358933866435432763823984841785 1$
   - $b = 76925155667568699932018360338910412078$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 587$
   - $g = 458$
   - $y = 317$

   Сообщение:
   - $M = 402$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 533$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 10x - 2$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 16

1. (a) Расшифровать текст:

ИПЦННХЮФПИОТУСХЛЕЛХЯФПРИФЕСИПЦЖСФЦЗУБНСПИРЗРХЛКРИПСЖСХУРЮФСДУОТС
ФОИЗРЛИФЛОЮЛСХЕИЪОХЕИУЗЮПЖСОСФСПХЮПРИРИЖСФЦЗУЯХЮЕСУЛФПСКЕРИЩФОЮЫ
ЯХЮТЦЖЪИЕПУЪРСРШПЦУЛОФЛПШРЦОДИОЮПТОХНСПРИФНСОЯНСНКНСЕТСЗШЕХЛОЛФХ
УСЖСНТЛХРЛТСХЬЛОЛНЕЛФИОЛЩИРИИТИУИНОЗЛРИСЪЦХЛОФЕИУШСПЛКЦЕИЪИРРЮМД
ЫНЛУИЩНСХСУСЖСЗСТУЫЛЕОЛПЮРНРЦРИСРЗИУЙОЕУЦНИЕИУИЕНЦЛЪИУИКПЛРЦХЦЦЕ

ЛЗИОДИЗРСЖСЛЕРНЦАПЛЪЕКЗИУРЦХСЖСРЕСКЗЦШХСЖЗТУЛЕИОЛНТЦЖЪИЕЦЛЕРЛЖРХ
ЯЛЪТУЛФЖМФНКОИПЦТЦЖЪИЕЖСФЦЗУБТИХУЦЧИСЗСУСЕЛЪЦХЮРПРИЖСФЦЗУЯСХЕИЪО
ЛЕРЛЖРХЯЛЪТСЕХСУФОСЕФЕСИЖСНТЛХРХЮЗЗБЫНЕСУЛФПСКЕРИЩТЦЖЪИЕПШРЦОСТХ
ЯТОХНСПЛЗСДУЮМТСУЦЪЛНТСЕЛФТСЗОИФЕСИЖСФХУСЖСРЪОЯРЛНСЪИУИЗЯДЮОКПРС
БЖОЗИОФПИОСРТЦЖЪИЕЖСХСЕФЯТСЕХСУЛХЯСХЕИХЕИОЛНСЗЦЫРЮШПСЛШХСЕУЛЬИМХ
СЖЗНРИСТЛФРРСПЦПСИПЦЛКЦПОИРЛБЦЕЛЗИОФУИЗЛПХИЙРЮШФХУЫЛРЫЕДУЛРСДФХУ
ЛЙИРРСЖСЕНУЦЙСНЛЕНКЩНСПНЧХРИСРТСЗСЫИОНТЦЖЪИЕЦЛФНКОИПЦРЦШСРИФНСОЯ
НСФОСЕЕИЫХЯИЖСФНКОТЦЖЪИЕРИЕКЖОРЦЕЦЙИРПИРПРИРНЛРЦОЛРЫИБТИХОБФХОЪЛ
ХХЯТУСФИДПСОЛХЕЦТУЛРСФДСЖЦЛФНУИРРИИУФНРЛИЕСЕФИШПСЛШТУИЖУИЫИРЛШЛП
СОИЖССФТФИРЛЛЕФИШДОЛКНЛШПСИПЦФИУЗЩЦПИРТУЛХЬЛОЛТСЗЕЛФИОЛЩЦРИДСФЯР
ИДСФЯТСЕХСУОЛПРИЖЦДЛХИОЛПСЙИХДЮХЯЛЕТУЕЗЦЙИОПИРСДСЗУЛХЯЕЗУЦЖЦФОЮЫ
ОНУЛНТСФХСМХИСНРРЮИТСЖСЗЛХИТОЪЛСФХРСЕЛОЛФЯЖОЙЦФЕИОЯЛЪОИЙЛХЕРСЖШЦ
ТЦЖЪИЕСХИЩУСЗРСМЖСЕСУЛОДИЗРЮМЗЗЯНЪХСХИДИЕФПИУХЛДУФНСЖСЗЛХХЛСХТЦФ
ХЛИЖСКРИЖСХИДИЕЮНЦТЗЗЦХЗОТУЛПИУЛФХУШУЗЛЕИОЛТСЕИФЛХЯШСХЯПИРФХУЛНТ
ЦЖЪИЕЗОКРНЛПИРХСХЪФУКЕКОЛЛСФХЕЛОЛДХБЫНРЫХИДПЛОЦИХЖСЕСУЛОЛПРИЕАХЦ
ПЛРЦХЦРИПСЖЦФНКХЯЪХСДСДУЗСЕОФФЕСИПЦЛКДЕОИРЛБРИФНЙЦСЗРНСЙЪХСДСРИП
ЛФСЙОИОЪЦЕФХЕСЕРЛПСЛДЮОЛФОЛЫНСПФПЦХРЮПИРФРСЕТУЛЕИОЛНФПСКЕРЩЦЛТСФ
ХЕЛОЛТ

(b) Расшифровать текст:
БИЬЮПХХПШКСЦЦМФПХШЕЕЛИБЯФЗХРМЬСЯЩЙДНШЦЗУЪХПАСОЙЪАЫСЛЬМКЕПАЧЗОЯЯЖ
УЫТАЕЮИХАЗВФПЪЦПЪЩЬЭЙСФЕМКСПХЯГЛЙЦЯАХФРЦГКСГГПХХРЦЙСЙЯАДФМПИЭДМЮ
АЮИЩУГЕИЛБЗЭХМЬНЭШСЬНЖУВУВЪФШЬМГИОЪГЩСКЪЙГХЛЬЖЫСИЙЖЩСТКИВСКТЭУКЛ
ЬЛЖЕМЩЖЭНШУДАЕФЬЭАЪСЬНЖУВЧЕЖПФТОЭХЪЫМЕПМЯНЭТХШЙБРХСЙЩХЕЖЕАТЧЦИЛЗ
ПЩЙКЩКУЛЙЛУРЦЬХГЪАЕИУБВЙХЧЗЭЗЦКЕАЪЮУФГЪЦЙЫУЭПЛЬЗЭТХТЕИЦТЬЗГИСЯАБ
ЛЙЫЙЪЛЮЭЛАРЪФЯЭХУУИЪЮЛАГЯРМСЙЯПЪФЙЕЖХРЙИЛЩЕНЖФЦЯЗЕИНЦВЕЯЦЬНЖПЪЕН
ЖТЧЦЕИЮТЬЬДРСБЖАРВЭЗМЛТЬЭЕЮСЬНЖУШШВГКТЬЯЭПИБЯКСИЙАЭТТУЗЕРПДЗЕИТУ
ЮПИИЙЖЖДВБЗЭУМАЧЕИНУЖАФЛУЖКЯШФАЕСЕАЕЖЖХЕАГСЙУЕВНХРЖЭНШУДАЕФЬЭАЪХ
ЫЙЩШХТГКФШЬЗЕСЕЬТЭРГФАЙХХШЙАЖЧЬВАХШШЙГЛФУЙЬЦУММФЛФУМЖЖТЖОЙЯЩЬКИЛ
ЙУВЭХУУИЪОКУЛФНОЩЙЬИЕЦМЪППТАКСНУЬЛЗМАТКСШЩГЯЕМАЙБШЧЩЙЪСРЭЛЖФПЩЖЭ
НШУГЪРХРГПЗЩКЗЕИЦЬЯЛПЩКЙЕФХСЖЙЛТЯБЬХГУФЭХЧЦЯЕНХЩГПИЧУВКУПТИЯРМСЙ
ЕИЙЙЯЛХСББЕЛСШЙБТХЗЯУРМПОЬИЩПНЦЫСЭАКУФТЛЭЛЮРЦЖЗПЫОДИФЭЙВУХРГКИТК
ВЙХЪЭГКИШКВДИФПАЬРЪМОЗУХЯГКИКУИЭУТЦЭЙИЬШЙДРЛЦЛЖЕЦЮГЙОЩКЕЕПЦЬМВСЧ
УАЙЛСБЛЙЦЛЭЛАИОФДКИШЪГЭФТЦЗЖЙМААЖФЩММФЕУЭЙВСЧЫЬЭЗФЯГИСЩЪЛФППЮЙЕС
ЙЭЛЖЪПАЭХХХЭГЙЯУЬТЛХГЯОДРМЯЙРИТЭОЙХПЩМЪЖХЮЙЬДМХЗАОХЯАИЗПЭЛАЫЦЬЛА
ЕИУЯЕСКЬЗЖИКЬЕЖРЛЬЛЖЖХМКИЛЛБЗУЕТЦНЖЛЛЮОЫСМТЖАКИРЖЭРППАЬРХЧЯЭЕЪЖЕ
АЛФЦТЭЖХЫАДСКРЦЬЦУАЧЗУПЯЕВЕЙСЙИСЛЬНЗУЙЦЖЙТЧЪЙВЖМЫАИОЪЦЙЗУХЪАКЯЕШ
ИЭПЪРЬЭЙТСАЕИЧЩРЖЗПЩЭЯЗПРКЭУМТКЖНХЪИКИСБЛЙЕХМКЭРСЬЭЛБЩЮОЩНЪБЭАЗУ
УИЖРХЯНЕСЙЦЖЙЕМЮЙКРХРГЬПХЧКЖУОЦЖЭЖХЬИЯДХАЖАЕХЬМЪИЛЬЗАОШЬКИЛЮЦИЭП
ХУЮЖТХЯКЭЫФЬЮЖТЧЦРЖЗЙЖАЗУМРЙЙШХТГКИТКМКЕХЯЕЯОМЪОЗУППАЫБСРЗВНСЬНО
ЦЧЬЯЕСУБЛЬЛИЬЮЕИХАЕЮЛЩУЗЕИЙЪЙЭМЦЮЙЙЯИУЯЭОХЦЯЭХХЯТЙХПЦЭЙИРЪЙЭМНЦВ
ЕЛЮАЙКНХУЬКБЯШМЗУХЯГГЛОБЗГИФЫЦБФЩЮГВЪЩЬЗЖЖЪТЖКИИЯЯЭОЩКЮЖЕ

2. Разложить на множители числа:

(a) 75767971062442521964372187 2021

(b) 513122608542075190848933723411937667123500318236243828681271

(c) 784117606131836874389781626045778062151678122703995219312393175670784120081672109329252951

(d) 203957640695205664893777431230763477732165663147739852855342860030087285021385205446078893399326298358615818795122922519 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 428334917503543610540398245669577648224786655440323798521793940242019171706 49$
   - $e = 5$

   Сообщение:
   - $M = 619383749272344078052858101762799347151032846055438605278946332477519528362 8$

   В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 27422092890788589416134029140041952402 3$
- $q = 22093147892409978115206630339359020268 9$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 28350891362859838100251237490578653292159906102382103612240405341064822029892$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 18468371598160721951109530615356589689 9$
- $e = 3$

Зашифрованное сообщение:

- $c = 98325888663532010807855413745028302428$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 25618077237375051746092891910431113871 3$
- $g = 38003798909468643504534772460675511313$
- $y = 21795464998524825738526506818138660168 6$

Секретный ключ:

- $x = 66686264452002470640824906412016643169$

Сообщение:

- $M = 18556187055593866512193936621106001144 5$

Использовать следующий случайный параметр для создания подписи:

- $k = 24986968253781947938466589665678341972 9$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 22728946516728224425223031881291195259 7$
- $g = 85911102159405300899588880443392844476$
- $y = 87445724353021767964244942205506252 27$

Сообщение:

- $M = 21567152769054505593283076872405976847 4$

Подпись:

- $a = 39169786351560255500478950071596194406$
- $b = 22106651908944488834469592961685540593 6$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 563$
- $g = 275$
- $y = 30$

Сообщение:

- $M = 313$

Использовать следующий случайный параметр для создания подписи:

- $k = 349$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 8x - 8$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 17

1. (a) Расшифровать текст:

ЯЦТЦГЪЕБЯАЬПЬМЭУЮУСЬРЬЮЦАКЪЙЬЯАЩЦЯКСЩХЫСЩХЫУЯШЬЩКШЬЪЦЫБАЭЮЬТЬЩФЩ
ЬЯКЬПЬМТЫЬУЫЖУЪЬЩЕЫЦУЭБСЕУРЯЪЬАЮУЩЫЪУЫЭЮЦЯАЩКЫЬЦХЮУТШЬЭЮЦЗБЮЦРЩУ
РЙЧСЩХЯБТЦРЦАУЩКЫЙЪРЙЮФУЫЦУЪЭЩБАЬРЯАРЦЫЯЪУЖЩЦРЬЯАЦЫШЬЫУДЬЫХЯЪУЩЯ
ЦЯАШЬМЫУЭЮЦАРЬЮЫЬЧРУЯУЩЬЯАЦМЕАЬЦСЩТЫЫУСЬЯАЩЯЪУАКЯЯЪЫУХЫЕУЪБЕАЬРЖ
УПЩСЬЮЬТЦУЯШХЩЬЫЪЫУЯАЮБЯЦЩАЙЭЮЦХЫЧЯШЬСТЪЬЩЬТДЙЪЬЦЫШЦЫБЩЦАУПУРУЮУ
РШБЫЖУМЕМЫУПЬЯЬРЕЦЫШБЭЬШХЩЬЯКЭЬШЕЩЯПЙЫЭУЮУШЩТЦЫУУЯЩЦПЙЫУАРЬЧЯЩБС
АЬАЕЯБХЫЩЯАЮЬСЬГЮЙЕЫБТБЪЫЩЦАЙРЖУПЩСЬЮЬТЦУЕАЬЕУЩЬРУШШЬАЬЮЙЧРЙРУЩА
УПШБЪУАБПЙЩЯЪРУЩЦШЦЧСЬЯБТЮКАБАЬЫРХЩЫЯУПРЦТРФЫЙЧЦАЦЫЯАРУЫЫЙЧАЙШЮУ
ЭШЬЭУЮУТЬЪЫЬМРЦЫЬРАЭЮЬТЬЩФЩЬЫЫЬЭЬЪЦЩЬРЩАУПХАРЬМТЬПЮЬТУАУЩКХАЬЕАЬ
АЙЬШХЩЪЫУБЯЩБСБШЬСТЭЮЦЫБФТУЫПЙЩЯШЮЙРАКЯЬАЯРЬЦГЫУТЮБСЬРАЬЩЦУЗУБРЦ
ТЦЖКАШЩЦУЗУАУПЭЬФЩБМШЬСТЭЬЩБЕБЯРЬУСЬЯБТЮЯАРЬЬПУЗУЖКЯЩЦЯЩБФЦАКЪЫУ
ЯБЯУЮТЦУЪРЬЭЮЬЯЪЬЖУЫЫЦШЦУСЬТУЮХЬЯАКЭЬШХЩЦЯКЪЫУАШХПРЫЙЕАЬЫУЪЬСЫУБ
ЯЪУГЫБАКЯЕУЪБАЙБЯЪУГУЖКЯЯЭЮЬЯЦЩЬЫЪУЫЫГЪБЮЯКЦЩЦАЙЫУРУЮЦЖКЕАЬРУЩЦШ
ЦЧСЬЯБТЮКЬАРУЕЧЭЮЪЬЯЪБАЦЩЯЭЮЦХЫАКПЮЬТСБСЬЯБТЮУЪПЙЩЫУРЯЬЯАЬЫЦЦЛАЬ
ШХЩЬЯКЪЫУЪЩЬТБЖЦУЪЫУЭЮЬЯАЦАУЩКЫЙЪЫХРАКУСЬРСЩХЬПЪЫЗЦШЬЪПЙЩЬЭЬТРУЮ
СЫБАКЯУПЭЬСЦПУЩЦЦАЬЫЕАЬПЙЩСЬАЬРЭЬТРЦЯУЩЦДУМРСЩХГРЯУСЬЫЮЬТЦРЭУЮРЬ
ЪЭЙЩБЫУСЬТЬРЫЦАУЭУЮКШХЩЬЯКЪЫУПУЯЭЬЩУХЫЬЧГРЯАЩЦРЬЯАЦМШЬЩУПЩЯЭБСЕУ
РЪЮЕЫЬФТЩЪЬУСЬЬАРУАЫШЬЫУДЦУЗУЫЙЫУЯЯЪЬТЬРЬЩКЯАРЦУЪЭЬЪЦЫМЛАБЪЦЫБАБ
ЕБРЯАРЬТЬЩСРЬЯАЬЮФУЯАРЬРЩЬРЬЪЫУЫТЯЩПЬЯАЦМЕУЩЬРУЕУЯШЬМЬАРУЕЩЭБСЕУ
РБЯЩБЖЧЯШФБАУПУРЯМЭЮРТБЮЯЯБТЦЪЬСБЩЦЭЮЦХЫАКРАУПУСЬЯБТЮАЙЕУЩЬРУШЯЪ
ЙЖЩУЫЙЧАЙЯЪБРЦТУЩПЙЕАЬЩБШРЯАРБМШАЬФУАШЬРЭЬАРЬУЪБЮХБЪУЫЦМПЬСАУПХЫ
УАЫЬШАЬПЙАЙЫЦПЙЩАЙЖБАЦЖКЬЭЯЫБМЖБАШБЭБСЕУРРХСЩЫБЩЫЪУЫП

   (b) Расшифровать текст:

ПЦЩЦЩЖПУХЩОЦХЙФСЦЦЦЯЙЯУЩИТЧЫЬЕЗШНЬВСРЕЦНЧТЪЧПТХЩКИХКЦНЗТЩЪПЕЖГСО
РПТРЛОЧЯШЧЗЖЦЪОНЯУТТОРЪЫВНЧТЫМЪЦШЫОМТКРСКЖЧШТИМЪЦНТФРЩЦЕСЩТТЖОШЦ
ЖЕСЦЛЧЮМУЩЧМФЦЪМЯСРТСВЗЦЩЦКЖЦУАКТФЧЙНЙЧЫЦЩММКЦВРХЦРИЙЩЫСВИЦФХЕИП
ЧЙФАЖТМОЦНХЙЙМЦЙЧТТФХЙЮЕДРРКЗЦКТНТФЩЦНМТЦЦЯТШЦЦЕПЩРУНТКЦФФПЩУТЯФ
КХЯВСЦПИНМЯЪТПЯЪФЬВУЯНЬЩХЪШЯЖЩШГЫДОШРЫИЩУЦУРЬЪНЕВИФШЖКЯНХТДИШРУЛ
ЗЦМММФРМЙПМЪКТВЖШНРЮТЛМХПМЪГЭЕУЮЦЖМТХЖЩВЬДЧТЗРНЩЦЩХФЦЦНМЯЪТЮЦНЙЙ
ЮТШЦИЕЬТРСВЖГШЖИЗЦЩУЛИНХФИЯЧШТЯТПЛПОМУККТЧЫЗФЙКЧТИСКФХОТШРЦЩХХН
ЕВИНЩПЕЕРКХВТШНСЮЧШЛХЗМНЩТЮОРМФШЗУРСЛЗФРУЛИЦМСЛНЧНФВОУММКТСЙИБЙЩ
УМКЬРТТЮЙУРРВКЩЦЕЛВЧНФВЗШГЛРЦЩХЧМТФРФЕЦНЩАТПЦЧХМЙНПЛЕЦШТБТКХЙОО
ПУМКМЩУТЯМФШЫКТЩФТПФНУМБФЫЛСБФЫЛЧЯММНПКЙЦЙЩЛИРФТОЦДЧЙНЙФНСЕЦДШЛА
ТКЦФЗТЪЦФШНФЦЗЗТХЯМПАЩМПЙЙХЦЫВСДХЙЯЯЛЦИКЯФЦЕНЛЦФМЛЕШЪХЩОЧЫЗФЙКЫХ
ЗЛУНРРХКНХВПГФЖЕИЦФЩЮЯУЦМДЕГУЕИЗЦМФЕЦДЪЙЮЛУЦЬБАРПЦРПЫЧЕВЛЪНЕКЙМЦ
ЕНПЩЙЯБТЛЦФЛИРПРВФПЙЯКИЦШТАЙЫУТЯОФЦЧБПЩДУРЗЯНЖНЛКНХВПРУХБТУЛУИЦН
ОТЙОШЩЙКХТППЛСФРЗЕУШРЭРФРКХЩФЩЩОГМТФСВЦНЧЙНАТТТВЦНЙЙБЙУЦИЛЦЦСИВЖ
ЫАОЕОЦЪТНЧЖАЖЮФРХТЮМОНЦРКХНЛДСЦЙПЕХНШИУЧФЦПЛИНЮОЛРЫЦСКЙКНХПРЦЦЦЯ
ЙЯУУРЗЯНЖРЖРМЕИЗЦЧФЕЦХЫВМЙШНРВСЫЧТАТМГМКЙХЭТБСЫОИШХТШЯЯЦДРХПМХЫЦ
ЯТХНЖВХЪПОНМЯУУРЗЯНЖФЦЦОЦШУШНКБЙХНХЗЛУМРШЦНЙКВСРФМКХКМАЮЙЪКТВНЧЦ
УЕФЫНРМТЪЦРЛЕШБХЩОЙНПЛЕЦШТБТКЫХИЧАСШВПДМРНЬУФЯОЙЛЦЕИЗЦШТБМНФХПФГ
НУНМЪНПЕХМНРЗИЧЦЧГМХНРРЦШЦЖВЫНШРРИШНСВЙПКЦНУЦЩРЛЦШРРФЦЦЩСЕРЩМЙИЙ
ФШИЮЯУЦЦЗЛЪДХЛЦЧШЙБПЛНРЛНЯНХПМХЦИВПЪДЕШПЦХЙФЙЛЦИЯЙФЦПЛИГНОДЫТРИЛ
ЫНШМТТПРСЕЛЙГСЗФГУМОЦЦУЕВПЦСХЗЦНШЦЩВЧШМКЙЩУМТПНЙЧТМРХЙООЦУАЗТАЪТ
СТКЩЖЕСЦФМММКЦРЕ

2. Разложить на множители числа:

   (a) 388807381579411911638309212219

(b) 1438601044512977781401970662471248875654336042285474626548237

(c) 19258868812095428070917606006323762882526576847956714717682129051329234091325932723117913 91

(d) 167302796445888778641552496454205853705357870607063862996767232760318040383598706143778455579669197276448380585351618480 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 5417837479804743473736653301160929159326013265467862368074099761281876048959 9$
   - $e = 5$

   Сообщение:

   - $M = 5405371008949707553887520353022491493229158179181167160733315762624407536512$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 254198852754716069176832178903308212541$
   - $q = 203441725016582491004681336558773860629$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 258360756946787506601994074221341242625219205106772677457749268579196215978 78$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 140967488194727671098140122559958713869$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 125156948390936012832677396847586964083$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 32236440209299251048547036747124629 8607$
   - $g = 31614688294725250408575415457041806 2464$
   - $y = 16958490710553112890742768527487048 2492$

   Секретный ключ:

   - $x = 15641977738851940700456225650134511 0912$

   Сообщение:

   - $M = 13539108789688313376344271897486459505 4$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 14418480274979618531980841787086807 4061$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 29347402663628783625161117262853195 4497$
   - $g = 19820092555832568400043857069124116 5055$
   - $y = 14022365535431543030781975994486647 3463$

   Сообщение:

   - $M = 28398229872099340269031517673272496 5772$

   Подпись:

   - $a = 13966406547896872701568578246242147 8735$
   - $b = 61126573387443359735387377040190718 482$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 719$
- $g = 65$
- $y = 234$

Сообщение:

- $M = 289$

Использовать следующий случайный параметр для создания подписи:

- $k = 397$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 2x - 15$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 18

1. (a) Расшифровать текст:

ЕЕЕГИБОДЗЯБЙБМЗЩОКЛЗКСККУБЙШЛЗКСКЙАДНТДЛЗДЙПМГЭКЕЙДЖКЮЙДЖЖЙБЗШГЛ
КЗКВДОШНУОКЭПАБОНЭБАЙКЕАБЮПФЖКЪКОЮБУЗУОКАКЭБЗКЯКМНЖКЕЖМБЛКНОДЙБА
ЗБЖКДУОКЮБМКОЙКБЯКЛМБЮКНСКАДОБЗШНОЮКЙБГИБАЗДОЮЧНЗОШЮКЕНЖКАЗКНЮКЭ
КВАБЙДЭБАЙЧСББВДОБЗБЕЯБЙБМЗЛКЖУЗЯКАКЮПЪНЮДАКИЙБАКЮБМУДЮКНОДЛКНИК
ОМДИЛКНИКОМДИНЖГЗКЙКЭЩОКИИЧБХБПНЛББИЛКОКЗЖКЮОШЛМКФПЖКИЙБЛКВЗКЮОШ
ЙУФЖПУЪНБЯКАЙПИБЙЭПАБОЮКБЙЙЧЕНКЮБООЧИКВБФШЙИАОШЮБМЙЧБНЮБАБЙДКЭБГ
АБЗШЙДЖБЛПЯУБЮБДКЭБЯКЮКЕНЖБОБЛБМШЛКЖИБНОШЛКАДКОАКСЙДЛКФБЗЙЖЮМОДМ
ПИЙБКОЮБАБЙЙПЪЯАБНЮБЗЩДУПВБСКГЕЙДУЗДНЙБОБМЛБЙДБИНОЗКВДАОШЙГЙУБЙЙ
КЯКЮМБИБЙДУДООБЗШЗБЯЖКНБЭБЛМБАНОЮДОУОКЙБЛМБИДЙПЗЮДОШНЙНКЮБОАКЗВБ
ЙНОЮКЮЮФДЕДИБОШОЖКБЮЗДЙДБЙНПАШЭПИКЪЮЙГЙУБЙЙЧЕУНПВБЭЧЗПЯБЙБМЗГНОЗ
ПЙБЯККАЙКЯКДГЯКМКАНЖДСУДЙКЮЙДЖКЮЛКИЙДОНАДМБЖОКМОИКВЙДОКЗНОКЯКДМП
ИЙКЯКНОМДУЖЮЯЗГБОКЮКИЖРОЙБКЙНОЗМННЛМФДЮОШИБЙКНПАШЭБДЮЙЖПГИДУЖКОК
МКЯКЙГЧЮЗЖПИКИДУНОКЛМБМЧЮЗИКЪМБУШАКЛКЗЙДОБЗШЙЧИДЮКЛМКНИДДЙМЮКПУД
ОБЗШЙЧИДГИБУЙДИДЖКОКМЧББНЗДДЙБКЭЗДУЗДЮЙБИУБЗКЮБЖНЮБАПХБЯКЮЮКБЙЙК
ИДНЖПННОЮБОКЛКЖМЕЙБЕИБМБКЭЙМПВДЮЗДНИБОЗДЮКНОШДЛМДМКАЙЧЕПИИБВАПОБ
ИНКЭМЗДНШДЛМКУДБЛМДЯЗФБЙЙЧБИБВАПДИДЖМКИБНИКЯКЯБЙБМЗЙБЭЧЗКЙДКАЙКЯ
КЮКБЙЙКЯКУБЗКЮБЖЖКЯАЮНБПНБЗДНШДЮНБИМГЙБНЗДЛКУФЖБУЪЯБЙБМЗДГЗКВДЗЮ
БНШИНЙКДЛМКНОМЙЙКЮУБИНКНОКЗКАБЗКОБЛБМШЯКНЛКАЛМКАКЗВЗКЙЙАЗБВДОМБФ
ДОШЖЖЙИАБЕНОЮКЮООШЛМКОДЮПИОБВЙДЖКЮЙНОПЛОБЗШЙКДЗДКЭКМКЙДОБЗШЙКЖВАЧ
ЕДГКЙЧСНЛКНКЭКЮДИББОНЮКЪЮЧЯКАПДЙБЮЧЯКАПАБЕНОЮДБЙНОПЛОБЗШЙКБЛМБАН
ОЮЗБОЭКЗББЙАБВАЧЙНЖКМБЕФББДНОМБЭЗБЙДБЙБЛМДОБЗАБЕНОЮДБКЭКМКЙДОБЗШ
ЙКБЭКЗББЮБМЙКДЭБГКЛНЙКДОЖЙУЙБИНКЭДМОШЯКЗКНЛКГЖКЙЙКИПЛКМАЖПОКБНОШ
ЙУДЙНИЗАФДСЛКУДЙПЯЛМЛКМХДЖЛМКАКЗВЗКЙКЭМХНШЖКИЙБДГЮКЗШОБКЭЦНЙДОШЙ
ИЮФБИЙБЙДБ

   (b) Расшифровать текст:

ЪНЧЦЫПЦЛНЫШШОХЕЛХЧОБМЩФЖШФЪОЦОПЦПЕЮЖЦКЙЕИУВИБЕНЦЬЫНТУЫЮСЪХЧДХРТЙ
АФЙЛИАССЧМГСЪФВЭЦМУРФСЛХЧЕЯЫРКШХФБЗЧИЙБЦОРРЗЯЮЛЯШТФЮЩШТФСЖУМДОЫЭ
МЮСЩВОЩЗГПИШРДЗЧЧИФЗТЦПЦСМЕЯЦЧУДИХОМЦУНЮСБМЪИТШММЩЬЫНПСТДЯЩЩФБЕМ
ЩЬВЦЛЭЙХДГСЦГСХЩЦЫРЙБЦПТЦШЖБИФЩХЭКУФСЭКХОЦПХТРЛАЛЪВКЮСКШАЕНОСТХХ
ДШОБЕФФНБДГЭНХСПВРЫФНЗЙДЕЦДОГФКОЪЖЕННМШИТЩИИСЯЛЬПЛМПЖЯДЦЙПСДЦИАЧ
ФЦИЙЕХЫШТАСЙФФБХРСХЭЫКЗФЫРЫОЖШОНСЖОЗЪВРАИЧЦТВЦЩРЖБЕЩЛЛДХКБМЭУНХТ
ДХРХТЧЕУЧЦАЮНЛРЖЫКЗФЫРЩФЖДИФЩСЫЪЬФКШРХБНДХЦСОЭСЩШТЮДНУЙЮЮСХЧЦЪНИ
ТЕТШИМЮФЦЧРЕУРИЦПНШЛУБФЪВЬХДШОСШЖЦЧТВУЦИТЩЗУФХЕОЩХТЧТШЛИЮСЛФРВУР
ЙТЕСКСЙАЛСРТЕЭННИЖТЦЗЙЩОКЧЖШХУОЪЖЗКЛФЫДГСМЪТНЦЦОТЦЧЦЖЪУЧОЕСЪТХВУ
ЦЧМЮТУЮСЪЕУЧРЫОГПЗБОЦЧТЭПШВМЫЕХФЖАЮШНИЮФРНЛЧЕНЦЙЬТЦЙТЧЛЪЛУШХШУИГ
ИРЭУШУНФИШЕЖЧАДХЫХНЕИТРЧЮЛХЛУЯЧРСТХРНЧЙЬЪЩШЧЧЙНЗЧЧЦЧФЖЫРЦИПДЛЧФЬ
ШОККТЯСЪЬЗШУЩОРЫСХОУБТМВЖОДНМПЫНЦТСШРКЧЦГИЯЩХХИУВМКЛЭЩКШТШЛИЖТШЛ
ИЫОПКФХФЪИЧЬХНХЙЕУХКФШЛЯЙТХСШОПВСЧКАВУРИЙЮДЦЙТВХДЩЖЫЗНШАДНТХТЩЛК

ЛЦШПГШТВУЦИХЭЙМБНЧИХВУБПРУПЫПШВЦБЛКУТХРКЧЙЦСХШЙГТНСХПДННЖДПЦЙТЮЦ
ЙЩЬЭЗЩРКЫХНТТЬСЪЛЪЭНЕШТХЮЩХЧЦЪНИЯЯХЦХТЮЗРСМЭНЦУБЕСКЧСШЦТФОБЫРСИБ
ДШФХВФРЗТЪОЦКЙСЛПШТВСУУТДХШЩЩВУНЦЖЮСЪЛЪЦИШЧМЯРНИХШХЦИФЫЪЪФЛАИАВС
ШФЪВХВФНУМХСФУТЦСФЙПЦСУУМЫДЪДЬЭТНШФАЗШЛМКЕЦПИЫХНТМЮСЩШМВУЦЧМЯЗКУ
ТЧЕХФСШЕРКПЫФДХТВЗДЧЦЮЦЛФЭЕЯФЛСКИФЗТЦТЦЧПЮПНМИЖХНТЗБЕЦЦМЮДННЧЯСУ
РЧБРШЧХЭКУТСШНТОРБДШНТЯЫКЗФЫРЧЦМАЦМОПЫШКБИЕЯНТЧЯУДДМХРЦИСЖНТТФПЛ
КУТХРЧСОЮЛХЛЩБХНСХАЛФОФДФЪШАДНТТФПЛКУТХРРТЙЮФХЛВХФНЙИЛРРЛХАСАЛСЫ
ЪНЦЙЪТУЮОЖЗНИОЖДЦПОЖБТФЦБУРЩФЧРРРЛДХКСЙЕТУЧЦПТЦЧЖБИСКЧЧННРОБРЧЦМ
ДСКЛЦБЕУТФПЛРИСБЕХЛСВЛЩШАЭС

2. Разложить на множители числа:

   (a) 830860697557287813427881651377

   (b) 9317715040093442192146021320267565461117113686186033288586 93

   (c) 889097998083963430684901178130912154360272014163286130161142204543678938854667010312230279

   (d) 230589329149258298216814518852931824827016196046997349154095126118539273354211399646643232833095419599456620159401174997 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 6364748585785081052027075722043402921473798707955686522993031352387947367 4253$
   - $e = 3$

   Сообщение:

   - $M = 1738327539357583624608066339244468484085260034158715583345284526093780298 1817$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 173408438766302886739785671877207474901$
   - $q = 216378739601854228907667913369394779519$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 298770146287578711956636890560081768011798671605195856620497017542247714188 89$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 166239234632603124897194643668482995329$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 10330096464196913367256213233198698727 8$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 303773066455062932000700892186460929831$
   - $g = 255016255397413897842906775208544019477$
   - $y = 901796287389162112727217732846797456 34$

   Секретный ключ:

   - $x = 285214039254651717329911617601416583 48$

   Сообщение:

   - $M = 422355904857640488795223189129055423 30$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 215036689319676808594603112855282891303$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 3047280304615178499252002655833628972 61$
- $g = 96473858310646872312061680089488033 12$
- $y = 19476329345144528045617048793070881 6654$

Сообщение:

- $M = 26370038008531652683003387644791579 8215$

Подпись:

- $a = 26997280989990360209469207465702620 9727$
- $b = 14162924525077543586304920421405878430$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 683$
- $g = 512$
- $y = 681$

Сообщение:

- $M = 181$

Использовать следующий случайный параметр для создания подписи:

- $k = 679$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 12x - 13$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 19

1. (a) Расшифровать текст:

ТЕФТЗТОТСХЖЙПАМЫСЦТЭЧВМЩФТРЧВОПЫЧОТЦТФЧВИФТРТЦИПЙРЧТИМСМЛЗТФТИХО
МЩКМЦЙПЙНСЙМРЙЕТПЙЙХФЙИХЦЖОТФРМЦАЙЙРЯУФМЙЩПМОЗТФТИХОМРЖТФТЦРОФЧП
АСЯЙСХУФТУЧХЦМПМРЯЖЯЙЩПММЛТФЙСЕЧФЗСЫМСПТХРЙФОЦАХУЧЦАРТНЬЙПРМРТЕЙ
ФИХОТНХПТЕТИЯУФМХЦСМЭУЧЗЫЙЖХОТЗТУФРИТФТЗЛСЙХЙСЕЯПХСЙЗТРСТУТЖХЙНХ
ЦЙУМЖМИСЯЕЯПМОТСХОМЙХПЙИЯЙКЙИСЙЖСТТЕСТЖПЙРЯЙЙЩПОФЧУСТНФЯХАВХЖЙПА
МЫЙИЖРТЗХПЙИТЖЦАЛРСТВМЛИПММОФМЫПРСЙУТРМСЧЦСТУТЦМЬЙХЧИФАФИМЕТЗУТЦ
МЬЙУФТОПЦОПЫТСОРТСЙЧХУЙЖЙЦЛЦЖТМРИТПЗТСТЗМРЕЙХТРОЧИХУЙЬМЬАИТЕФТЕЯ
СУМФЦТУТИТЕЧЩЦТЗТМЗПИМУЙЦФСИФЙМЫЕЦВЬОУЙЦФСИФЙМЫСЙУТЗЧЕМЗТХУТИМЖП
ИЯОТУФТУИЙЦЕФХОТЙИМЦЖХОТФЙЛХЖЙФОПМЕЙФИХОМЙТЗСМРЯУТИЮЙЩПМОТЖФЗРЙХ
ЦЙХЦЖЙССЯРЧОФЙУПЙСМРХПТЕТИЯХЖЙПАМЫТЦРЙССЙТЦХЦЖПСЙУФЙФЯЖКПТЕСЯЩХЖ
ТМЩРТПЙСМНСИЙПХТЕЮЙЩЦАХПТЕТИЧЕПЗТУТПЧЫСТООЖИФЧЗЧЖМИЙПЖХЧРФОЙУФРТ
УЙФЙИХТЕТНЫЙПТЖЙОУЦАРЧКМОТЖЖТТФЧКЙССЯЩИЧЕМСРМБЦТЕЯПУЙФЙИТЖТНОФЧП
УЧЗЫЙЖХОТЗТУФМХЦСМЭСХТОПМОПМСЙЛСУФТПЩТЦЙПРТПЫУФТЙЩЦАРМРТМЩСТТСМР
ЙСЦТЦЫХТОФЧКМПММТИМСМЛСМЩХЩЖЦМППТЬИАРТВЛЧЛИЧЖЯЩЖЦМПХЕПВМЧИФМПРЧК
МОУТЗТПТЖЙЬУОХУХПЙЗТТИСОТТСЛЬЦПХМЖЯУЧХЦМПМЛФЧОЧЛИЧУФТЫМЙХРЧЦМПМХ
АМТЦЕЙКПМЖТХУТПАЛТЖПХБЦТНРМСЧЦТВУФМЬУТФМППТЬИАМУТХООПЦЙРСТЦУФМЕП
МКВЭЙНХСТЫМРТЗПМЛЕЖМЦАРЙСТЦЖХОТНТУХСТХЦМООЖИФЧЗТЗПСЧЖЬМХАЧЖМИЙПЫ
ЦТХЖЙПАМЫХТРСТВСЙЕЯПТЕЙИСЯНХЦФМОСХЖТЙНЩФТРТНПТЬИМСЙРТЗЧХООЦАТЦФЛ
ЕТНСМОТЖЫЦТЕЯПТИЙПЦАУТИТКИЖЙЗТСЙХОТПАОТРМСЧЦМЧИТХЦТЖЙФХАЖЦТРЫЦТТ
СЛИЙФКСУТЖТФТЦМППТЬИАМТЦУФЖМПХЙЗТЖЯФЧЫЦАУТИЮЙЛКОТЖФЗЧЧХПЯЬПМЛИПМ
ЬЧРОФМОММЗТПТХРТЙЗТХЖЙПАМЫУТЙЩПХОТФЙЙМЖХОТФЙТЫЧЦМПХХСТЖРЙКИЧОФЧП
АСЯРМРЧКМОРМТХЦСТЖМЖЬМРМРЙССЙХОТПАОТРМСЧЦЦТРЧСЛИХЖЙПАМЫСЩТИМПХРЙ
КИЧМРМТСМХЦЭМПМХЦФМОХЙЗТОПЫММ

(b) Расшифровать текст:

ЬСНЗБПСМНУПМСПИЛРЫДРЙИУЙЦШНРИЛНЕННЪООЛБСКНЭРУИБРИРЙКОЗЛЕИМППЙНРО
ЦДЧЗБРЖБЭКТПЙОМСОВККФОСКАЛССМЗШИВРГШТОГПОУМПНЕЬЕЪИНЙИРОХЭНЩККМОЖ
ДМТТДНЕУЬУКЦЦОЗВСФССДШЦСПНЕССССПСТТТМЛМСОЪЦИННЗССЗРПИОИКРЛВИТРНЙХ
МПИРОУСИКВУЙССЕДДФУЬРБКУИКЙКОИКНТПХРГИТМРЖЕОЦПЛСТКДТЕТТТДЕПЖККРШ
ЛЮМЛЛОДБСКСМАИТПЗЦРПДТДПГШКФЕОДЗЕЗЖНГДФТИНЗИРРЗЖУЖНПНЖПБХМХПВЫЗН
ИУТЗРРОНТЪЙЛСНЕЖЛЗМЛЖПЗПИРРДЗХЭСЩДУЖЗДНОДУПДФУНХНТЙСЭБХЭНЪДЖППРФ
СЕИРЙСОЧПЗЕПЙПЪФЛЖХЙССОФЙСШТРАИЕСФБЛЖДРФСЕИННЗПКТИРПСФЗПЬПТНШПДК
КЛШЕТДКТЕНДРЙРЙНУЖНПЪИВУПССГЩКЙПЙИСНРЖВРКИПТГЗУМИХАИЕНЭФЙЙТЗКИКТ
РЦХПУУОИМИРМЛТПУСЛРРДКИОИЗАЮМОСНЕТЮЖТТСЕМПЬЖНРОСНЕЫЗНЙУМПЮГЛКРЯР
ОНДФНШЛЙЛСЗГНМОИМНЕИЛРГИКСФБСГЛКОСГСАГЦОЧНЫРЙККНХЕЕНЫРЬХРСУЕОДРП
ПВНРХООПЙКЬВНЗЛНИННЕМИУНФУОПЗИГСЗВСПБЪЗУООЕННСГЖДФГИТДТТТДНЕМПРЕ
УВЫННЦЗСПНРЖПТЗЕЖДКАСДВКГИУЬТТФТККИДФНФАИТСОЪФМЕПМЮКИГДФРОЫГРЬЙС
ТЖШЕДАИЗЛСПИТЛЗГЦЖМЭИЛГНРЛЛГНРБЛШЕОЛЛЦЕНЫФПНРЛЕТКРПИФЗПКЛНЫРРСГЕ
ТЧИОНРЛИДОТЖДЙТКЗРЛОПДЩИУТЗРРОНТЪЙЛКЖЕЖСФЗИППРЗПЛЕУЛСИВПХЕНЕУСИТ
ТЗЛЛРОДДОЖНКДСТТПНЕЙТЮРЕПЙПАЮМКРМЪЖНПЙСОЕШЛРЖМРЕРПБЭКСЖХФЫННОКЛУ
ПДКСИММОЪФМЬКФСВНФЫЦГИЖДХЭМТЫБЙВПНЕОУРСНПТРПСКНЗЗПЖЛПЗНЛОЕНЛИВЗР
ХЙОЖТЫЖВНКПЖНДНФУОТВСНПТЪЖМКМПИВЕПННИУТЗРТМЗКФЙГРБССИНОСЗИОООЖЧО
ЗРЖТФДДЖНЗРЗПБТНЕУЬИДРЙШЮРРЙЗЩССРРРОЗЖШЮМСНЕИГЦУЕОРХСНПНИШУДРХГО
РСУГЛННППЮТГСТТЮЛЮТЛЮНКМОЖДИПБТЪКДНПНПЛРРБЛЯСФНОЭККФРЖВКМРЬХИДУУ
ВКННИНКДЖПОИЗЗЯЩЗИХСЕДНЙЙЛОДРРОПДЕПЛЗДПЖЛЗЛИМДХЛОТДРРЗПЮЙЦИННЗМХ
ЛНХКФУЫПЧХЬКККЛОЕСНЗГЕТМЦМССНЗЛРФДЪЭЛХЦЫЖНКЦИДОПДППГГЪХЬПТЗЗФМФЫ
ЪУОСПЛЛЖЗСИЕЕНСЯНЫУКЯПНЗЛРЖРЙКЦШНГЪОГООМИТМЭРОЙЮРОСЪДЗГРООЛЛРЖИО
БСЕНХЗКФЖУМЮЦМКМЦУЕЕНЙЙЗПЗЛПБКЖДГЛЗМЛЙМРДМОЕДДФУЫКЖУФКЕМЦТНРВСЩВ
ГПЛОЗХПЛОДНЛРЖ

2. Разложить на множители числа:

(a) 660813777008434985656654693183

(b) 10121933527121915495901026404922427505322837880404942192009 41

(c) 935198495105678054478096717711756287909964105874966319532152582170542194705458357601125667

(d) 172722297263570978782313263680247938685180652112486277862168749082265193092670652871087231475077909246229906588758547515 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 65371462618972384683058394080981692432635487811897728957049928344637743096097$
- $e = 17$

Сообщение:

- $M = 55995580317971636377452776540943254342129110588070157035216100772360716856435$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 23535270068663689374331605804149812447 9$
- $q = 17614017647372837705236661590900765089 1$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 28724404073814967073795943913746385280298927226130163566954012891064748665 33$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 31237626324162345340191146262734459552 9$
- $e = 5$

Зашифрованное сообщение:

- $c = 94834470294834870520552361418285153 55$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 24061874368991503222852080043751360315 9$
   - $g = 22060576814170690600308392116191563440 7$
   - $y = 11851480317040652197378276940802116216 5$

   Секретный ключ:
   - $x = 23819858384486628887971244038139373599$

   Сообщение:
   - $M = 11185279588201564550004911262144616819 4$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 92106981196626680670179660970602205329$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 25039824995578016845337062333676303403 7$
   - $g = 19007853685553597796671127532280308888 0$
   - $y = 90139643167172563752275773821457027317$

   Сообщение:
   - $M = 95073847820275372769120098085979310613$

   Подпись:
   - $a = 20301463997462287330970285023371959148 3$
   - $b = 13576754829728297614862716821882793667 0$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 643$
   - $g = 83$
   - $y = 226$

   Сообщение:
   - $M = 622$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 509$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 11x - 13$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 20

1. (a) Расшифровать текст:

ЯБЪХАЙЫЪБФГЪЫЮБЧБХБЮПАБШДЯБЮСФЫШЧДЭЪЮБАДХШДШЮОЯХЫЧБЯХБССИБЕПЭЖЧЪ
АСЕЮЫЖХДХБГШАФЖГЦШБДГЩШАЫЫВБЧСЪШШХБЬДБГБЭШАГЮБХЖФЫЕБКШЕОГШГЯЫЫХЪ
ЕБХВБЮБАЭЭЕОЧЖЯШЛПВГЖДДЭЫЬЭБГБЮПЯБЦЮЫФОДБЯАБСВБЕЦЕПДИХДЕЮЫХБДЕПГ
ЪФБЬАЫЭВБЭЪЮДПЯАШЪФХАДЯЭЭЕОЧЖЯШЛПДЭЪЮШЯЖЖВГХЫЮДЮЫФОЕОДЗГЫЧШГЫЭБЯ
ДЗШЧБГЗШЧБГБХЫКШЯЭЭЩШАШЕДХЛЫЯЫШАГЮЯЫХШЧПЩШЖВГХЮСДПБАЫШЦБФЫХЮЫЧБД
ШЮШБГЖЩЫШЯБШФОЮБДКДЕЮЫХБЧЬДГБЭЕБЮЫШМШФЖЧШЕЭЭВБЬЧЖАЯБДЭХЖЕОВБЮЦШЛ
ПЫЧЕЫАЯБДЭХЖДЯБЪХАШЙАЩДЭБЮПЭБЪЧЖЯЮДЫДЭЪЮХВБЮЦБЮБДФБЦХШДЕПЖЮЫЙЯБЕ
ШДАХБЮЫЯАШЯЮБГШФЕЯБЫЖЯАЫКСЕБАЫХБГОЯАШЧБЮЩАБЧШГЩЕПЖИБХБДЕГБВГЫВШГ
ХБЬАШЖЧКШБАЫДХБСЛШСХОЭЖВЕЯБШСЦБЮБХБСЕБЕБДЭЪЮВЖЦКШХЖАШЮЖКЛШЮЫЕШФШ
БЕДЕЕПБЕАЫИДЯБЯЖЪФЮЦБХГШЯШААБЧВГЫФШЦАЖЕПЭЯЫЮБДШГЧЫСЦБДЖЧГОАЫВЖЦК

ШХЦБГПЭБЖДЯШИАЖЮДАШЕБЕХШКЮБАВБЪЧАБЯАШЭЕПДЧЮЯШААШФЖЧШЕВБЯЫЮБХАЫФЖ
ЧЖВГБЧБЮЩЕПЭЭАКЮЭЭЪАЕПХБДПЫЖЧШЕДЦГЫЛЭБЕГШВПШХХШЧПВБЙГДЕХБХЮЩШАЧЯ
БДЭХБСЪАШЛПЕОКШЯБАЭБАКЫЮШЦБХОФГБДЫЮЫЪБЭАЪГШЪЮЫДБЩЦЮЫЪГЧЫЮЫШЦБВШ
ВЮБЯВЖЛЭЖЫХОВЮЫЮЫДЮЖЛЬДЭЪЮВЖЦКШХДЭЭЫЯЕБЧЫЭЫЯХЧБИАБХШАЫШЯГДДЭЩЖЕШ
ФШДЭЪЭЖЭБЕБГЖСХГШФКШДЕХШЯАШГДДЭЪОХЮДЕГЭЮЯОКЭБЧАЩЧОБГШЮДВГЛЫХЮЖХБ
ГБАДЭЩЫХБГБАВЕЫЙБЕКШЦБЩЫХШЛПЕОАФШЮБЯДХШЕШЕГЫДЕЮШЕХДШЦБАХДШЕБЮПЭБ
ЕГЫЧЙЕПЕГЫЦБЧБЕЕБЦБФЕСЛЭБЕХШКЮШЯЖХБГБАКЕБЕОВПШЛПЩЫХЖСЭГБХПВЫЕСДП
ЯШГЕХШКЫАБЬБГШЮВБЧЖЯЮЧХЬВБВГБФЖШЯЫЯОВЫЕЕПДЕШЯЩШИБГБЛБВБЮШЕШЮЫБГШ
ЮЧХБГБАХБЕЪХЫЧШЮЫВЮЖСЮБЛЧПДВЖДЕЫЮЫДПЫДШЮЫХБГБАДЕЮЭЮШХЕПЧВБИХЮЫХЕ
ПБГШЮЭЮСАЖЮГЪЭЮСАЖЮЧГЖЦБЬЯИАЖЮЭГОЮБЯЫДЭЪЮХБГБАЖАШЕФГЕХБГБАКШЯЕГЫ
ДЕЮШЕВЫЕЕПДВЧЮПСЮЖКЛШГЪАВЫЕПДЩЫХБЬЭГБХПСЕЯКЕБФБЦЧДЕЭЭБХЭЮЯОЙЭДЭЪ
ЭЪЕШЬЮЫХ

(b) Расшифровать текст:
ЩРМСЪЫЦМЖЬЦУУТБЮАРЖГЧССХМГЧЖВДАСГЩЭГЙГПЗОТГЩГДНКИЮУУБЦЪУКАКЪЯНУМ
ЩАЖОТШАЬГПГФКИСЪАЭГПСЮУАСВАИММЬЮКЛСЭЬУЛЖЖДРЖЖРККЙМЬЬУКСЗНСОАЭФТМ
ЖВАЦРЖНЪЦЪСЪЦНЛЙЖЮЧСЬЯАГМЦМГЧЖТЦМЦЛМАЧОПЖГЪФОЙЩБУЙТЫЧТЖРЗЕЭИХГГР
ГЛБЪУЯСАЧКЖРГЭНЙЕГХУЯПШАФМПИЙТМРЯАТФЙЬЮАЦПЪЯТМЗГЦКЙРЕОГЖЖВАЗЛЧЖЯ
ХВМАЬНХЙЕЧМЛЙЖЬУЙАЯАЙЛЙЮАТМЦДВЗЖПЖОЗВТЕАИСХЧЧХЛТЮБРЦЙЮЪЦАЙЕЯАКХЧ
ЧРЪММЧСИТЗАХЩНВГНЙАЖДЗГСВАХЕПИЙКЛСРЫЦМРВАГСЦЪКРПУГЬХЗСЪЫСГФЪЮАПП
ЭРЬРТЖЭШДМЗЯХГЫЪЯТМНБАКЗСЪФКПЦЬЮХЪМЧЯУАСЦЭИМУГЭШХСГБХЖЕРЭЗПТЙЪГЖ
ЧЬЯЗЛУГЙЧМЖГЮЙАТЕЧЬРТЩФУОСКАЙЖПЖФЧМЖЕЧСАЪЕГПМРЖЧРГФЪКНЙХСДШРТЖДТ
МЖЭДБПЙЮАЧАЙАЪШБТААПЕУЪВКБТЕАЙИТЮШКЛХБАЧОМЗЧРРТЗЙЦПСЪРХЕЗГФУОМАГ
БМЕПФНЙЫЗАУЛУАЧСЛСЭИФОМЩФУОСГХУЖХЗАФЛМЯЪФМХЧДНЙЙЪФУАХЪДНЛХЗФФОМЩ
ФУОСГЫЛЖЛВЪУЛФЖГПЕПЧЬУРТЕАСХХИХУПЧЩВАЛТЦНПЛТЧЧТЛТДВУПЯДЭЦЪОИКРИТ
ЙЧОНФГХШЙМЧЭЦЪОЯЪКАЙАОСМКЭЯЪМИЭЭНПАЧДУАФЪЮФОМВЧОХЦГЪМАТАЪРМСЧЙКО
ЬВЪОВЙВОИМЖГВНРАИГКЯЛЖДУЙТБЬУБТДВНЛМБЭЗГЫЪВУКХААЗМРЕЩИМЖГВТЛЯЧЭЦ
ЪЙЧЯАПЦГЪРЛЙЖЬУЙАЯЪЪПЦЕЯНФМЖДУОММЧЦИМКЩФЖХГЬНЯЯАУАВФШАЫГСЪЯЙЙУГД
УКХЗФСОАЭФТМЖВГРСЬАЧКПТЧЯНКСЭЧСМСЭБУЦПЭФЦВСВФРПАЪФТОХЖЬМЙМЖДУОМУ
ЬЛВТЮЭРГМЭЬЛВТШАСМХЗЪПЖСШЕРАЬЭГБМСЭФУЕЖЕДНЙМЖОТПЦВИНЬТМЧТЪИГФУЙА
ВНКВФИХЙОЧШАСЛИЕЕИМНЩЧТЬФВАШРФГЮСОАЭФТМЖВБХМХВЕРПАГЦКЙХСЪЧЖЩГЯБИ
ТДАЭЙЖЖЦШРФГУАЙТДВКИФЖЯУГХГЭТФЙГГЗГЭААЗГФНЪТЩПЭБФМКЪЭЧГЖНЪЪСКЪБУ
ВХЧЧЛЖРЩНЪЛМЪЮУПЙВЪЭЖФГЬУГТЬЧХМХЭЭУЛЙДАЙАМЫЯУНФГГТСЖНЪКППЪУКВМЧШ
ТМЖРБРЩЖАЬНЕУГЦПСХЗАЗМХЪЯГЧМКУКОЙШЮХЪМЧЯУАСДАЭЙТЯАРМУЕЧПОХВАИМПИ
ХИВЙЗАРЪОГЙЧМУГГЧАПЪЯЖЩПДЮЧЛМЯФЬГХЗОТГИЧЯНУУГУКВЗЕЖФГЦЕЭКИХВЦХМЖ
ЭЙХСРВИКАЖЩВШБЕЪЭЦМЕМЬТБПЭЫЦИТЮБУОТЩНМЙПЭБУЯЙЫЭКЗСЧГЧОЙМЕСОАЭФТМ
ЖВЪЦНЧШЭЦЪМГГЧЛТЧЪРПАЧПЧСХБЕГКМВЕЧСФЬЦРПУЕЪЧЛЯЮШКЛХЯЪОБТА

2. Разложить на множители числа:

(a) 75799818047424354822525028837 3

(b) 958169612492706475469270383542133109507061283653790638350201

(c) 92093684055305940414621002701850509150045274376136501550403637314719705828935921955047651 1

(d) 19621789487373679924111822494305215898046307346021318735983587132018375249136427513689010754451695496708120748181836518 21

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 55121668697283092242355012657548727384653062891843647192869546399657094698247$
- $e = 5$

Сообщение:

- $M = 12359034989700165275014937960146717748885308168194617797813779708597168038119$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 29710334779757257486743258822043769 1607$
- $q = 25811996002841857021844016356156331976 1$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 689302334425978018182594944663456000421334663357067921503874318212265885196 40$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 25162037174589567771792160712634674 4707$
- $e = 5$

Зашифрованное сообщение:

- $c = 539020074454275521752800632551590729 93$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 18241231150419374356093888463423574 3163$
- $g = 16828943473442420625485091015886863 4751$
- $y = 13466806119111623580846572739384464 3473$

Секретный ключ:

- $x = 48241833817372071222006566315558335219$

Сообщение:

- $M = 30896668689371387792975836834991244712$

Использовать следующий случайный параметр для создания подписи:

- $k = 14451381765255009815517136174267621 3901$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 33816755115213735164487549222117142 7753$
- $g = 88686371526586513987717446703078150398$
- $y = 93109895127366120797260154309808736 3$

Сообщение:

- $M = 42025655893046756078106891928619350793$

Подпись:

- $a = 14428620066263644013928978825941360 7464$
- $b = 11958391712701127050763073314256992 4697$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 983$
- $g = 58$
- $y = 89$

Сообщение:

- $M = 648$

Использовать следующий случайный параметр для создания подписи:

- $k = 39$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 5x - 3$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 21

1. (a) Расшифровать текст:

ЗСОЙИРФИМЙИЪФСХТУЕЛХЯЕФЕХБУЯПЦЛКЕСОЯХИЖСХСЕРСЕХНСМРЗИЙЗИЪХСЗИОСС
ДЭФРЛХЯЗСКЕСОЛХИПРИТУИЙЗИНРЙРЛРФСИЗЛРИРРЮМХНРИЪРРСФПЛОСМЗИЕЦЫНСБ
СНСХСУСМИЬИЦХУСПХНПЦЪЛХИОЯРСДИФТСНСЛОФРИЕИУЛОФПСПЦФИДИЛЕССДУЙОЪХ
СЕФИФСПРСБФОЦЪЛЕЫИИФДЮОСТЦФХСИФРСЕЛЗИРЛИПУЯЛЕРСЕРЖОЗИОФКЗЦПЪЛЕСФ
ХЛБХСРПИРХСРЗСУСЖЦЛНКОСФЯРИЦФТИОИЬИСТСПРЛХЯФЛТУЛЗХЛЕФИДПЮПСОЪОЛФ
ИУЗЩРЫЛФОЛЫНСПДЮОЛЦХСПОИРЮРИТУЛПИХРЮПСДУКСПЪФЪИУИКЗЕСЪЦХЛОЛФЯПЮЕ
ДОЛЙРИМНУИТСФХЛХНЙИТСЗЕОФХРСМТЦЖЪИЕЦКЗИФЯПЮТИУИПИРЛОЛОСЫЗИМТСФНС
УСФХЛФННСЕСМЛШКТУЖОЛТСХСУСТОЛЕСМЦФОЦЙОЛЕСФХЛДУЗХСЖСНКНТСФХЕОИРРС
ЖСТЦЖЪИЕЮПЕНСПИРЗРХЮЦЕЛЗИОЪХСДОЖСЗУДСОХОЛЕСФХЛПЬЛНРФТУЛЕИКЫИЖСПИ
РТУЛРЛПОЛННТУЛЗЕСУРСЖСЕУИПИРЬЛНПЮСХТУЕЛОЛФЯЗОИИФХОСФПИУНХЯФПЮТУЛ
ДОЛЙЛОЛФЯНЖСУСЗНЦЖЗИТСФОСЕПДСУСЗХСЖСНСПИРЗРХРШСЗЛОФФЛОЯРЮМСХУЗЛЗ
ЦЬЛМРФСИЗЛРИРЛИНФПСКЕРЩЦПЮДЮОЛСФХРСЕОИРЮНУЦОЯРЮПЛРЕСТУСФНХСИЗИХП
ЬЛНСХЕИЪОЖУСПСЖОФРСЖСФЦЗУИЕНЦПФСФЕСИБШСКБЫНСБЕЗУЦЖХСОТЖЦФУСЕСНУЦ
ЙЛОРФФЦЙФРСБДУРЯБЕЮШСЗЛДИФСЕНЦПФНКОПРИЦФФХЮМЕШПЛФХУЕСХЦЙСХИДИДЦЗ
ИХДРЛФХЕСИБШСКБЫНСБЕЮЫИОЛКНЛДЛХНЛЛХУИДСЕОЪХСДСХЕИОЛПИРНЛШРЪОЯРЛН
ЦЦЕЛЗСЧЛЩИУФСОЗХЮТУИНУХЛОЛДУРЯЕШПЛФХУТСЕИОПИРНПЛСУЦФЕИОЯЛЪСХПИРР
ИСХФХЕОТСЖСЕУЛЕТУСФИДЕСХХИДИЛЖСФЦЗУИЕНЦПЛКСЖРЗЕТСОЮПЖСФТСЗЛЕОЗЮН
СЪИПАХСЕФИНСРЪЛХФНЛДЛХНЫЖСПТСИШОКРПЛЪИУИКТХЯПЛРЦХПЮТУЛЫОЛНЗСПЛНЦ
УНССФЕИЬИРРСПЦЕШПЛФХУСФХЕЛОПИРТУЛНУЦОИЛТСЫИОСДСПРИЗСОСЙЛХЯСРХСХЪ
ФЙИЕСУСХЛОФСДЭЕЛЕПРИЪХСИЖСЕЮФСНСДОЖСУСЗЛБРИНСЖЗПИРТУЛРХЯЪХССРЕИО
ИОСХЕИФХЛПИРЕСФХУСЖШСКБЫНЦНФИДИТУЛЕИФХЛЪХСАХСКРЪ

   (b) Расшифровать текст:

ПОЮЧЖСВХЧХФИСУЯЗТЙЦЮЖОШШЖКШШМЗДЛЧУИОЫПШРЛЙЬХБКРЧЦЭИЛШЦЮЬЕЪККРЕТУ
ЖДЫШУЛПЕЪШЯИБШНАНОХЗКИЕЖКЖИМЫИЙКЛХЬБХЬДЧЗДЫКЧЗДЫШУЬСВЫХБОИРХЮДЦИ
ФЙЦСЪКИУУЮСРХЫЪКЕЪТИЗЭУУРРМРВИЭДЛЗФУЪОКХУАУИШМЙИЛХЮЮЦЖЮТЗИКЪСЖЕС
ЯХЮЪУЬРФОВХЦБОИГШЛЕЕЭЛЭИНЪТИООЯШЛИЛПНКИЛХТИИРТПДЗИЪКЪСЛТМЖИНЪУЮО
ЮОУИЮТЮЧЫСОПРЭИЛЫСЖСЮФЪЗХЕШЗАЖЛЪШЛЯНШНПЕИЮКДЯНХПЗЕПЫСЗИМАФЙЛКФТБ
БГЭКЪЩЫФЫЮТИШНИООЯЖЬУОЩРЗЗКЩУЛСЛЧТМОСЙУИОЫПШРЦЮПНКЛЛХЫМЕЫЬХФЖНАР
БСЧАЧБОСЩКЯЗУАЛКРЫЩНКХОШЖЕЛРЧРМРОФХДСБТМЗДРУКЖРЫТРБЩНТЦРФТЪАОСДХ
ТБКНХЪЪЮЛЮЧЙЮЙДШЫЫДЭШЬСЙЭШКФКХОГУЕЮЧХРИЪЦБОЬЪАВЛЗСУЙСВИОЕОЫЦРЮХТ
ХТЗЕЗРРЖЦВЪЧЙИТЙКЬССХРХРООАДТОЭЛЮРИЪКЕСГАЙЮУЖЯБКСТУРЗДНЫИЗЕОЮПДЛ
ЦЪНЦХООАДЕНЙПЪИДЪАВПОЦЗЖЯКЬУЬОУЬУКХИЮЗЗИЙЬХБФТПЭБМКЬШЬЪЕПШЖЗНХСБ
ТРХЖБХБИРРИРЪЙЗФКЪПЗХОЭУВДЕШАЕЛКЭШИРЫЩНЪЦКПСБДЫШУЖТИЮТЗЕОЭАБДУЪЧ
ЗЕЩХПБЖРТЖПЮСЩУЛУЕШНЙЕНЫЙМЫНЫНЗЙИСРБПЕЪШЭИРУНЫТЛЫЧЪЖРЫСКИЛЫФЛЯВШ
УЭНУЬРЗХПЫФДЮЛПТБКПЫХЮНЕПНКЛЛХЫЭСЛРУРИРЪКДЕОЩХГИНЧУЖИЦЫТБФЧТМДЛЛ
ЫЙГПОЬХБЪЛХРГЕЫЮУГСМАНГУУЯУЕЦБТХЮЖУЖКЭУОЭЦИОТХРКФГЭКЪЩМХУЭЛНХМЖЛ
ХЬУЫИЛЩКЖНВИЖЗУНЫСМЗЕЭКЫРИЪЪЗЗИПЭЮМСАФЮУЕПУАЕОЕКДФНХСЫПЕЮЧЮЕИФЖМ
ЕЫОУЙРЫЦШКОЫЕЬЛСТЭКЪЦЮШУСЗЕЦФЙЛНШЖФООЩКЖЗОПУДЯНЫИЙЦБЫТЗПОЦЗЗЙТИО
КНЗШКЕЦТХЪЗРЕЮПЗОЬЧУКООПНЮЖОЮШЙСВЫЦЛЯТЫЧРФООХЛЛЛЮБЫХОЭУИОИПШЧЦСШ
ШЯОИПУКХЬПУЭРУЩНЖЦТАЧЙСЙЧЖФОГЫЧЗЕСТРЫХЕШКЯНУХЗЮОЕШЦЮДВТМЛЛВЪЭМЗЕ
ЭКЫРЮЮПГОПЫЖЗОЬЕУВЗОЭУЬИМХСЗФПЖНОЗЕЭКЫИНЙЖЗОСЫЙЖСГЫЖФХЬЫЦЛРОПРЮР
УЪЙЗУОРКЮФЛХТЗЪНПЦЛУЕДСЗРВЫРЬИДЫПАЮВШФЙЛСАЧКХВХКЪЦНЯУЫЬИЧУЫХОЫТЫ
ПЕЮЧЮДЫШЙЗНЗЯКДЯСЯЗЗПИЮНДЯНЫИЗТРЫЧБЕУСКВФТПНИУВХЧЮОЬЮЧЫРВЮПЗМСШШ
РМИЩКДЕКЭСЖИПЭУИЦСЧЗФЗНЪАВПНТФМЖЧТЗФПИЬХБНЗЬУДНОПТБНГЭНЖИВЪУЖЛКЯ
УЕРЕЪКЫФТЭКЛЛЛЮНГЦТЭШАЕИ

2. Разложить на множители числа:

   (a) 417248341337466934383971292539

   (b) 7775476572753243151348020108368241036662329977604778069954 87

   (c) 630759512399794494662714081927391073031854819138490878880673736008620250017089961099649331

   (d) 2340601878729368619313460230448728638145644213480859428540253375736579325206139583442579914670179450290119809687698136199

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 70410889513511539595996087294911018913044659516844243356253369160885438117737$
   - $e = 5$

Сообщение:

- $M = 10301100869929289876443528575023156681197323926292763268601953371614492925055$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 221615649139051075625052857039382999677$
- $q = 209219528523702990363976366927973917937$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 234580580660106499393468091089596588095252056825982227694408335335784911823 94$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 14198601105791322362226926242116214231539$
- $e = 5$

Зашифрованное сообщение:

- $c = 95838327207042856974047528204142737729$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 319695957344698961723304747169834915121$
- $g = 119504086204941264212664556031994918563$
- $y = 122914019967878797172819312549624236580$

Секретный ключ:

- $x = 127002468553304478818104597645359665542$

Сообщение:

- $M = 190263898018958656485863381799974977 37$

Использовать следующий случайный параметр для создания подписи:

- $k = 385881477991909097364835761509674694 93$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 271025278219434500529671369305580659801$
- $g = 222822851043856768295952617629442242 68$
- $y = 240767193734344466432207873966638953258$

Сообщение:

- $M = 571146183374944560184488472845360226 35$

Подпись:

- $a = 237521797812764980245589969578056645571$
- $b = 270007649468618407119336411108807950397$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 907$
- $g = 37$
- $y = 568$

Сообщение:

- $M = 296$

Использовать следующий случайный параметр для создания подписи:

- $k = 341$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 13x - 8$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 22

1. (a) Расшифровать текст:

КФОЦЦЪСОЬСШОЪДСЧОЭЧЯТНЯЦЫЯПГСОЯФЫЪЦЦФШЫЪЬЯГСЩФШНЗЧФШЯЫЪЮЬСНЧСЩЪЮ
ОСГЧЭЩСПЪРЪОЩФСШГЮЪЦЦЪАФВСЬФРОЪЬЩФЩЩФОЦЦЯКЭЧЯТНЯЦЫЯПГСОЯОЭЮЯЫЮИФ
ЩФЦЦФБЫЪЬЯГСЩФХЪЮЩСПЪЫЬФЩЮИЩСШЪПЦЦФШТСЪНЬУЪШОЪУЬУФЧШЪХРЪЫЬЪЭГФЦР
ОЪЬЩФЩФЪАФВСЬЪРФЩЫЪЕТСЩЭШЪУОЩВСШШСТРЯЮСШЦЦОЭССПЪЮЪОЬФЕФУЧЪРСХЭЦФ
ЯШСЬЕОЧСЩЗЦЦФШЪНЬУЪШЙЮЪЮЭШЗХЪАФВСЬФРОЪЬЩФЩРЬЯТСЭЦФЫФЬЯСЮЭНЯЩЮЪОЕ
ФЦШФЫЬФЩФШСЮЪЮПЧОЩЪПЪУЧЪРСЫЪРЬЦФДЯНЯЧЬДРИФЫЪЧЮФЩЯРСЩСПЪЮГСПЪЫЬЪФ
УЪДЧЮЦЭЮЬЩЩРЬЯТНФЩГСШЪЩЪЭЩЪОЩСЭЧФЩСЩФУШСЩСФЧФЫЪЦЬХЩСХШСЬСЩПЩЯЭЩЪ
ШФЫЬСЭЮЯЫЩЪШШЧЪРЯДФФНЗЧПЧЯНЪЦЪЪЭЦЪЬНЧСЩЭЧЪОШФПОЬРСХЭЦЪПЪЪАФВСЬФЭ
ТЬЪШЩГЧЭОЪСЪЫЬОРЩФСЬЭЭЦУЧЦЦЩГЧЪЭИШЪСУЩЦЪШЭЮОЪЭЫЯПГСОЗШОЭЮСЫФОЪОЬ
СШНЯЬЩЦЦЫЬФОУЮФФНСЧЪПЪЬЭЦЪХЦЬСЫЪЭЮФЪЩШСЩЯУЩЧФЫЪЕРФЧЭЦУЧГЮЪЮЯЧЯЫФ
ЧЪДРИЫЬОРЩСЫЪЭЪОСЭЮФЧЭЫЬФЩЮИЪЮЭШЪУОЩВЩЪГЮЪНСЧЪПЪЬЭЦЯКЦЬСЫЪЭЮИУЕФ
ЕЧЫЬЪЮФОЯУЧЪРСРЪЫЪЭЧСРЩСХЦЬХЩЪЭЮФЩЦЪЩСВЭЪЭЧЧЭФЩШЪСПЪПСЩСЬЧЦЪЮЪЬЗ
ХШЪПУЭОФРСЮСЧИЭЮОЪОЮИШЪСЯЭСЬРФСОЪОЬСШНСРЭЮОСЩЩЪХЪЬСЩНЯЬПЭЦЪХЪЭРЗ
ЭЮЬЪПФХЭЮЬФЦОУЧЭЪЭЮЪЧЬЮЦЬЗЮЪСЫФЭИШЪФЭЮЧГФЮЮИСПЪОЭЧЯБЩУЫЬЪЭОДСПЪЫ
ЬСОЪЭБЪРФЮСЧИЭЮОЦЪЭЮСЧИЩЪЫЫЪЬЕФЦПЬФЩСОЦЪНЗУШСДЩЩЪПЪОЩЗЩСДЩСШЭШЮ
СЩФФФОЪДСРДСПЪОЭЩЪДСЩФЭУЧЪРССШЭЧЯТНЪКЩСРЪУОЪЧСЩЩЗСФРЪЧПЯЫЬФЭПФЫЬ
ЪЮФОЩЗСЪНЖЭЩФЮИФШСКГСЭЮИЪЩЗХЫЬЫЪЬЕФЦПЬФЩСОЩБЪРФЧЭЩЭЧЯТНСОЪЬСЩНЯЬ
ПСЪЮЩГЧЪЦЮНЬЫЬЪДЧЪПЪПЪРРЪАСОЬЧЩЗЩСДЩСПЪПЪРОЦЪЮЪЬЪСГФЭЧЪЪЩФУПЪЬЪР
ЪЮЧЯГФЧЭФЭЮЪХЫЬЬЗЯТСОЦЪШЩРЯШЪКЩСОЧЧЭЭЧЗДЩЪЪЮЫСЬСНСТГФЦЪОГЮЪЪЩНЗЧ
ЯЫЯПГСООЭЧЪНЪРСФЭЩФШОШСЭЮССУРФЧОНСЧЪПЪЬЭЦЯКЦЬСЫЪЭЮИОЦЪСХЫЬСТРСЩБ
ЪРФЧЭЪЩЩЭЧЯТНСГЮЪЦЭСЮЭРЪСПЪЫЪОСРСЩФЮЪШЪПЯЮЯЮЪЩЫЬСЬОЧЭОЪСГЮСЩФСФЭ
ЦУЧШЩСЭЯЬЪОЪГЮЪЮЗЮСЫСЬИЭЦТСДИЭСНСОЪЫЬОРЩФСБЪЮСЧНЗЧЪЫЬЪРЪЧТЮИЦЦЩГ
ЧФЪНЖЭЩФЮИШЪКЭОУИЭШЬИСХФОЩЪОЩЪХЮ

   (b) Расшифровать текст:

ЛЛЩНЗИШКНФКФЪЙЗОИЩИУШТЮФЕГСЬЛЛССРЭСГЩЭМЛСРШЗЕОИЮБПГЦЦЙИВУЯОСЛУАК
ПЧШЬЭЮГФЩКЕЗЛЪННОЙЬЭЮЛУЫБФКФЩШНОЭЯКЕВБЯОЕЛЛЫЙЫЕЧАБЦКЗШЯЦСЦЙЮСЗИЮ
ОЛЛОЯШФПФСКРИНГЮХВХЩБРНЛЯЖСЛВШКЪЕСЬЮИКОГГТЕЦЩДЕТФАНПЫПЫЭУВРЬОСРФ
ЪЮЮДЛЮВОИТЙАССШЬЛПТУБЪССКБИЮРНЬФОИЧКЖЙДБЧЛССИЬДПКФЪЙХМЧАМЛКТЫПЙЕ
УПЧООШТЧШНЛЯЛЕШОДБОУДЫКЪЬЗЮКФИСЯЙТОЧАБОЬОШМИПРЬГФНЩЩЯУИУУЮТОЮУЗЗ
ЕСАШФВФЦМФПФЮВИНОРБЪЕЦЬИПЫЧЬБЗИУЦЗЛСВРЯССШЦЙСЙФШКООЧЪКЕРИУНИЛФЮГ
ЖОИЮДЕОТЦЙЦВЮУЕСПЧЫКФТОЪМЯИИЫКЕНЦХЗЛВСЕЕФЕСЭКЗЛЛЫБИИНЫЗФЕДЦННЛДЕ
ДХЕСКЙСРФТДХЕСЦИСИРХЗССВПЗЖОЧШЗСНУЬНПОШЮБОИУЫБЙНФЯОЯНЮЦССТУЬФИНО
ЧАССЛЩБАТФАЮИЧЛЮВЛВЛАЮПОЛЪЮССХЬИЛНУЦДДЫСЯУФТСЦЮФЧЧАЗЛВЧЬЮИРЮУЙРО
ТЫКЖОСЦОНОИЙСПИУБОЕБЛТЙСЙМЦГРИЭУЗСВЛЕБФКФЧЙЗРЩСКМДЛЫШЗОСЬВЛЛОПОБ
ШРУУХОРЮБФТВЫБЕИСЦНЯНЗЮННОПТЮСРЧЭКЕИУЫКББШМФНВЕЖБОКУЦИРКЦЙЗЯЦФЭМ
ЛЕЙЬЛСВСУЙЛИТБВЛКОЯООИУШКОЕУЦЙЦЧШЬАЦРРЦННЗСЬЙЛМНЕБПВБРГЗУТЩДДУУА
КЕТВРДРОИАЧЖОЧБАУЬШЙЙЫОШРБЪЛОЬЙЛВЙЬЗССШЬОСВОЫКЕТБЫЛУОРХОЗИЧЪДРЕЦ
ТЧТРФЗЪЕСКЩМЗОЧАДЪТФПКЖПЦЦЮИЛТЫБФВОТБХЬЧЯНЮНФЪЛИТЦЬИРДЦУДЪЕТЫПЗО
ЗЮКТОИЦЙРУДСКООИБИИЧУУНИЧЛАЮЛНФРОЮКФЫБЪНФРДРОИАЧДОЙТЗЕЕКЮКТОЦПЧФ
ЕУЬПДРШКЮЮДЩЮУЯЕЬУЗЮЕШЮДЗНЭАКЗЕСЩДФТЦЬНХНЦТДХЬХЬЯСЛФРЙСНЧУЙСКФЯА
ФМФАМЛРБФЭИСШЦУХОЗБИИНРЦЗЯИУБАРЮИЯБФЕУЬЭЮЛФРЖСПУГПДИЦЧОИСВЪПЙИРЦ
ЛСКСЬЙЛЛОЯШЛПФЖЗЛНЗЮХЛНЩШЖРИИЕБПНЛПЧЕЛФЮЙЫВЗЮДРОРХЗФЬУУНПЕЦАБОЬУ
УЯССРЬЙЕОЛЪКХПЦРДОИИШГРЬИЦАИЛОХКННРШБЖОЩЩКЙИСЦЮХЕСУЯЦВНЬМЮНЮЦЮФТ
ЦУОЛЛОЯШСНХЬОЦПОЩЯСЛФРПТОЧЭБЫНФЬОСШЛЩКХОРЫЭСЛЧЭКНЗБРОЯВОТУХОШЬМЙ
ЕЧАЮЦЮУТЙИСЭЯОЛЕТЦПРИМУЙЛЕТЫБЗРЩСЯУИУУЮЗОСФБРББЩКХПЦРДХЬЧТЗИЕЦУФ
ЛЛЧХЙЛМХЬНОЕКЬЮХЬУУНПОШЮЙПОЛФБОНОУЛУОЗЙОЯЕЯУЙИСРЬЗЯКФТЙИЙХЬ

2. Разложить на множители числа:

   (a) 70411897183166348380123496308 1

   (b) 834703337058646525911573437589745824460055318828123348787791

   (c) 92073055391453341706839997874594503943776884524900847412887628181502495991214112375967120 3

   (d) 125217876733078640916211787558047403689415406037782497023618976744682047900678558627358521924879847378950947756348919389 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 6364281711563517168769669479676000510801706281103199918715638912788621072333 9$
   - $e = 17$

   Сообщение:

   - $M = 45124406081631893740374834590525346215394902855681131902687019655088309069357$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 211303614871760382671219694120576614011$
   - $q = 178276110255651830782322757394436532401$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 19224912396433854343463933703246940591038123978620054859117016317251294943218$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 22235325386955129603828088322217213 0049$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 21436653570074296668834962480566966 23$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 22486725924358964736429434683056091184 9$
   - $g = 22340941145663466454809991652780286895 6$
   - $y = 86735602431970206058411323541216848 15$

   Секретный ключ:

   - $x = 20218654744118440077993957781336171551 2$

   Сообщение:

   - $M = 16948991779795619525507417026208759230 2$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 65428624378785952411963746554041841703$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 17693362877702861526388440284957092818 7$
   - $g = 80795081789341626377444191633044052248$
   - $y = 12008879444182586627652493029854746621 6$

   Сообщение:

   - $M = 17291977413754918352360576431189057449 3$

   Подпись:

   - $a = 14424056774006784765692743084823390952$
   - $b = 57308152207110143215028826024782485119$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 601$
- $g = 518$
- $y = 379$

Сообщение:

- $M = 478$

Использовать следующий случайный параметр для создания подписи:

- $k = 463$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 2x - 15$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 23

1. (a) Расшифровать текст:

ИЙЗЬЖЬЙЕГЖЕПВЖЕВЬИЙДЯНЬЫЩЬЗЯЖЬЗЫДЬХЕЙЩЕЗЯВЯИУДИЙЬЭУЕДЖЗЕПВЫВЯДД
ТАЗЫЖКИЙТМЩЬВЯБЕВЬЖДТМБЕГДЙБГЬЗВБЬАКБЮТЩВЫЕЗЕЪКДБЕДЬНЖЕЫЕПЬВБЮЖЬ
ЗЙТГЫЩЬЗГЕДЕШСЩЯВОЙЕИЬАОИЕШДЬАЫЕВЕЭЯЙЯЕИЙЩЯВЬЬЕЫДКГТИВУКЩЯЫЬЙУЯГ
ЖЬЗЙЗЯНКВЯНЕГБВЯНКЙБКИЙЗПВЬЬОЙЕЕДИЙЗКЫЕГГЕЪВЫЬЗЭЙУИДДЕЪМОЬЗЬЮГЯД
КЙКЫЩЬЗЯЕЙЩЕЗЯВЯИУЯЕДЩЕПВЩКШЕЗДКХЪЕИКЫЗТДЯЯГЖЬЗЙЗЯНИЯЫЬВЮИЩЕЯГЙК
ВЬЙЕГДЬИБЕВУБЕЖЗЯЫЩЕЗДТМЕБЗКЭВЯЬЬЯЖЕОЙЯЙЬВУДЕЖЗЕЖКИЙЯВЯГЗУХЯЩДЕЩ
ДКЪЕИКЫЗТДВИБЕЩЕБДЬАЕШЗЙЯВИУЯГЗУЯЩДЕЩДКЮДВЩДЬАЙКЫГКИБЕЙЕЗЕАЙБЕЙБ
ЗЕЩЬДДЕЯЮСИДВИУЕДДЬИБЕВУБЕГЯДКЙЙЕГКДЮЫЪЕИКЫЗТДЖЕЫЕЮЩВЬЬЯИБЮВИКВТ
ШБЕХЗЫОЙЕГЕЪВИЫЬЗЭЙУЩГИЩЕЬИВЕЩЕЯЯИЖЕВДЯЙУЩПКЖЗЕИУШКЫЬВЕЩПЬБЕДОЬД
ЕКШЬЭЫЬДШДЬЩЯДДЕИЙЯЩПЬЪЕЭЬДЯМЩЕЙЖЯИУГЕБЕЙЕЗЕЬИГЯЖЕЙЗКЫЯЙЬИУЕЙЩЬЮ
ЙЯБШКЫКРЬГКИЩЬБЗКГЗУЯЩДЕЩДЖЗЯДВЖЯИУГЕЫЗЕЭРЬХЗКБЕХЯЮЖВБЩКЖВБДЕЪГЯ
ГЖЬЗЙЗЯНТБЕЙЕЗЖЕЫДВЬЬЯЖЕНВЕЩВЪЕИКЫЗТДЗЮЪЕЩЕЗЯВИУИДЬХЮДХОЙЕЩТДЬШЕ
ЪЙТИБЮВЕДДЕЩЫЕВЪКЖЬЗЬЫЫЕОЬЗУХБЖЯЙДГЯЗЕДЕЩДЬШЬИЖЕБЕАЙЬИУЕШКЫКРЬГШ
ЬЗКДИЬШКИЙЗЕЯЙУЩПЬИЕИЙЕДЯЬЕШВИБЩШЬЫДКХИЯЗЕЙКЪЕИКЫЗТДЬЬЕЙЖКИЙЯВГЗ
УЯЩДЕЩДКЬМВЩЙЕАЭЬЖЗЯЫЩЕЗДЕАБЗЬЙЬДДЩВИУЬЩДДЬЙЬЗЖЬВЯЩЕЕЭЯЫЩПЬЬЩЕЮЩ
ЗРЬДЯЕИТЖВЬЬЩЕЖЗЕИГЯДБЕЙЕЗТЬГЗУЯЩДЕЩДЕЙЩЬОВБЕЬББДДЩВИУЬЩДМЕЙЯШТВ
ДЬЫЕЩЕВУДЬЬШЬИЖГЙИЙЩЕГДЕЖЗЯЖЯИВЕДЕЬЖЗЕЩЯДНЯВУДЕАЮИЙЬДОЯЩЕИЙЯЯЯЮЩ
ЯДЯВЩЬВЯБЕЫКПДЕЩЙЕЙЭЬЫЬДУГЗУЯЩДЕЩДДЬЖЕВХШЕЖТЙИЙЩЕЩЩЩЮЪВДКЙУДЖЬЙЬ
ЗШКЗЪЕШЗЙДЕЖЕЬМВЩЫЬЗЬЩДХЮЫЬИУЖЗЬБЗРХЙИЮЖЯИБЯЖЬЙЗДЫЗЬЬЩЯОЪЗЯДЬЩЯЮ
ИЬГЬАИЙЩЬДДТМЖЗЬЫДЯАЯЮЩЬИЙДЕОЙЕЕДШТВЕИЩЕШЕЭЫЬДЕЙЮБВХОЬДЯЩБЕДНЬЪЕ
ЫЖЕЯГЬДДЕГКЖЕЩЬВЬДЯХОЙЕЕДЖЗЯИКЙИЙЩЕЩВЖЗЯБЮДЯЖКЪОЬЩБЕЙЕЗТАКЮДВЬЪЕ
ЩЙЕВЖЬЯБЯЩДКВЬГКЪЕВЕЩЕХБЕЙЕЗОЬЗЬЮГЯДКЙКГЬЗЙЩЯЕБЗЕЩЩВЬДДЖЕБЮДШТВД
ЗЕЫКЩИБЕЗЬЖЕЙЕГЖЬЙЗ

(b) Расшифровать текст:

ЮЦЙПЭЮЮЕМЫВЫРКОДХТЗЩЫЮЖДПЮЬУИЫЮЭГЧЮИБЭИАЗАЗСЩЮАРНШЫЮЗНЧДЬЮЖХЛДТК
ЧДУСМТЪЬРВХБЭПБХЩБФШПЪЦПШРЮАРКСГЯОПРЖЯЪПЪЫХНЮИЮФТЧЕИЫЩОЫЧГРЗЙАЯП
БХЩБФШСЖЯОУЯДАРБРДВНКПВВОНЧШЦТЙЬЖЩДЧДАВРЯШЗЩННХГГРГАЖЩПЮТБЦНЛЫЪГ
ЮЛАГЙХДАЩЯДКЭЮЬОБЪЕЯСМЫЧЯДОЙЕЯДОЫЖИФКЧЗЬХВОЫЮЖКОГЯОЙТЕБКЮИАГЮЭТЭ
АХЙЕЙИФКХЗЬХВОЕЯУЗАОЬУБРДЭЗВСЙГЗИХЩБПФЬЖЯЖКШЬЬУШДЫЭЩХТЕБКСШЫТЭЮШ
ДГОКТЩЯУОЧГГЗИЮИЮРЮХБВРОПЬЮЗБЕЖМСКЩЮЮХОЪДЬЗОШЮДОБЪНЦТБФЧЯТОРДБЩД
ШЗТТЙХБЭТЖТЖЫРОЫЖМЛНДЮГНЭЫЩУЗАТИЫМУЮДГЩНАЙЭПКУБЩЕМАЗЬРЮЫВУЗЗЮЫТМ
ЖЩБНЩДЕАУЭМПШЙКЕЮГУРЗЛВЦИААИЦОЮЭЫЭСМЫОЬРЙТЭЭЗОЪДШХМХГУЙЯШГДНЙДЗМ
СКШДЧКЗЧЮЪККОРУКЗЩГЦЩОЫЕБРДРЖЬУОЫЖДГЗТЯОФКЩЫЮПБЩГЯИЖЫЗЭХОХБЯЖБЪТ
ФКИЫЮТЭЗХЙВДБШТЩЩНЯБЩЙЮХГГЮНФЙБКЙЩЫЮСМТЖУНЛЫВЩНПЦГЦКГПДЬЮДОЫВСКЧ
ДЩФШЮВЯЕПХЕЯЖКУЪГЮЛЫАЭЗНЯТАРБСЫЭММХГДЪЖТНГРЛЭЮЫИБЯЫХЗЙЙАЯПУХБГМВ

ТЧЦУЛАИЮРЖЧЮЮЩЗЩСЯФПУЮЮНДАЖЩППЕАЩЙПЭЮЮСКЩЮЮХОЪДЭПБЬДХНДПБАРЮЯДБЩ
ОЫГХРЭЪДЫУЗАЬТЗЛЭЮУЭЖЯТУУОПЮШРНЯДЬЩПЯТХЗМУБВПЙЫЩЖДЛЫБЮРУЙЭДТДЪДГ
ДБФВЦПЮЯЖЫФДЭЗУЗЗЙЮИДНЯЖЦФДШГВПЖЭСЬЮТТДЮЧЙАБДДДСГЦУКЩГЦПЙИЫАТДФГ
ЫКИЫЫФРПЮЫБЖДЧЗЬХВОЫИФККИЯУПСЖНУОЫЧЯАНСЫЬНКЮТВМГШДЮИЗЧЮЭЕКШДВРИР
ЪЦФЧКИЯПЯЭЙШКЗЮЛГКЯЫЗАРАХДГТКСЙГМКРДФТБВГЦГЧПБЯОКШНЩЧМИНЯФЮТНЬЗИ
АЭАКЙЮТГЭЮТЖЮРЛЙГАРФТБВСОЙЮДНКУЮЭЗЙЪЪБХЯЫЯХЗЙЙЕБРНЪЙЬУНРДЬРЮЪДПГ
КШТПУИАИЮРЛЭЮАРИХГВЗЭТШИЗМЕГЩЗЛЭДЩУФТЪВФЮХЖШОЧЕБЦПДЩДЩСМТЖУПЧОСЬ
КНПЫЬЮДДЫЭДКЕЫХЪДЩАЯОЙТЗИЪЖЫФИТЙЫЕЦФМЪЪБЗДДЗЫЙЗЫГЭПБЧНФРЗЫШЯАМЪД
ЮЩДЪЫЙЮЯАБГЮДПАЯЕКЯСАРФТБЫИБЯЗЮКЭЯФЙМЙХЪЦЖПЕААЮЙХМЭКЙТЧМДЗХДЭФПЕ
АЦКЯЫШЯТДЯТЮЗУТЩЯРОЭДХХЖЭДЭЗЖПЗДДМЫИЮКУТЩЯПБХЭУРЗХБТТОЙАГРЮЮЫЭХЮ
ХГЯДОЬЖЯМЗЯСЪОПЮТЦФКХЪЦНКОСУНКЧГГКЛЙЫУПБФЧЦИДЯ

2. Разложить на множители числа:

   (a) 810683889340350526375717938637

   (b) 1409167085115156566863451053778821127647775709834036803225189

   (c) 10732983487156296612693623692053953790645719481447353270021691027755435314221170273019597 41

   (d) 190581426903867258634382515809715060208009924703018828318362873365497989605949245166104956200672320338159315850675271059 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 660934286063328486566274411777392092352326669656329821002055538686113251951 21$
   - $e = 17$

   Сообщение:

   - $M = 235320048044292137490659917299877209065692029066265648182812563656337483489 24$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 213857165561781315974540519538820475167$
   - $q = 292867033028154926330249416138970239027$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 382618646887578945982967786794653788839310267451815430315807360107996744310 96$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 282934589376463699308842266670919869459$
   - $e = 257$

   Зашифрованное сообщение:

   - $c = 115689813858559796737320612395171062666$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 252880441770169995095327498394919655873$
   - $g = 202553202072709672991315537940550972300$
   - $y = 252028847744310502669467221086104837044$

   Секретный ключ:

   - $x = 77909265770790539040859486102828949667$

   Сообщение:

   - $M = 75853632144021393545368614293521369807$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 252563479863161540826068051712331106091$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 19450051789567390021305829087702988841 1$
- $g = 13263562617899908102012279670629782 7634$
- $y = 92789715209406203147547572308446520 37$

Сообщение:

- $M = 11449726403326495097808814684140198456 3$

Подпись:

- $a = 56377533217206902699557137991236214814$
- $b = 88645461950106191340894471166286472237$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 541$
- $g = 339$
- $y = 239$

Сообщение:

- $M = 375$

Использовать следующий случайный параметр для создания подписи:

- $k = 77$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 11x - 8$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 24

1. (a) Расшифровать текст:

ЙНЩЫЕЯКЛЯКРЗЛПЛНЮШИПЗЛЮНБЛЯКЙЛЕЙМНЕОРПОПЯЕВЙФПЛЗДИОЩОЛЯВНХВККЛОФ
ОПИЕЯЕОМЛЗЛЖКЛЗЛИЛМЛИРБКЕРОИШХИЕЙШКВЛЮШФЖКШЖХРЙЕЗНЕЗЕФПЛЪПЛДКФЕП
ОЗДИЛПВУРГКВПЯЛЖИЕМЛИЗЛЯКЕЗМЛБЛОМВИКВЯЛДЙЛГКЛЛПЯВФИЛККВЮРБВПМНВГ
ББЯВФВНХРЙРЙКЛГИОЮЕИЕЯКЮПМЛБЯЛНРОЗЗИЕЗЛКККШВИЫБЕЯЪПРЙЕКРПРЯРДЗЛВЛ
ПЯВНОПЕВМНЛНРЮИВККЛВЯОПВКВМНЛОРКРИОЩОВБАЛИЛЯОЯВИЩЕФЕЙЛЖЮВБКШЖББЩ
ЗМНЛЕДКВОГИЛОПКШЙАЛИЛОЛЙКБНВЖМВПНЛЯЕФЯБЛПЩЯОЕИЩВЯКЮПЫХЗПШЙЛЖМВПН
КБНВЕФЙПРХЗЙНЩЕЯКЛЯКЮВБДИЛБВЕЯЛХИЕЯОВИЛЕДКВХЩИЕМВПНКБНВЕФЗПЛЕТМН
ЕЯВИХЯЮНЕКИВЗОВЖЕЯКШФКВИВАЗЛВВАЛМЛЮВНЕРОИШХКВКЯЕОПКЛВЕЙЙНЩЕЯКЛЯК
ЯОМИВОКРИНРЗЙЕЕЛОПИОЩКВМЛБЯЕГКЛЫМЛОИРХЖОЗДИОЯВИЩЕФРМЛХИЕЗЛАЛКЕЮР
БЩЯВНЩТЛЙЗМВНВЯЛДРКЯОПНВФРАРОНОЗЛЙРМЛИЗРЕЯВИЕБПЩДКПЩМЛИЗЛЯКЕЗРЛЮ
КХВЖЛМОКЛОПЕБЗЛАЛГВМЛОИПЩОРБНЩЯОВЙИЩФЕХЗЕЮРКПРЫПИЛХБЕЯОВДТЯФВКШТ
ПЕЯЛПРГКБЯЛНВБЛКЮНБЛЮЕНЫПОЯЪПЛЯНВЙДБЯВНЩЫНДБИЛОЩКВОЗЛИЩЗЛАЛИЛОЛЯ
ЙЛИФБИДКЗЙПРХЗВЕЙНЩВЕЯКЛЯКВРБИЕПЩОЯРАЛИЛЮКГЕИОЮИЫЕМНЕОИЛКЕИОЗОПВ
КВРОЙЛЖБЯВНЕЮПЫХЗЯДИМЕОПЛИВПШЕКЛЮЛЕТЯДЯВИЗРНЗЕЕОПИМЛБИВЙВКДАНВЙВ
ИДЙЛЗБЯВНЩЛПЯЛНЕИОЩЕАЛИЛЯДВЙОЗЛАЛМЛЗДИОЩРБНЕИМЛКВЖОЮИВЫЕЛКРМИДАН
БЕЯЯТЛБЯПРГВЙЕКРПРЮПЫХЗЯШОПНВИЕИЯБЯВНЩЕДМЕОПЛИВППЛИМЛОГБЯХКОЛПЮВ
ГИОМНЛЗИПЕЙЕМВНВПЦЕИФВНВДМЛНЛАНКВКЛАЛЕДМВНБЯВНЩЯКРПНВККВЫМВПИВЫБ
ЯЛНЮШИМЛИЛКЯЛЛНРГВККШТИЫБВЖЙВГБРЕЙЕРДКИХЯЮНЕККВЮЛЖПВОЩОЗДИГВКЦЕК
ЙВОПЩКБВГБЯШЮПЫХЗРГВЮЛИВВКВОПНВИЖПВМЛЮВНВГВЙМЛОИВБКЕЖДНБЙПРХЗЙЛИ
ФЙЛИЕИОЩЮЛАРЙНЩЕЯКЛЯКОПЛИМЛБИВКВВОКАВИЩОЗЕЙОМЛЗЛЖОПЯЕВЙЛГЕБНВХВК
ЕОРБЩЮШКХВЖДБЯВНЩЙЕНДБЯИЕОЩРАНЛДШЮНКЩЕМНЛЗИПЕОПЛИКОЯЛВЙЙВОПВАЛПЛ
ЯОЩЕДНРЮЕПЩМВНЯЛАЛОЙВИЩФЗЯБНРАДИЛБВЕДЙЛИФИЕРОИШ

(b) Расшифровать текст:

СЭЙВОЖЫТЧФМУСГХСЯЦВФЖДТДСФЙТЧЧЛЕЙЧФМЕХЦБМЯТЦЧУЗМЫЛОТЖЯЦФЭТЯУОЬРЦ
БМЕЕГЦГДСРПСГОЭШУЗХЯОЖПФГИСТУГКОЬХЪТФОЬЯЩШХТВФУЩЙЩСЙЖТБФСРМАЧГПЙ
ЦСДЕФГКЙЬХЩЛМАЦЪТОЬЦЯЩЯГМАФТЙАДЦЙБКЭШЖЖТЩУЖИЦЭЧУБСЧОООНВЛОПЙЯНЧБ
ТЪХЙЙАЪЧПМТЗФКЯХДФМДМАЛДЕКЪСОЯЙКФИЯСЧБОКПЭНТЙЖЛЮУЕШЭЧУБСДФЕЕЬЪСЛ
ДЙБЩЙЩЛШСОКЖЪТФЩПЭЬПФЩЪЧЛЮПГУПЖЦСШЬЩСНЛНБФУФУБТАЛВЕЗДЦЙДЙЖИПЭЦРП
НЕНБОДДЧАНООМЗЛМУСГОПЙЖЪЭМЖТШФГЕФЯФЯЩТШФСЕИАЛУВОГУПЖПЭРМЬЖАЮГТФВ
ЩМШЕИЮЛБРИЮЛЕРЩТЙГТВЩШЙТЧЮЙЫЫЗФОПМГШГЬЫАЫПЮМВХСЕИГСЗЯСГЧЛЮЦЪСЭДЯ
ЮЦИЪТЧФСИЦАОВТПГРГЬЫЪЦОЯЛЧФОЯЦСКРЕУЩВОЬЖЪСЙЙУГХГЪТЖШЦОЙЕШЙДУГЙПИ
ЦЪТПВЫЭКЕЩТЬЦИЯПБФКШФГКДШЧЩЛУЫТЫКЙБЕИКФЙМШЦЙШОЭЗФЫЧЗЙСЯЕЯОВКИЪШЙ
БЧЬФГЙЙДЛСУЦИШПДРЭЙОКПГХУУЛЗРОЯЦГХПЗЛЖХЙДЧАЛТДММОКМТЩОУЩЬЪЗМЪТЕФ
ЕЯЙЬИЩЬЛЩФСЕЖСЛРЗМЖОЦИПГИЦЕСЧНМИЦЯУРЬФЪРСЬХЗОМИМЧБРЯПГКОЯРЩЩЦЕРД
ФУЕРДФЛВТВОМИРВЛЙЩТЕФУЯПЖУРЕПЗООЯЫЪЙПДЙБФДЙТШКРЕСЗВЙЮБЗФДЕЖГЦПЩХ
ЯФДЕФЬЙПЩТЕУПЖТЖСЖККЩФДЫПЖЭУЕИЪСППГФЕЬПКОЧБТШФГЕНЖРГЙТЧЦЖГЦГСЭБ
ТМШПКХБОСЬСВФДЕУГЧМЬЕИУУЪТЩЧГЬПСОШИПИЮМИЖЭКПГЕГСЭПТШФОЬЧЩФГЕПСЧУ
ЩМГУРЕХБШСЯЖАЧРЕИГНСЬСЭЛНЙТВЫПЮМВШПДЖГМУЕЗГХПИЦГСЬАИЧФСЯПЭХПЙРГЮ
ОЬРИЩНЬЦВЫПЫМАЧГИЦГЦПДЙЧЧУЬУЭКМЬЫЪФУЩХЯФДЕХЪСЖДМЭФШЬССХПМТЩОМДФЬ
ЗПАСЭЭЖИОИДРЗМЖШОУСГКЖВЦСЗЬВТВЛШЬЗГУЖВАЬЗЬВТЭХПЫЧБШЭЕУЕФЕЕПЫЛОЯМ
ДЩУЯЕЪЧРЕОГПТЙЖГЧГЬПСОШЕЫЪУЭГЙВНВЩПАФНЬКЩЩУЬРЕЧРЕПГМЙВХВФШЬЖЗВЙВ
ЙШУМЩОИЧГЬПСОШЗЙНОМИЧЦЦУУХВХЖОАКФИЯСАЛДДУГСФИОГЦПЩХЭНВЮЩЕХЖВМЬЧО
КПЯРФШМЗБКЖФГЧОКЖНОТУУГЩУЗЧЩФГЕПСУПЖТЬКОЕЧЧОЕЬПМШПШЧЕЩУЯЩАЧПВСЛЛ
ТЯПГЧОЬЗАЛЗВТЖСЖЖМЗЛМУСГПРЬПЪУПХСВЛПШТЬЦЙГТЮЧУЬУЭСППИЭЗЬВМЬХСЭЙВ
БСИУАШЙВХЖЫПЮМВФНБТЗФСТНЧНМИСЖШЛКВИТЖЗЙВУФХУАШФОЦГКЗЬХЧЛМУММ

2. Разложить на множители числа:

(a) 658397050055244898928375994961

(b) 769703944168397220926051168911483341783672236515769870896993

(c) 944700133210725303908442124458521666821584001589578910180664612143738665421921805026925331

(d) 14904287521390804736978890866472809713052101450075679496093943230746523409828047292291689907655831153856942106834319972 97

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 583529206319399282454915823608370408539220359721767334076314808368902053863 03$
- $e = 5$

Сообщение:

- $M = 492659572098267858082959672005086518702109586408558888180776785219328562596 47$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 238975822384162936442914806135003954419$
- $q = 310357244725184200351985756634999839561$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 425228492263937427701608334826949018069862967171836452017244225134198962037 88$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 120138584368511628604321350536580519473$
- $e = 17$

Зашифрованное сообщение:

- $c = 116010690363299497716496186360690229871$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 237968840889168776513318114969955787693$
   - $g = 977018909941378645869208982587040 3958$
   - $y = 221986392985254567470232319494005811658$

   Секретный ключ:
   - $x = 116000637186504777283936738427183133485$

   Сообщение:
   - $M = 30183241442656532554841589969803962782$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 121949773545379378868315701353466524341$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 27004722409240415295058542111037318 7209$
   - $g = 67850534255306414211820870318641667181$
   - $y = 79531616415683743337240562850056451955$

   Сообщение:
   - $M = 15993120953979951868541758763356 1466473$

   Подпись:
   - $a = 53335908802996530953053717449112646118$
   - $b = 89800216744662096378724844828471401919$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 719$
   - $g = 595$
   - $y = 228$

   Сообщение:
   - $M = 91$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 155$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 12$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 25

1. (a) Расшифровать текст:

КВЛФВКЩМЛКЕЙДКФВКЕЪПЛАЛОИЛЯЛКЮШИБЛЮНШЖЙИШЖКЛЯВПНВКЕЮВОМРПВКБЛЗНЖ
КЛОПЕАИЯКЛЫВАЛОИЮЛОПЕЫЮШИОПНОПЩЗМНВЗНОКЛЙРМЛИРКВНВБЗЛДОЯЛЕКВГКЛО
ПЕМЛИРФИЛКПЛИФЗЕЛПЗЛПЛНШТЛТИМЛУВИШЙОРПЗЙЗПЛЙРГВКВЮШИЛКМЛВАЛЯШНГВ
КЕЫЕЯНАЛЙЮРПШИЗЕПВАЛЯЛНМЛНРООЗЕИЫЮЕИТИВЮКРПЩИЕХКВВКЛЗЗЯЕКЛМЛБЯИЛ
ОЩРКОПЛИЩЗЛДЛЮВБЛЙЕПЛМЛНЫЙЛФЗВМНЕФВЙРФЕПВИЛЮШЗКЛЯВККЛЕЛЮКЛОЕИЕПЛ
ЙЛЖЮЛМНВЛФВКЩОЗЛНЛМНЕЯШЗЗНРООЗЛЖКОПЛЖЗВЕБГВОПИМНВБМЛФЕППЩВВЯЕКЙО
ЯЛВАЛЛПВФВОПЯЗЗКВЯМНЕЙВНЮЛИВВМЛИВДКРЫБИГВИРБЗЙШПЛПФОМЛИБЕИЕЕТЛПМ
ЛЗЛКПНЗПРЛЮДКЛКЮШИРФЕПЩЙВКМЛСНКУРДОЗЕМЛКВЙВУЗЕЕЯОВЙКРЗЙКЛЛКМНВБМ
ЛФВИКОЗЛНЛЯШРФЕПЩОЛПЙВКЗЛВЗЗЮЛИППЩМЛНРООЗЕЕМЛПЛЙЗГБШЖЕДКОДКЕЙИОР
ГВОЯЛЕЙБВИЛЙЙШГЕИЕБРХЯБРХРБНРАЛАЛЙВКПЛНЕКВГВИИКЛЯОЗЛНВОРБЩЮКОНДИ
РФЕИЕЯЛПМЛЗЗЛЙРОИРФЫМНФЗМИХЗПЛИОПЕНЮБВЯЗЕЗНЕЯЗЛНЛЯКЕУЗРИЩЗЗЗПЛОЛ

АИОЕИЕОЩЯЛБКЛЯНВЙЗЕКРПЩОЙПРХЗВЯКЛАЕЯЕКОЩЯМНВОПРМКЛЖОИЮЛОПЕЕОМИФВ
ЙГИРОЩКЙРОЩВЛЮЛИЩОПЕЯХВАЛЕТКВЛМШПКЛОПЩЙПРХЗХРПЕПЩЪПЕЙКВИЫЮЕИЕМЛГ
ИЛЯИОЩЮПЫХЗВРКВАЛНОМНЯЮШИЗЛНЛПЗЛКПЛПФОМЛПНВЮЛЯИЗКИЩЫСНКУРДБЛИЛГЕ
ИЕФПЛЙРОЩВБЯИЙКВОЯЛЖРНЛЗЮПЫХЗМЛХВИЯЙЛЫЗЛЙКПРЯЪПЛЯНВЙЮЛМНВОМИКЗНЛ
ЯПЕОКЛЙКВЯЕККЛОПЕЮШИДКПБВИЛЙКБЛЮКЛДКПЩФПЛБИЙВКЯШМЕОКЮШИЕДЙЛОЗЯША
ВЛАНСЕФВОЗЗНПЛКЯЕОВИКОПВКВЮВДЛЯОЗЛАЛРМЛПНВЮИВКЕЕБЯКЛОЛЮИДКИЙВКХЕ
НЕКЛЫЕБЛЮНЛПЛЫЮРЙАЕНВХЕИООБВИПЩЕДКВВДЙВЖЕМЛИЩДРОЩОКЛЙЮЛМНВМНЕКИО
ДНЮЛПРЮПЫХЗЯЛХВИЯПЛОЙЛВЯНВЙЗЗМНЕИГЕЯИЙЛФИЩКШЖТЯЛОПЗЙШОРБЛЮНЛЖКБВ
ГБШРЯЕБЙЛЕРМНГКВКЕЯАВЛАНСЕЕЮПЫХЗБВНКРИЙВКДРТЛМЛПЛЙМЛБЮВГИЗЮЛМНВН
ДЮРБЕИВАЛЛФВКЩКВЛОПЛНЛГКЛЕОПИЛОШМПЩРЗЛНЕДКЙЕЮЛМНВЯОЙПВКЕЕТЛПВИЮШ
ИЛМНЕЯОППЩЕКВЙЛАКВОФОПКШЖСНКУРДЮШИЙВНПЯЛМЩКОВЙЩЮВБЛБЕКЛПЯВПЮПЫХЗ
ДЯЛНЛПМНЕМЛБКИВАЛО

(b) Расшифровать текст:

ЭГХЯШВДХКЧЪЖИЛБЯДМЖКАОПЙЕГДРЕЧРАОЩДФЫОЩДЭЭСВЧЮЮСЪФЪЪМЗФКАСВЩНШПА
ЪДДППЫАУЦЖХАЯМЪЦЬЙЛДСЙЗЙЫЧЦГЦВРЕНМГЪГАЛГУАВЙЕНЯИЬЗФКАУЖРАШМЩЩЪГТ
ЩОЦИАЬМЦЫКЭХКИЧКЛАОПЬОФЙЬВФЧИТЙЕЮГИОЫЪАФЛМЭДПАЯВЙРЕЪГШЙКФАЖЧЙДЮЮ
ЖЖФАЗРАМЭЪОЖРЙЫХЕЦНВМЯЬКЮОЖЫАЖЯЭЬЯЫНКУЪЩТИОЭЮХЗОВШТЫЧФЭЗГНАГСЭЧЙ
ЫСФХЯЫУЖЦВШМГЪОЗРЖЫВЫПЕЦЧЫХЗЩЧЪЧЩОШЪЙЕСЧВЬЪКВЮСЖШЪЗПДЦЧВЬЛУБЮЦЕЪ
ЬЙВЬЧЙТХЖЛЧЖЬЭЦЯДВЬЬВДЫВЧРВФФСФГТЪЦГЫПЪЬХДПАЪДБЬАЫОВЙЮНЕИЙДШАЪПА
ВЪШХАФЪЗЙЫЧВДЖЕЦЧШМЬХЕЬЖКЧВЮЫЕЧБДХГФЩГМДШЭООЛЪЬЬМЩЩЪГЧЫЧГИМЬОШЪЧ
КВЪЕФЖЪДССЛЫГБЖЩЧХЙЧПОЯТЙЕОЕЯИЭЫЕЗУЭОДГОИСЙИАЙУБЮЦЕЛГАТИОФЮПЙЪАЕ
ФЖЛАЬИЭХНЯОИСФСРЙЫВЮЫВЧЮНЦЖЖДДРЖТУИВРУГАЛГОЮЙКЭЦЬЙЬЕЕЧЪЖЕДЮЪЖЕЧБ
ДИЕЧДЫЕЕОЦДЛЖЛЧОАЙЪЭСЬФЫНШХАФЪЗЙЫЧВДЖЕЧДШЙПФЪШСВЬЩВМПКНБЛЕЫГБЧЮК
АЯХЖФЦИЧРОЬЙЫАФЪЕТГЦАШТЯЩЩЮПВШЪИСРЫАБАВЧГБЖПЫАЗТГНДЙЫАБОГМАХГБЧЮ
КЯЫИЭЫГГМКДФГЙБЫАБОЛЦЧШЙЬОКТХАНЧБЕУНАВИЩЧХЙРЖФЪБХКУУСПЖКНБЧПБЧЪТ
ИЧХЮЙЫЧГИМДСЭДХКСБЖТЙСЮЭХКЧЭВЯЙОЭЮТЩОЦИАЪЪЪБМЙОХДФЖЛЯГЙЛХАБОГЦЪГ
РАЦЕИЧАЧГСУГХЧГЖЖШВДХДСЬИТДЧЪЖТЬСДЫПАПЪШЯГСАГМЫНЧЬМЪЬДЮОВЧФДМНЪА
ЗЦЖЦЪЫЧЙФНОЫКЧЕЧЦЦБЬЮЦИСГИИЛБЬЖЙЙЫОГПЭМЬДПАЪЬЭПЖЦФЫИФОГИАЮОЯЗЖЭЫ
ЧЧТЫЫНЫПЦНЪЙСЙХАЯЕКЗКАЖЙОХДЦЖНЕОТЬЦЦЫЖВШЭООЬЪЭШЕЖМЕЬМЪОЮЕТДФЧГАВ
ЬАЪСЩОЦВЬЬОФАСЪДЦГААУЬДЙЛЦЧЯУИСЦГТЭАГИЯБМВЫЕЭЦОЪЖЭЦЪАИГЫНГИЭЦЧЩУ
ИЧГИМЩЧХЗЫЭХФЧСЦЪЗДИАЫОЛТИЧКДОЖФЪГНЬОДЗИЖКВСНПОЭДЖЭУДДХАНЪЗЙЩОФЪ
ЙЪУЗШЙВЧФЫЫЕЧЫГЙЪОГИТЦЛЩЩПЕЬЭГРИЕРЮЖЕЧФГЧЖЦФЗУЖУВЗСЭФЪЪКЭЪЭЫЛУУБ
ГЧГСЯЫЙКЩЧБОЛХЯЫХКФАЬПФОЧЮХЗОКЮПЗОВЫРЭЦЪИАИРХДЖЖЩГБЯРФГАЛГНАШТГЕ
ЯДСЭУГИЦААДДСЪБЕАФЭШАЗЦФЪАЧМИЗДЗСЗЪДТЕРУЪЖЪУЧД

2. Разложить на множители числа:

(a) 461693913184203927751338246373

(b) 894558159375977233362328605792857148490874236444150750391753

(c) 1524077981140900555595248684204869170370372461049262022304022776372553556460481001936988293

(d) 822669096348542743173872008953949613959188832196191298030763693525282880264278393160731692499757956165425027411784357679

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 34945549398906762946863742917664133384659150306108059019637773157448205358357$
- $e = 5$

Сообщение:

- $M = 34778980729454014919200095191758612487815095112243778538769395051757555989251$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 285854233573697390146462941388285642387$
- $q = 24454663061792892598979517053371182532 3$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 59613033677047200168947417791472922594030943868389458987481369302460617726438$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 17962747281645741652888140382863951984 7$
- $e = 5$

Зашифрованное сообщение:

- $c = 157741442930099785865399257308259380785$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 32415397947483917487854896131133017298 3$
- $g = 51621899472020947841042184735742481772$
- $y = 36513759545885959872934856016732380314$

Секретный ключ:

- $x = 22854150823980707416329804432532649651 0$

Сообщение:

- $M = 27321726375062182475765378315951836531 2$

Использовать следующий случайный параметр для создания подписи:

- $k = 71646799910960898297399037865358591997$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 24585578813025803570123144501036801177 3$
- $g = 90456762255995397359656477438555336 37$
- $y = 17350801553282975654733076034578814293 3$

Сообщение:

- $M = 18585036919987741096740195956391259440 9$

Подпись:

- $a = 13044253388486772442351236107008450478 5$
- $b = 17803206128298025836958895927204605344 4$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 977$
- $g = 173$
- $y = 92$

Сообщение:

- $M = 721$

Использовать следующий случайный параметр для создания подписи:

- $k = 897$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 13x - 3$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 26

1. (a) Расшифровать текст:

РЙЛЫПЗПЛДХВИЗЗРЙВБДОВИЯПЫНЩЙВЮВББЕПЛИЩЗЛЗЗМЛЗГРОЩКАИДАЛОМЛБЙФПЛО
ЗГРПЛКЕЗЗРДКЫПФПЛБЕПМЩВПЕЕАНВПФПЛЮРПВХЕПЩЮВБКЛАЛОЯВИЩЕФБИВЙРОИЛЯ
ЛЯМНВБЩЮВДВАЛОЛАИОЕКВНОМЛИАПЩКЕЛБКЛЫЗЛМВЖЗЛЫЛКЙИЛМЛЙИРРОМЛЗЛЕИОТ
ЛПЯОВВЦВЕДНВБЗЯЛНФИМНЛОВЮЗФАЛИЛЯЛЫОПЛНРЮИВЖИВАЗЛИЕБВИЛМНЕЮИЕГИОЗ
ЙВОПРЙЛВАЛКДКФВКЕЯЛЗНРАЙВКМНЛОПЕНИЕОЩМВФИЩКШВМРОПШКЕМВНВОВФВККШВ
ТЛИЙЙЕЕЛЯНАЙЕЯОВМЛЗНШПЛЮШИЛОКВАЛЙОЛИКУВОБЕИЛОЩЗЕЮЕПЗВТИМЛРДЗЛЖБЛ
НЛАВЕИЕПЛФКВВМЛОИВБРМНЛИЛГВККЛЙРЗНВОПЩКОЗЕЙЕОКЙЕЯБНРАЙЦЕЗОПИМЛОЙ
ПНЕЯПЩЯОПЛНЛКРЕКЗЛКВУОКЯХМЗРЛЮЛНЛПЕИОЗЛЙКВЕОЗДИЮНЕККВМНЕЗГВХЩИЕЯ
ЛНЛПЕПЩОЪПЛДФВЙЯНВЙКВКБВГКЛЯВПВНОИВАЗМЛБШЙВПОЯЕХЩЗЗЛКОЙВПВПМЛНЛХ
РФПЛГДЮВБЯЕБЕХЩПЙФПЛЙЦЕЗРЗДИЗКРПЛЙКЯЛОПЛЗКЕФВАЛКВЯЕГРЗНЛЙВЮВИЛЖО
ПВМЕБОКЛАЛКВЮЯЛКЯЛКЪПЛЛЮИФЗЛРЯЕБВИЯОЙЛЙБВИВКЗНЫКВЮЮВИЛВЛЮИФЗЛЗЛП
ЛНЛВМНЕКИЮШИЛОМВНЯДЛПБИВККШЖТЛИЙЕЗЙЦЕЗЕДЧОКЕИЙКВФПЛЛЮИФЗЛМНВБЯВЦ
ИЛЮРНКОИШТИЛПЙЛХКЕТЙПВИТЕДКИФПЛУВИШВЛЮЛДШЮШЯИЕЕЙЕДКВОВКШОЯВИЩЕФО
ЛАИОКЛОЛЙКВКЕВЙЙЦЕЗОЛЯВПЛЯИЯЛНЛПЕПЩОКЛЯВПВНМЛЗДИОЙКВКВОЕИВКМЛКБВ
ИОБЛЮНПЩОДЮИАЛЯНВЙВККЛБЛОИВБРЫЦВЖОПКУЕЕЕЯВИВИВТПЩОЗЛНВВЙЦЕЗМЛОЗЗ
ИКЛЯОВМЛАИБШЯИКЯЛОПЛЗИЛХБЕЮВГИЕБНРГКЛЯВПВНЙВГБРПВЙФОЛПФОРОПКЛЯЕИ
ООЕИЩКВВЛЮИФЗЛЛЮНПЕИЛОЩЯЮВИРЫПРФРЗЛПЛНПГВИЛМЛБШЙИОЩНЛОИЕМЛОПВМВК
КЛЛЮИВАИКВЮЛМЛХВИЙВИЗЕЖОКВАЕЯБНРАМЛЯИЕИТИЛМЩЙЕЯВПВНДЯШИОБВИИОЩЙП
ВИЩЯЛБКЛЙАКЛЯВКЕВПВЙКЛВКВЮЛОЙВХИЛОЩОЛОКВГКШЙЙЛНВЙЯОВЕОФВДИЛКРЮНЕ
КДЗНЕФИЙЦЕЗЮВБЮРНКЯШАИКРИЕДЗЕЮЕПЗЕЯОВЮШИЛЙНЗЕЯЕТЛНЩЯВПВНЯШИОПЗЛЖ
ОЯЕНВМЛЖЯШНДЕПВИЩКЛОПЕЫФПЛЗДИОЛБРХВЯИВККШЙОКВАДОШМИЙВКЕОЯВИЩЕФИЛ
ХБЕХИЕХАЛЙЕОЗЛНЛОПИЕФПЛГ

   (b) Расшифровать текст:

ДАТЙЛЯНРЗИОЗЗЧОЕЪПЗРЙЕДФПДЪПЗЗОБДМРЬЯЗДМТНОРГЩЯСЗРХЪБЪЗПЕВКОЕЪБЛ
СЬЕНЖБАИДСКПАНФМЬЗЗЯСЯООЕЗЩНТНМЖЫСТМЫЖДКЦФИНЕНЕИСЗАДЫНИЗЫБЙМСЬЧД
ПДИДБЗРЙГНЖНШЖННДБЗДЛЗЩГЪЩНДЭГХЧЬЩТГРЙШНКЗЮЩБТГЯЮБЭОЯЗМРМЯШВРРЖД
ГГНЪГДДДЗЙДФСТИНЩСЕИТЖЕЬБДЙДПТЗДМБЙЖОЗОШОРКДЫРРВВОКУРИШНЗЭИЙОТТЪ
ДЭКОЗЮВРБЗЮБНРВСЧЮСТШРККЯЗДЕНЗДБПОЗШГХВЕШНТЗЙЕНЗГЯГЙКУЕЖЛНЫДДЖСП
ЬПДПЪЩШНКМИАНОПЙЮЙХКЬВДИГКИДООВОЙДЖВЙМУМПЮЧСВЯЮНФМЬЗКДЦКБМПДГДВП
ДЮЗЛЗСУЗЧДАЗЮМУНМЖМККИШНАБЭГНУСУЕПКБИЫЛОНЬВТДЕЬГЗКЙЩВРМЖВДМЗИМБГ
ПНБЖНДМЕГДОНЪЙМЗЖГЫСКСУНСРМЖЖРПНЩСЗЙБЕБЗФДШЫРСНБДЗФЫИЕНЖБЬЖВПРЩО
ДОТИЙГХОЗЫГРРЙШЫФДФИНКБДЙЙХЖГЮЦХЬЙДДЕНЫЫКРФГДИГСХОЙДНЮЖЖККБДЛЗМЫ
ГСЪГЗЭБЗЛКЬЗИДДГДЗГЯГГХФЯЫГКМЖБНФЫЯШММТЮВЗЩЦЙДСЭЖЬШДЪЫИЫИЩРЗЗРЖЗ
ЯЛОРПЮГЪОТЪБЛПФВЫАЖМЩДГХЦЙДАХМЯЛГХПУИНСПЕОКЖОКЗСЮНЙЫХЕДЗЗЗОМВДЕК
СДГЗЧЬЖЮСКЛЯФЦФНШВННЗВЮТГНЪЕПРШЬГЗЖЙВЮРЮОЬЖДЖКХЪЫОЗЯШММТЮВЗЩМЬЭМ
НМОИНТДПЮСЮРГЖЫКБДДБПАТБЦТДЮШЪЩИДДАНДЫГЛННЖДЛНТШЙПХСЯЛКМНГЫМЖМЙО
ТУОЕАНККИТЗЙРЙШЗНМИЪПХВЫЖТЕОЕМКРБЙТОНЧБЕПКМЬЗКПЛДОЗЪОЪЮЛЭБТОККНЙ
АНОДДЪМФОЕШЗЖЗГДЛХОЗЮЛКПЬГМЭДЯШМКВДИЫКЦДЗРРОЗДБРЕЫБЙМБГГДУСТЪМРА
ТБНУЙЮБДОТИЫПЖЗЙДГРМЕЗЗФЫДГРМНГЫМЖМЙЙОРРВЫСРВЕАЙЖКЯВМЗРВДБРСЕЩНП
ДЫЫКФЫБААРВИШСКБДЙЙХЖГЮЦХСЕЩНПДЪДБРПЯБНФБЬНКРМЩЗЗНЗИЫВРПЕШМДЪЩЫГ
НБИЫНФЛЬГНПБИЫЛКПИЕНТГЯБРЮАЬЭБЗГЕВЙРЛЬГГПСЩЕПРЦЬВРНБШДВХЦЙДБУДЙА
ЙРМОЮКРРУЗЬФЗГЗКРБЕВНПОЕШДТМКБГРЛЕЯЧДАЗЮМКНИИККРУГДЖЗДЫМЪДЫЫКРЬЙ
ЮЛМНДНЗФЫИГДОНЭЫСУЙЮБДОТБДМЗЦДДНФБЬНКЪБШЖЗПБТЗБРДХАПРБУФАХГЬИДРС
ЩЫЦФЫГГДЙБПЙГЗПЮДРФЫДДЖПЛЯШДТНЙГНУСДЙССПЯЗЛФПЯШСЮМЬЗЙРКУАНЖМЬЯМО
ГЕБЕПНШЙГЗСЖЖЗФБЕЖСЮРЫДРД

2. Разложить на множители числа:

   (a) 895423277168452926574951898227

   (b) 776931937366972186696181166550511189651564156480517530703973

   (c) 165390339218750444386155369645875025859644033066659320349470124155662428748203533114013058 7

   (d) 743010951451237978001055144088064134324166536864827985885080895124134525023722773330025693018698477824473795172353879719

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 42255228035819689755678154306140796598705654494585665802166037000223822905689$
   - $e = 17$

Сообщение:

- $M = 244796611075887561698816817440252876095019336449101689440391689966665884125992$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 257942764000290972118769990920227972071$
- $q = 255321448455497723136500104704264163541$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 245155317748959119922492640247231324277452890869272410832209698293186585059 7$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 28286197288862860238412293347045386055 9$
- $e = 5$

Зашифрованное сообщение:

- $c = 221134022538477681070015627775215778526$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 28756828553945466700583632159360844 2823$
- $g = 120792917922757774775667197203939677308$
- $y = 132412894906287020952025468275169839481$

Секретный ключ:

- $x = 10304285630747159723428270535474048 2001$

Сообщение:

- $M = 57291247231498532965841354154659808766$

Использовать следующий случайный параметр для создания подписи:

- $k = 29470661001057368197868743424512056 85$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 19015442930677991253910513493602126 4549$
- $g = 26116999333286724884479831874262783 43$
- $y = 13627052242145707618788984457638219 5332$

Сообщение:

- $M = 50387700118380371124408037795059107220$

Подпись:

- $a = 17257830907217834900333210378846201 8208$
- $b = 75259335256308921432575001517719617360$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 577$
- $g = 496$
- $y = 213$

Сообщение:

- $M = 4$

Использовать следующий случайный параметр для создания подписи:

- $k = 325$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 8x - 9$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 27

1. (a) Расшифровать текст:

ЯАЩВНЩЯФЮЭАБЛТУФБКРВУФЗЛСЩЭЫЬУФЩЮЧБЬЫЧЯЭЬЭСУЭРЯЭТЭЧЖФАБЬЭТЭЖФЪЭС
ФЩБЫБКРВУФЗЛЬАЪВХРФЬАБЭИФШЬВЖЧЗЛАУЧАЕЧЮЪЧЬФСЭЯФЬРВЯТФУФЪБЛБФРФЬФ
ЖФТЭЯААФЬЧФСЯФУЬЭЫЭЪЭУЭЫВЖФЪЭСФЩВАФТЭУЬЫЧЪЭАБЧЮЯЭАЧЫЭБЭРФУБЛВЫФЬ
ЖАЭБЖАВЬФЪФТЖФЮЭУВЫЪЮЯЭАФРЩЖФЫВЮЭАЪВХЧЪЭЫЬФБЭЖБЭФИФСВБЯЭРФЫБФЯЧР
КЪВХФТСЯУЧЧАФЯХЬБЭЫЩВУМБЭЫФЬЦСФЪЭСЮЭЪЩЧСТЪВДВНЩЯФЮЭАБЛЬТЯЬЧЕВЩЧЯ
ТЧЦЩШАЕЩЧДАБФЮФШЭБЭРФУЪВЬУЯФЩЯЪЭСЧЖСБЯЭФЫАФТЭАБЯКЫУЙНБЬБЭЫАБЯЭТЬ
ФЫФЕЩМЩЭЬЭЫЧЕЯАБСЭСЪЦФТЭАБЭЪЭЫЧУВЫНЖБЭАБЯДСЧУФБЛЧЬЭТУЪЧЗЬФТЭТЭАБ
ЦАСЭФНДЭЪЭАБЭНБЯЮФЦЭНРКЪЭБЖАБЧЮЯЧЖЧЬЭНЮЭАЮФЗЬЭТЭВУЪФЬЧЫЭФТЭСТЯЬЧ
ЦЭЬЬУЯВТЭШУФЬЛЮЯЭАБЧЪААТФЬФЯЪЭЫЧЭБЮЯСЧЪАЩЫФАБВЫЭФТЭЬЦЬЖФЬЧТЪСЩЯФ
ЮЭАБЛЫКСГЭЯБФЕЧЧХЧСФЫДЪФРФУЧЫЧСЭУВЮЛФЫЩЩЪНБКФСЯТЧЮЯЧУВБЩЬЫЬЮЧЯЭТ
ЧЦУУЧЫТЭАБЫЮЧЯВЗЩВЦЯУЧЫЩЯБФЖЛНЮВЗЩВАЭЪУБАЩЮФАЬАБЯЧЬЬКФЪНУЧЫЭШРБН
ЗЩЬФУЭЯЭАЪЛРФЪЭТЭЯАЩЩЯФЮЭАБЛЬДЭУЧЪАЛСАЭЯЭЩСФЯАБДЭБЭЯФЬРВЯТУЭЯЭТЗ
ЪЮЭЩЯВБЭЫВРФЯФТВЧЩЯФЩФИФЬФЦЫФЯЦЪЧФФАСЧЬЕЭСКФСЭЪЬКТЯВАБЬЭЖФЯЬФЪЧС
ЭУЬЭЭРЯЦЬКДРФЯФТДЮЭЩЯКБКДРФЪКЫАЬФТЭЫЦЬЧЫЧЮЯЭАБЧЯЪЧАЛЩЧЯТЧЦАЩЧФАБ
ФЮЧЮЭТЯВЦЧЪАСЯЦЫКЗЪФЬЧРЭЪЛЗФНЖАБЧНЮФЖЪЛЬКФТЯЬЧЦЭЬЬХЧЦЬЛЫЪЭЧЫФЪУЪ
ЫФЬЮЯЧСЪФЩБФЪЛЬЭАБЧАБЯЪАСЭЭРЯЦЧБЛАФРФЩЮЧБЬЫЧЯЭЬЭСЫЭФТЭРВУВИФТЭЬЖ
ЪЛЬЧЩЧЮЯФУАБСЪЪФТЭАБЯЭТЧЫАФЯУЧБКЫАБЯЧЩЭЫЬФЦЬНИЧЫЬЧЖФТЭЩЯЭЫФАСЭФШ
АЪВХРКЧТЭБЭСКЫЦСАЩВНРФЦУФЪЧЕВАХБЛЫФЬЮЭУЯФАБЬДЪФРЧЬСЭУВЫФХУВБФЫЬЖ
ЪЭАЫФЯЩБЛАЫКФДЬЧУЭСЭЪЛЬЭАЩЭЯЭУЪФЖФЪЧУЭЩЯФЮЭАБЧАЮЯЭАЧ

   (b) Расшифровать текст:

ЕЫАМЩХЦМЖХВЦАДЩКЧОУЯГОЕСЬКЪЙВГНЬИФУВНТНЩПЕТУЗЙЧЙДЯЛХТЖЭМЧЖЖХВЦМЙ
ФВЦЙСЬКЧТОЫДФТТНЛКТНЮВЦЙТЬЕБОПЭДКТУЩИЪМГЮЗЬЛНЩФЦЙРЯФОПИЮРПСПЦНШТ
СГЛЛЦЭЯЙЧЙНАЛОИЙЮЗОЦЖБИЪЖЕЯАНОЦАЛНТИБВЦМНЯЕЧХУЮЛЛММЩОЕСЩУЮЩМОЦЛЦ
ТЕЩКСРЖЬЯДЗПХРЛИПЮЛЪЙЛЯВМТТЬВНХУУЕОРНЯАФТВМПЕЧЕЬВЦМЖЭЛОМИЫНОУПВП
СМСШНДЖТЫЛХЙОХКЫХЛЩЙЪЙНЦЖЪЦГЯЙШТЩЦИЧЕЫУЕЫАПТЛЛХЖЭЙЩАЖЩЯЦТГЮВЧСГВ
ПЩЙУЩИХЙОЮЗЩЯМНУОЫУЯЪЫТТУЙСХЕЦИФТТНОУЛМЯКЬЖЙХВЛРЖЮЗУЖЬТИОИОМЯЪЙЛ
ЯКАЙОЯЛЫЖЖИИСТУХИОНВГЫБОЙЮЛШМТНЙЧТОАЛКПЖХКОПГВЯЧВПИВЩЙЕНМЩТШЩПЛТ
ОУЛРЖСГЕФРОЦМСХЭЭЛНФПЧЦОВСДЗЧВЙВЗРПЕБЛПЭЙЭАЧППВЛХЖЙХКЧРОЦКОХФХЩК
ФПХКДЙГЙЕЦЙЦЯПЫРЖЮЯЪЖППООРЭПЮЬИЙУЛЛХЖЭЯЧПДЯОШТЕЮЮЧЗМДФБЙОЙВМТИЮВ
ЫЫУЯКХСЕЯЮЦТЕЦИЫАОЦФОЗПАВЫФОХНОМШТРНАУЦТЧЦЭУШЪЫТГИСЖЬОПЧРФЮВКЯГГ
ЩЛХЛБЕАПТЖЯЫМГЦВРФФЫРЫЯНЦКФВВЩХЕЗПГЛЛСГВВШТКХВХОЙЮВХХГЮЛММЛГЯЧМН
БЛНМУЦИХТОЩИЗИЙАНЧХУМВЦЙЗЦОЫТЛЯООФЕМВМТСХВЯЯПЮЕЦХВЬАЧХМЯЯЫРЬЯЮЛЙ
ОИВХХУЭОЧЖСЦЙОСЖЭРЛЙСЦКХЯФЭЛФМНЯПЯРПЦАЧРУДХУЕФХВЫЛОВЛЦРЖЮМЩТТГЕЫ
СЖГМОЦСЮБЩЙЙИЛЫЖЖИИХЬОЦЯДНЕДДЫЙВТВРЕМФЛЪППУВЦМУУЛСЩСЯБСЦЖЬВТЕЖШЕ
ЮЕМФЛЪППУВЦМОЦЮЬИЖГПОЕЖВФЪЦЙАЛУТСЩЙЪЖПЬВКТЗЩВТОПЬЕЦНЕЦХЕХЖТВЪЧЗЦ
КЬВЛЯИСУПЬЫКМЩНЕЩЧДДЫКТДВПЧЕППМОЦСЮБЩЙЙИДЛХПТЛСЩУДПЧСИАИУПЙДХФТУ
ЭВЦЩПГВФЕЬЬЛЛТКГЕРСЖПЯУТНЮПЬСПИРЛХУУЛЛППШГЛКЯМЮВЛХПВПЧСЙЩЯФИЖГЩЪР
ЙЭОЧЕППЕЛТСЯПСПТХЛХТКВЕНЙМАЛМФФЧВЦСЬЪЯМПФТЛУЧЯШБЬРШЩЯЧХУНЗУЖЕБРМ
ХГЦИЕМШАНОФГЬЙЧМСШЙДЬМЦКСЖПГОЬИСНОУЛМЯКШТЕУЙЦЙЙВМСХОЮШТПЙВПКЧНФЕ
ШТТЭЛЫФЙХЛЦТТИЕУПЙЮОЛТЖФЛКФЙЮЕЪЦСПОЕПЙАЛХЧУЩПЕХЬЮОЧЦЧЯЙЛЛМЩДЩЧЛЦ
АЧЕФЭАЬБУЯЮДППГЯОЦТУВФАЙИКШТМДФОСОЯВСРРЩОЕРПУЛЫТОЯПЪППУБЧХМЯЯМТТ
ДБЩАОХНОНРЦПЩТГЩФЧЦЖЗКБРЙЬЛЪЦЙУШТРЙЬЛЪЦЙУЛОУЙ

2. Разложить на множители числа:

   (a) 78560048176270978096033002535 7

   (b) 125748497558036575462514519134590200526846329954215599644272 9

(c) 735743245476786290401362509784212084990081012249266789358639529411483337290497503252444117

(d) 1283281262793173448521567793065222017165113844856636223288572179852097708427208550837597713769157450492884635101862372597

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 85744492974796774451728688639130012568168007788482431723629723360043989955869$
   - $e = 3$

   Сообщение:
   - $M = 816201420789950858669774515087347955714398576936439004456630471062115323449 66$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 189364678349698401296041498176627307603$
   - $q = 248152557702821564279090164575041082611$

   Открытая экспонента:
   - $e = 17$

   Зашифрованное сообщение:
   - $c = 225402678652372108100821613931539883572507735326675231174123395291075632719 02$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 159049235498926662674026754637674793929$
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 114015710393495026059519708286167389029$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 178010738083123376960509825023828776987$
   - $g = 108074400933148022055050584513560423 33$
   - $y = 147733947041077328726767314497895020535$

   Секретный ключ:
   - $x = 95681724390501666492545121211786338488$

   Сообщение:
   - $M = 44197685073307217870251257326228476936$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 59327994591426885353077140394975846259$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 21030631835246816962031424788184257279 3$
   - $g = 13554494100235220133236707905861616198 1$
   - $y = 18014824799190426183715837783970453688 3$

   Сообщение:
   - $M = 10604765274228581452632365138188497503 1$

   Подпись:
   - $a = 10343556591450176717510441992680743211 9$
   - $b = 15616252137568239853330397634813858021 7$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 937$

- $g = 350$
- $y = 740$

Сообщение:

- $M = 308$

Использовать следующий случайный параметр для создания подписи:

- $k = 449$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 16$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 28

1. (a) Расшифровать текст:

НИСОВЕТОВИЩУТБЛГОСКЛОННОГОСЛУШТЕЛИТКПЕРЕПИСВМОЮПЕСЕНКУПОНЕСЕЕКШВ
БРИНУКОТОРЫЙОДИНВОВСЕЙКРЕПОСТИМОГОЦЕНИТЬПРОИЗВЕДЕНИСТИХОТВОРЦПОС
ЛЕМЛЕНЬКОГОПРЕДИСЛОВИВЫНУЛИЗКРМНСВОЮТЕТРДКУИПРОЧЕЛЕМУСЛЕДУЮЩИЕСТ
ИШКИМЫСЛЬЛЮБОВНУИСТРЕБЛТЩУСЬПРЕКРСНУЮЗБЫТЬИХМШУИЗБЕГМЫШЛЮВОЛЬНОС
ТЬПОЛУЧИТЬНОГЛЗЧТОМПЛЕНИЛИВСЕМИНУТНОПРЕДОМНОЙОНИДУХВОМНЕСМУТИЛИС
ОКРУШИЛИМОЙПОКОЙТЫУЗНВМОИНПСТИСЖЛЬСМШНДОМНОЙЗРМЕНВСЕЙЛЮТОЙЧСТИИЧ
ТОПЛЕНЕНТОБОЙККТЫЭТОНХОДИШЬСПРОСИЛШВБРИНОЖИДПОХВЛЫККДНИМНЕНЕПРЕМ
ЕННОСЛЕДУЕМОЙНОКВЕЛИКОЙМОЕЙДОСДЕШВБРИНОБЫКНОВЕННОСНИСХОДИТЕЛЬНЫЙ
РЕШИТЕЛЬНООБЪВИЛЧТОПЕСНМОНЕХОРОШПОЧЕМУТКСПРОСИЛЕГОСКРЫВСВОЮДОСДУ
ПОТОМУОТВЕЧЛОНЧТОТКИЕСТИХИДОСТОЙНЫУЧИТЕЛМОЕГОВСИЛЬКИРИЛЫЧТРЕДЬКО
ВСКОГОИОЧЕНЬНПОМИНЮТМНЕЕГОЛЮБОВНЫЕКУПЛЕТЦЫТУТОНВЗЛОТМЕНТЕТРДКУИН
ЧЛНЕМИЛОСЕРДОРЗБИРТЬКЖДЫЙСТИХИКЖДОЕСЛОВОИЗДЕВСЬНДОМНОЙСМЫМКОЛКИМ
ОБРЗОМНЕВЫТЕРПЕЛВЫРВЛИЗРУКЕГОМОЮТЕТРДКУИСКЗЛЧТОУЖОТРОДУНЕПОКЖУЕМ
УСВОИХСОЧИНЕНИЙШВБРИНПОСМЕЛСИНДЭТОЙУГРОЗОЮПОСМОТРИМСКЗЛОНСДЕРЖИШ
ЬЛИТЫСВОЕСЛОВОСТИХОТВОРЦМНУЖЕНСЛУШТЕЛЬККИВНУКУЗМИЧУГРФИНЧИКВОДКИ
ПЕРЕДОБЕДОМКТОЭТМШПЕРЕДКОТОРОЙИЗЪСНЕШЬСВНЕЖНОЙСТРСТИИВЛЮБОВНОЙНП
СТИУЖНЕМРЬЛЬИВНОВННЕТВОЕДЕЛООТВЕЧЛНХМУРСЬКТОБЫНИБЫЛЭТМШНЕТРЕБУЮН
ИТВОЕГОМНЕНИНИТВОИХДО

   (b) Расшифровать текст:

ШЕБШНШУХЧБХВАЫЯЫСЪШЭЫГВГНЩОБЖБШИАТЙТУХИКЪШЪЮНЙТЩЮБЧОЫГАХРКАКЯОЯС
ББЬОАБПЕЛЧЗШЭЗРДЕЪИЩАВТТАГБСОЪЬЙЫБКДОПЕЖБДПНЩЙГЩИЖЗЗИШЬДЩШОУЫЕФВЪ
ЪБШУХВЙЫГЧВДЧРФЕКЮТЫЮЮХДЬДКЪВАВКЩДФББЮИЪЫЙФМФИДШШСЧМХНСДОЮЕШННАЗ
ЬЫИЪСБДХАЮФЩКЮИЪЙНЧЗЪАКЩЕЬЪЙЯВАЮЗХСФЩКЭОСГАЦМЬЫЖШЮЖДОЪБЯЮЮЪИТГОЙ
ИЖЕМХВФЪДЧБЗАДЭЦУЕМХКХЮЪШЮЮЖДЪЕАИДЮЮУЕЗТТФЯЛЫСБДЕХВЬАПФМЧННЧЗЪАК
ЩЕЬЪЙЯШСЗОПСЫЫНЯДШЙЮТДВВФАКВЪЙХБВЪШХЗУДИАТЭЙНШЫЗЮОЧРЧАЛТРФЕПРЕБЗ
АХПЯШААСЩЭОЙНФДСЫТЬЮТСОЯДГИСЩЗУЮТЪЮЮЫОАИЮЯЬАЕЧЯКСЗОЭИЬЙОЧБКБПЧОЯ
ЫЙТНСДЭИЧДЗПСОЮЖКХЗСДАЮТСНОЫБЪЩКСЕБЫЗЙНКЯПЧЗВГДДТЭЬДПШЧЯКЪУНЪКШГ
ЭДНЯВЪЗЭТЗЭШНЧОТДАТЙАИЮХДВВЗХЧБДНЫБАИЮТНЬДБЬРЧЭЙЪИФЕМТСБЙЛЪИЩГБЫ
БДДАХМЭЧЧШОУББРОЮДЗЪОТДКОЛЧНБЪИЫСНШЬЬЫОЫЛЛАКЪЕЭЗЙЫВБЫЗЙНЬДАУЕЧЗК
ПЕЯОБЪНЭЕМЫТЧШЙФДЯШКЩУНЖДСИЖЫНЧОЫЙНЩЫАБПХБЭЫНШИЭИМХЦЬЮБЬОУЗПСИЫД
ЯЫНФЕМХЕЫББЯССЪКЧЗБЫЗЙСБШКТГЭГБПИЬГКЮТЧИКЬРЧЭЙЪИФЫЯЫИБДЯЫМФГБТДЭ
ББВЪОРСОЙДЭАГЯЕЪТНЯВЭВБРОСЮЙЫВЬДНЯИУЬБХНКГБЮЛВНБЯСЫГБЮЛКООЙСБЖЧВС
ВЪБЦЖЪЫЪЖИДДЭАНЧНОЫЖФГДХВЯШМЮКЭЩКЫБКНЮЪШФЬБПРФВЙХКБДЙТСВВЙТВЪЮЬ
ЕЭЧСЫДЧВКЮТЧЕЧЯКЧГДЮУУТДЪИЮДАЮУУЮИИЕЧИЖЬРЧАГЪИФАКЩЕЬЪЙЯНЧАКРОЧЭЙ
ЮНФЙАХВЧБКХНФШНЯРФШКУИЪДДПНЧЩЙЯЬЧНКЯПЯШДШСЦЧФЧИЯМБЩКЭИКЭЫШЗДСЕЪШ
ЙОРФЕКСКЪФУЫМВАКЩЕЬЪЙЯШЧЮУТРФЭЙТСЩДЗЙКЭВДЪУБГБПОЪТЙХКЮЖДПЕЪЮЮЬЕЯ
ЫАЪЮНАКЩЕЬЪЙЯВФББШЕТДЖЮЕРЫЛЭЕУЗОПИБТЭЕКЧЖБГСБЖПСОЫОЯЪУЪНБЭЕЦЕКЭО
ТДЙОЫЪШЖЫЛЭЪЖТИАГЮПЫАДЖАЮАШКЛШЮАПЫСБГКПИЪЗПСВФЖБЦВЦЩЗЪУЪГЙТГЭЮНЫ
ДЯДЯЪУЪЗЙХКЭЩАЪЕЦЧПСУМИКРОЖЫЗЫВФАБЩУЩЭЗЫСЛББЯЗАЫИЙДФЗОАНФЩКЪЕРСЗ
ЫНЧГКЮНЧЙФТЙТДЗЫВФЩКОЫЪШЧОРЧИЮЩЕАИКООЯДАИТЭЖУШОЬЫНЧОЪТЖЫСФЪЧВВЭБ
КЮОЬЧЧШМЪДЯЫРЭЗОАТЭПДЮГЭЖЭШЕЬГКАЗФГШЧИФЩЗФЕТДНПЕЯАЗХЕИЫКРНФВЩВЕА
АГШКЭВБЪДЬИПФНСЕКЮТЯОЙИМФЩ

2. Разложить на множители числа:

   (a) 843462169256889160390331170331

   (b) 10103084892600153802328096274106742558165175761905605134543 99

   (c) 1325445795861236152730149062001613544472102856883578960843309972347553824707986388472537271

   (d) 1788197333754727743000956221092155678773746834391868245016896517131348489961499102714977842040107994791062179438898093037

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 72012300094564032219970853340017104768057983485962082449116685429431094466047$
   - $e = 3$

   Сообщение:

   - $M = 51195376666523243109413506332244643992716760657216589151180300898535001642387$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 257030258779472899376451254004512609939$
   - $q = 253044970460945454113473825574704855339$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 323565581950266765951577200711883498074727854595312396091373577367038048486 91$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 241045118160659705569771488994088091139$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 147355428219587900809241569199357416360$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 29494377016117864959830409611474872768 1$
   - $g = 25722164822467487606968782524513474113 1$
   - $y = 12943684525141228147648916279798542836 3$

   Секретный ключ:

   - $x = 13505324805915818060644764409960955475 7$

   Сообщение:

   - $M = 476452427851275630991525285948202547 37$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 28533401686733742860900334445675602417$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 17839467364609656393055892932267699646 3$
   - $g = 13633865448472838905624128496627274951$
   - $y = 17412049063722556192685653145640865178 9$

   Сообщение:

   - $M = 14012324389717911570758923084097794504 6$

   Подпись:

   - $a = 21988589582660079633367749710976058694$
   - $b = 23549323717322505907372205285119286774$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 907$
- $g = 766$
- $y = 860$

Сообщение:

- $M = 236$

Использовать следующий случайный параметр для создания подписи:

- $k = 829$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 15x - 9$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 29

1. (a) Расшифровать текст:

ГАДЬАДАВАХАЩДВЧБЧДЭФГЧФАЦЯАЮБАЭАШЧЯЪЪАДФЧЙЭГФЧЭОЪЙГАФЩЦАЗАЮФГЧУЧ
ЩБЮДЪФАДЕШЧБДНЧГЕДЬЪЗАДЧЭАУАВАДЪДОГЯАЯЧЮАХХЦЧЬДАЩЦЧГОГЬЩЭГЕГЪЭЪЧ
ЮЮВОЪФЯАФЯБАЦАКЭЬЮАЧЫЬВАФДЪЬЯЬЭАЯЪЭГОЬАЮЯЧЙДАЬЬФНГЧУЙЕФГДФЕЧДЧГЬ
ЩЭАЯГЭФУАХЕАДФЧЙЭГЭУНЮХАЭАГАЮПДАФНЮВОЪФЯАФЯГЬШЪДЧЮЯЧЯЧФГЪЭЗУНЭБВ
АЦАЭШДОЪЩЮАЭЙЭГФЧЭОЪЙЗЯЕЭВЦАГДОЪЩАУВЩЪЭГОЯЧХАЭЪИЧАБАЮЯЪЭГАБАЮЯЪЭ
ГБАФДАВЭАЯГЭФДЧУЧФЭЦНЬАЯЕУДРКЬБЧДВЯЦВЧЪЙЯБЕХЭДНЮЧЯЭЧХЬАЭЪБДНЧГЕД
ЬЪЮВОЪФЯАФЯБЧВЧВФЭЧХАВЧЙОЯЧХАФАВЪГЯЪЮЮЯАХАГФЧЭОЪЙГЬЩЭАЯАЯЧЛЧГЭУА
ЯФНКЭЪДЪЗАЯОЬАБВЪДФАВЪЭЦФЧВОЮНГЭЪЮАЪФАЭЯАФЭЪГОЪДЬУНЭФЦАЮЧЬАЮЧЯЦЯ
ДЮВОЪФЯАФЯФЗАЦЪЭЬАЮЯЧЗАДЧЭГЦЧЭДОГФЧЭОЪЙЕЯЧЬАДАВНЧФАБВАГНЯАГДВЪЬЩ
ЮАДЭХАЭАФАРЪЩДЬЯЕЭГЧУЧЕКЪГЦАГЦАРЩЬВНЭХЭЩЪФГЬАВЧЩУНЭГГЯАЮББВАГЯЕФК
ЪГОБАЦАЩФЭГФЧЭОЪЙЪФЮЧГДАЧХАЕФЪЦЧЭБЧВЧЦГАУАРЮВОРЪФЯАФЯЕЯХЧЭОГЬЪЫХ
АЭАГЧЧЮЧЯБВЪФЧДГДФАФЭЯЧЮАХЕФНВЩЪДОГЭЦАГДЯАХАЙЕФГДФАФЭЦЧФКЧХАЮЯАР
ФПДЕЮЪЯЕДЕГЗФДЪЭЧЧВЕЬЕЪБВЪЭОЯЕЭЬЯЧЫАУЭЪФГЭЧЩЮЪЕЮЪЭЧЯЪЮКЯЧАДВНФЭЧ
ЧЪФЦВЕХЧЧХЕУЬЪЬАГЯЕЭЪГОЮАЧЫЛЧЬЪЪБАЙЕФГДФАФЭЪЗШВЬАЫЪГФЧШЪЫБАИЧЭЕЫ
АХАЯОБВАУЧШЭБАЮЯЧЮЪЭЦАУВЮВОЪФЯАФЯГЬЩЭЧЫУЕЦОЮАЧРШЧЯАРГАХЭГЪГОЯЮАЧ
ГЙГДЪЧАЯАБАЮЯЪЭГОВЦЪУАХЕГБАЬАЫДЧГОГЬЩЭАЯАДЯФЕЮЧЯГФАРВЕЬЕФНЧЛЧФАБ
ГЯАГДЪВЯЮАШЧДАДЬВНДОГБАУЧВЧХЪДЧГЧУЗАДОЦЭЮЧЯГПДЪЮГЭАФАЮАЯЕКЭАГДФЮ
ЧЯФЕБАЧЯЪЪФАГДАВХГЙГДЪЧФАГЬВЧГЪЭАЮЧЯАЯУЕЦЧДЮААЯЮЧЯЭРУЪДПДЮНГЭОЯБ
АЭЯЭФГЧЮАЧГЕЛЧГДФАФЯЪЧГДАЫБАВНЮЯЧЙГАДЙГЕГДЯАФЪЭАГОЭЕЙКЧЮЧЯЭЧЙЪЭБ
АЭЬАФАЫИНВРЭОЯЪЬЪУАФЬВЧБАГДЪЦВЕХАХАЭЧЬВЯЧУНЭАЪГЭФУАХЕЯЧЕЮЯЪЙЭЮАЭ
АЦАГДОЪББВЪВАЦЕГЬАВЬЭЪЮАЧФНЩЦАВАФЭЧЯЪЧФГЧГЧЮЧЫГДФАЬАЮЧЯЦЯДЩЮЯАРЕЗ
ШЪФЭАЮВОЪФЯАФЯ

(b) Расшифровать текст:

ПФБЫЧЛЭЖЕСТБНЗФТЖФЯЩЫЪМЫСРФЧАЦУЕБМИБЭКБСРЧЙЗЫСЧЛИЭХЫЗЭБРДИГСДЮДЬ
ЦСШМЖЭХБЙЭСЛХАЕЯЖХЧДЧЛЮКДЮЯЭМЗСЪПСЧЮЛЮЮЖШЦСНЕСЗЫЙИЮСЮЛРШХШВВФНЫК
ЗБООЙИЧЛХКЦСФЕКЕЪРОДДЪТЕДАФФПЛЕСЗХКЩФХШЗСФШБНЗЧФБАЭЩЕВБЕСЗЫКВШШЮ
НЦЧИСДЯУОБНСЭЙГКБФШЖЯГОУЫЮАЦУЫЖЭОЛЪЯИШСЮЖВЯЕЛДЪЩПЫЙИЮЦЕКЗГФДЙГОЕ
БГГНРБЮЭЧЛДШВЯУШЭЗЭНЪЗЯЪПШЙЩЩХЕБДСУПКЗОСГЕЧЪУБОЦСМХЭЕНРГБЦЮЕВБЕС
ЗАЮРЧКЭПЬШРБЪЯЪПШЙЩЩХЫЮВФЖАОСФЪЫИЭПСЯКМЯХЫЗЭЭЯЪЖЕСТБНЗЩЮЯЮАЪПАКГ
НУБЭЪЧЮЬЯЕЩЛЪКВЩИЕМГЩЦЮНМЮСЩЮРРИЕПНЦЛДОГФХШГЯЬЛКЗЭОРЭПЬШЛКПБФУЕШ
ЗЦЦЯДЕЮЯЧБАЪФЮПЫФЕБЧЙХЖИЭЩЦЕПБЮИЩЙЭЦЛАЭЪТОЫЙВЭЛХКЕООЫНСОНГБДЪФЕ
ШЦЬДАПБЪОЭЯЕЩЛЪКВНУБНЭЧУЖВСШИАННФДЮДЦЗОБНВЪЖАКЧЭХЮДЧШИДОЪЭПЕБЫЩЛ
ЭИЭОСЛБАОНГБДЪФЕШЯЪПШЙЩЩХГЙЪЩЮЬЮШЪОБЮИЭХБЗЧЦЦКЖЪУОБАЪСЕЭКЗЪУОБЗЬ
ИФКЧЧЛБОВСЖБЖАКЪШЕЦЬСДДАЭДОЗГЦРШИИЩТБИГЕЯАБЖЦСЮШЯЪЗСВЭБНЪЖГОФИЮЗ
ФОЫИЪЩЛДЮЬЧЛЭПНЦПЫЛЕФЖБЮЕФЕХКЗЯЙБЮБНЦЧБЗПСДПЩЬИХЧБЪФЮПНЩЛЭИВЭТБО

ОФОЫЛГЯОЫТБТЛЕБАФЕОСГРЛЮДЭУЗБИГОФИЗЪНСЯДЖЪОПЪЕУЗХЗЖЦСЮКЯЪОПЙРХКХ
КВОЗГПШУНГДМЧЛХОГЧТШУЗЪЖБНИРУПЙДЧСМАЭЪЙЫАЪЮТЮБВЩЮИДДЬЛАДБСХВМЭЭЖ
ЖЙЕЪЗВКЧЧЛЮЙДЧСМАСЩФВКШЩОЫОИРЙШЛИПЪШЮЖФЗШЗЧЦУШНАБРЭМРЧЯЙБЯЪПШЙЩЩ
ХДЖГПСЧКБЩРШИЦЗОЭМЖЩЮЬЖЬВНЫЕЯАХАКЦДЛЕЧЮПОЖЙБФЕОНГЦФБЭГЧЯЛЛЯЭКБЗГ
ЮЮЯДЯФФЕИЭНЮЮЙЩОЛАПЗЩИЦКЖОИГЖУЕЛШЯАУОЫТГСЖБЛГЦКЮКЖИПАБЬЩНБИГЦКЙЖ
ЭСФЕМНФРОКЯЬЦЩЗЭСЖБКЗСЩЦБЕЭЛЯЭАСЗАЧЮФЗГКЫЕЛЬНЗЪОЖЖЕЗОПТЖЦУШНЗЪПХ
МИЦШЫЖЬЧСДШБЪОКПБЪОЮБШЪКВМЪРФЕКОФИЩБЕЮЕОЙДЧСМАЭЭХХДАФРДЖГЬСХДЖСО
ЫТИЦСЦАБЗТГДЦЧЛЩДАФФПЭНЦЛГТРЬКБЯВЧЛАМГРЛАНДЬИЧНЗОЛЮДДЯЖКБЧЯНБЗГЦ
СЮШВЗМЪЮГЩЦЕДКЩФЕЗШЧЦФКЯЮЛЛДВЦСЕКЕЗМЭКБСРЧЙЗЭТГКЖФОДИГУЕАБЛЩЫЖМЩ
ЩЛЭЮРЭХЖЛЭЧЛЪОГЧТОДИЦКЮЙЭОРЭПЬШЛКЛИПЪШЮШЬСЪЙГОКЦЗВЯОАНЗЬЛЭДЖЦКЮ

2. Разложить на множители числа:

   (a) 560134014966577386660018702269

   (b) 542890029835098121100658408669520822712671695837579204387457

   (c) 80122663794217308936330344942232928772539050706671516736989898693617307282457195762019477 7

   (d) 126894344667128904430781911672236471807331019440440934513931363279609212961859299761036761923631740211266584786054755849 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 100833023230899547539404066778446640646224616940146504282973079504980330228921$
   - $e = 17$

   Сообщение:

   - $M = 435644333735249294986163590847239929879770074037333846940845127902697643724 10$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 27830507842538969631125867548375966664 9$
   - $q = 27184521888430728181583056468994356650 7$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 15151108152519253417331653789008702870810512469998256673158624049297048809914$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 28909003234474669115119161224325235650 7$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 13157905820497748019538262100398030583 5$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 25274922761612806265855034786486837133 7$
   - $g = 11113346509219188930139303823617061368 8$
   - $y = 19900052410901174545143174203936548263 5$

   Секретный ключ:

   - $x = 19319168154117887995392754216122461080 2$

   Сообщение:

   - $M = 19738521879045376544608112232390136000 5$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 23290663668017198793700467183713224853 3$

   В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 198734522633845879755377861459283522169$
- $g = 855905539673970172658353020795044331217$
- $y = 804724796657296247923435272454450948 79$

Сообщение:

- $M = 81257211025155925358963283222613108 55$

Подпись:

- $a = 14113261825894354839761318371314668361$
- $b = 11397068183683605639584300966295174 3973$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 733$
- $g = 157$
- $y = 10$

Сообщение:

- $M = 174$

Использовать следующий случайный параметр для создания подписи:

- $k = 727$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 8$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 30

1. (a) Расшифровать текст:

ЙДПЬВПЩШЗЯДЯЩДЯЪДЙУЯОЯБЮНБЕЪЕКЗЫДЯБЩБЕГДЙЬДЬШТВЕДЯЩИЯВЯИТЬЪЕЗЕЩД
ТДЯГЗУЯЯЩДЕЩДТБЕГЬДЫДЙИЕГДЕХЖЕЮЫЕЗЕЩВИИЩЯЫЕГЕЮШЕОЬДДТГЕДЮЖЬЗЫЩЬЗ
ЯЩИЬМКИЫЯВБЗЕГЬКЗЫДЯББЕЙЕЗТАИЙЕВКЫЩЬЗЬАЩТДКВЯЮБЗГДШКГЪКЯИБЮВДГЪЕ
ИЖЕЫЕЛЯНЬЗТЩЭДДЕЩЕИЙУИВКПАЙЬОЙЕЖЯПЬЙЪЬДЬЗВЙКЙЕДДЫЬВЕОБЯЯЖЗЕОЬВИВ
ЬЫКХРЬЬЪЕИЖЕЫЯДКБЕГЬДЫДЙКШЬВЕЪЕЗИБЕАБЗЬЖЕИЙЯБЖЯЙДКГЯЗЕДЕЩКЖЕИЬБЗ
ЬЙКИЯГЯЮЩЬРХЩИОЙЕКШЬЭЩПЯАЯЮЖЕЫБЗКВЫЕДИБЕАБЮБЯЗИБЕВУДЯБЬГЬВУДЖКЪО
ЬЩКОЯДДЬЖЗЕИЙЯЙЬВУДКХЫЬЗЮЕИЙУЖЗЯДЙЯЬГДИЬШЯГЬДЯЖЕБЕАДЕЪЕЯГЖЬЗЙЕЗЖ
ЬЙЗИЕШЗВЮВЕЫЬАИБКХПАБКЖЗЕЯЮЩЬВЩЕЮГКРЬДЯЬЩЯНБЯМИЬВЬДЯМЯКЭЬЩЮВЯЗЮЕ
ЗЯВДЬИБЕВУБЕБЗЬЖЕИЙЬАЖЗЕЯЮЩЕЫЩЬЮЫЬЪЗШЬЭЯЯИГЬЗЙДТЬКШЯАИЙЩЙЕЪЕЗЫЯИ
ЖЕВКОЬДЯЬГИЬЪЕЯГЬЬЙЬЩТЪЕИЖЕЫЯДБЖЯЙДДЬГЫВЬДДЕЖЗЯДЙУДЫВЬЭРЯЬГЬЗТБ
ЕЙЗЭЬДЯХЖЕГДКЙЕЪЕЮВЕЫЬЯИГЕЮЩДНШКЫЬГЕЭДЕЯБИЕЩЬЗПЬДДЕГККДЯОЙЕЭЬДЯХ
ЕДЕЪЕЬИВЯЕДЕШЗЙЯЙИДБЗЬЖЕИЙУЩЩЬЗЬДДКХЩПЬГКЖЕЖЬОЬДЯХЖЗЯДЙУДЫВЬЭРЯЬ
ГЬЗТИБЮВБЕГЬДЫДЙИДЯГЕОБЯЯИБВЫТЩШКГЪКИВТПУЙТВЬЪБЕИБЮЙУЮВЕЫЬАЙЕЩЯЫ
ДЕИЯВЬДКДИЩИЬЪЕИЙЕЙЗЯЫНЙУОЬВЕЩЬБДЬИОЯЙБЮБЕЩДБЕЙЕЗТМЖВЕМДЫЬЭЫДЬЩК
БЕЗШКЫЯЙЬШЬИБЮДЕГБИЯГТОКЗЫДЯБКИГЬМДКВИЕЫДБЕЫЬВЙУДЬОЬЪЕЪЕИЖЕЫЕЛЯН
ЬЗТШКЫУЙЬЯИЖЗЩДТКОЗЬЫЯЙЬБЗКВТЫДЕОДТЬЫЕЮЕЗТЩИВКОЬДЖЫЬДЯЮЖЯЗАЙЬЩЕЗ
ЕЙЫЩТЩЕЫЯЙЬИЕВЫЙЙТГБИЯГТОИГЕЙЗЯБЗЬЖБЕЮИЩЕЯГЯБЮБГЯЖКПБКЕИГЕЙЗЬЙУЫ
МЕЗЕПЬДУБЕЩТОЯИЙЯЙУЖКРЬЩИЬЪЕИЕЫЬЗЭЯЙЬЩИЬФЙЕЩЙАДЬОЙЕШЩБЗЬЖЕИЙЯДЯБ
ЙЕДЬГЕЪЕЙЕГКЮДЙУЖЗЬЭЫЬЩЗЬГЬДДЕЗЮЫЩИЯЯЖЕЩЬВЬДЯЯЩДБКЮГЯОДИЗИЖКИЙЯВ
ЩТПЬВЩГЬИЙЬИЕПЩШЗЯДТГЗИИКЭЫЕЙЕГОЙЕГТИВТПВЯБЬЙТЫКГЬПУОЬГФЙЕБЕДОЯЙ
ИИЖЗЕИЯВЬЪЕШЕЪЮДЬЙЕЙЩЬОВЕДЖЕИГЕЙЗЯГЩЭДЕЪЕЖЕБГЬИЙУЬРЬДЯОЬЪЕДЬЩЯЭК
ЬИВЯЭЬЙКЙЕДЮЫКГВИЯЩЗИИЬДЯЯИЙВДИЩЯИЙТЩЙУЛЗДНКЮИБКХЗЯХДЬИГЕЙЗДЩИЬД
ПЯ

(b) Расшифровать текст:

ББЫДЬДААОЬЬГДТЕДЗЫЧКЖХЧЫВВЖЫУЩЩЖНЛЕЕХЧЕЫЕЛШЕДБФВУИГЮЛОГГЗЛОЫХФБО
ШОЫБЕДЮАШТЗЩСГЕГЗЭГЮДЗЪЖТНПКАЗВГМЩЧЬЦАИНЬАГГСЕБЬЖДКНБЯМЕТДФБЯАМФ
ПЬЕЮГККЛМВКЕЦЖНИДЭКДСЬШЕДЙЮЖЖЙЛЙВЖАИГЧЗБОИЮЗВЗКБФШНКТЪЙРВКГЙЮЖЩК
ГЮЯЦКЫПЕШОШТЯЯБЛОЗВЕГЕПЗЕЮМЙЬАЫЛЬБЭЙБЗВЫЙШББЮВЕПЭЕГЕЫВЪЖОГЗЕДЛЕШ
ПЙДКАМЪУГЖБНТЕЫМИРГБЮЪОШДЗВУГВДДДНЗЫЪОЖДЗЗИЫЖБЕЕЗЩЭЩРЕЫЖДГЕЕМЪЬХ
ЕЕДГЕКЙЫЩЬЕЛГЕЙЧ3ЗУЫДХМРУАЮГСЖДСЮВЙРЛССБЪБЗКЭЬЭЫТЯБМОКБДЮЗТУБКАИ
АЕФГУЭЮГЗКЬАЛСВЕДЗШЛИЮЮВРЮХЗЯДЬДЯБЕРЩЕГОЪВДЮСЙВЪДЙШПДДТЕЦЙЮЩЬЭКА
ЖКЖЮЧЕДШЮЬПЗЦЗЗЛЩБФЯЦЗРЫЗЕЬГЙШДКЕГЬУЙЩЪЫВИТБЗТЯБМНТЕЖЗШРЯНЮЯУГЩЖ
ЧЫВВРЫТЩЩЙДЕРЩИЫРЩПВВОАЖЗШРЯНЛЫМДБЗНЬЩЖЗЖОААЗЯТЕЦЙЮЩШЗДИНТЭЖДЖБЮ
ЛЖЕЙЬВИОЙВЫЖИРЖЗВОАШЗЧРТЭГДНУЛЮИВЬДЛСЙГВВИОЩДБПТЕЖМЩОАЯМАЧЙВЙЗСТ
ЯХПИБЬЕДИЙВГБЕДПКИРЬЯФНТЕЦЗЭГЕЦЗЖИЙБЭЫЖЖДЫДСВЦЖСЙНДХЮСЖВДИЬЙЩЪЫД
ЬЖБГУПЮГЖЕИЖХГСБЬВЗЫДЛЛДУГЩДИЫЩВЙДВЙРМВЕВВЛШЕЙШЮЖЖЙРАИОЙЩЪЪЕЙЬЖЙ
ШБГЗЬЛКТКЫРЬШБЕОВЙЗЖОГАБШЫИВГЮМЯЛЛДДЩЗЕБИИЖЗББГЬКЕЕЗЩГБДЯБЗЯНЬЦЗ
ЭМЕЪЖДРИЕГЭТУЮГДЕЫЩВЗТЩЬЮЕРЕЬАШЕВБЕЫНФЖИЖОИЖЗГРЕШЖЕЕИБИЖОЩЬКЫЛЯК
МЖСЖЩЫЫМВТЭТМЯВЪЖЕОЩЖГЫГЬЫЮСЬЯБМЕЯЙЬЖОЮБФЫЛЯККИРЕЭЖСЕЪВДДСКБФБОЬ
ЦФЖЖЬББЫКЕЖЗЖОЬГЙЮДЩЯБДНЯЕДДВГЬЪЫЗЙВЬДВТДАЮТЬЯХГЫГЦКЫПЕЖЙЗЛЕАЮГК
ББЬЕИОЖЬБИИОЩКАИГЗЯЗОГЧ3ЗТЯЦФЕИВЬЮПЕЖВКИКДЗЫЗТВЬБЭОИЖЗБИЖДЗ3ТЯЯБЗ
ЬИГМЩЧЬЦФВХЕЖЮБЗДЬЕЮПЕЕДЫДЕЦЛТНЕГМЩЧЬЦКАЗВАЖЫ

2. Разложить на множители числа:

(a) 544972720196505493783770032311

(b) 57203706700376979704427150441867263952406640727954937780 2817

(c) 13387390763818616606782461670180645613729571369688401351154638543158627235092886463541344 27

(d) 11156411383549028371084875152691265911329204946063538104280217865436999070695725212656814487871735295907828923211254638 97

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 59361109164080813920761321915565967951684931973640346783642375868649394914989$
- $e = 3$

Сообщение:

- $M = 18308991186209306065091898682676028358618063136244271280420756246618057263136$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 29238625799870330379205130533662430384 1$
- $q = 31252204638229461237896636294478048856 3$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 77916299889183149581591930397418626690052967472264197398734671107884718011792$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 17326336408933118056388671455861430500 1$
- $e = 5$

Зашифрованное сообщение:

- $c = 10859577977417134490129894173979199002 2$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 32096284493936315936463540432853196555 9$
- $g = 15326499028428602428060668484769630638$
- $y = 36473413087286018967308668831798897751$

Секретный ключ:

- $x = 31346690339811574662884802347273518913 7$

Сообщение:

- $M = 30602536001375592208270709567098440937 4$

Использовать следующий случайный параметр для создания подписи:

- $k = 16825363887395397187149515384923375970 5$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 31051033312512899869126474475228167430 9$
- $g = 86740715730858772006012847672981625 53$
- $y = 37389779196925322603407281749698667780$

Сообщение:

- $M = 83095785817338402650160321163097551925$

Подпись:

- $a = 11218557946895709422592160074873168359 3$
- $b = 14670440534997388184454257605486298554 6$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 811$
- $g = 761$
- $y = 705$

Сообщение:

- $M = 306$

Использовать следующий случайный параметр для создания подписи:

- $k = 131$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 13$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 31

1. (a) Расшифровать текст:

МДВЫХМЦИМЙКЬВЖЖТНЖЯЗВЬИЛЗЯЗЯЙКИЛВЗЯЙИЯЮНЗЯСЯЭИЖЗЯЙИЮЛМКИЛМЦЕЯМКЛ
ЛМЬМЦЛЛМИЫИШЮВЛДМЦИЮВЗИДИГЖИЭВЕХЗСНАИГЛМИКИЗДЯЬЖЯЛМЯАВМЦЬЖЯЛМЯВН
ЖВКМЦВМИЮЯЕИЛДБЕДИЖЯЗЮЗМЗНЖЯЮЕВМЦЗЯСЯЭИЛМНЙГЭИМИЬВМЦЖТНЬЮИКИЭНБЬ
МКСЯЖЛЬЯМЯЯВИМЙКЬВЖЮЮЮВЖЯГВДИЗЬИГПИМЦЕШЮЯГЕВТЗВПНЗЛВЗЯМЮЭЮЯАЯЖТН
ДНЕВЗХЙЖОВЕИЬЗХИМЬЯСЕДИЖЯЗЮЗМТЯГЛЮЯЕЕИЛЦЮНКЗИДДНЛЕХТЕИЬБМВВЗВАЗЯ
ИБЯКЗИГЫИШЛЦСМИЫХЗЯБЗЯЖИЭЕЭИЛЙИЮВЬЕЮХДИЮИСЯЭИЖХЮИАВЕВЬЛВЕВЛЯЭИКИ
ЬЗНТЕПЕИЙИММЦИЫИМФЯБЮЯЮИСЯКВКБЭИЬИКНДИЖЯЗЮЗМЙКИЮИЕАЕЛЗИНАЯЬЗЯЭИЗ
ЯЖЯТЕЛВЗВСЯЭИЗЯЛЕНТЕЖКЦВЬЗИЬЗЬВЕЛЦДНАВЗНЫЕЯЮЗВБЙЕДЗЗЖХИМНАВЗЕВЖИ
ЕСВЬЛМЕВВБИЛМИЕЛДИКЯЯИЫХДЗИЬЯЗЗИЭЙИКИЛМЛЦЛИЬЛЯЖЛЯЖЯГЛМЬИЖЖХИМЙКЬ
ВЕВЛЦЙИЮИЖЖЗИЗКИСЗИБЫХЕЛЬИШТЙЭНВЬИКИМВЕЛБЗЯШЙКЯЮСНЬЛМЬИЬЕСМИБЛМЗ
НЖКЦШВЬЗИЬЗНИЮЗНЬЛЖИЖЮЯЕЯИЗЬЛМКЯМВЕЖЯЗЬЮЬЯКПВЬКНСВЕЖЗЯТЙЭНЙКИУГМ
ЯЙЯМКЗЮКЯВСЛДБЕИЗЖЗЯЛИЛЕЯБЖВЖЯЗЙИЛХЕШМЬИКЯЗЫНКЭЫНЮЦМЯАВЬХВЛСЛМЕВ
ЬХЖИАЯМЫХМЦЭИЛЙИЮЦЙКВЬЯЮЯМЗЖЮКНЭЛЮКНЭИЖНЬВЮЯМЦЛЯЛЕВАЯЗЯММНМИЗБКХ
ЮЕИЫЗЕЯЯЙКИУГЗЭЯЕЖИГЛДБЕЙКИУГЖИЖВЕЖИАЯЕЗЗСМИЫХЛИЖЗИШЗВЫХЕИЬЯКЦСМ
ИЙИЛЕЯЮЗЖИЖХЛЕЦВЙИЛЕЯЮЗЖИЕВМЬЫНЮЯМИМЯЫЯЖТКХЮЕЙКВЕЦЗНЬДЖИЯГЭКНЮВЛ
АКИЖЯЯЙИРЕИЬЕВЙИЛЙЯТЗИЬХТЯЕВБДИЖЗМХЭЕЬЙКВЛМНЙЭИЕИЬЖИЭИЕИЬНТДЭИЕИ
ЬЙИЛЕНАВЬЙИЛЕНАВЕЖИЭИЕИЬНТДКИЬЗИМКВЮРМЦЕЯМВМКВЭИЮПЗЯЬХЛЕНАВЕЭИЕИ
ЬНТДЗВДИКХЛМВЛЯЫЯЗВКЮИЛМВДДЗВЛЕИЬЛЯЫЯЮИЫКИЭИВЗВКЗЭНЛЯЫЯЬХЛИДИЭИ

(b) Расшифровать текст:

ИСЗГЯБББЩЮСАЦЬЫЯЛЭЕШЬФХЕЦУЫТШБЩЭПЯАЯДЭГЦЭЮХЦУЬХЯВЪЫЗЫШЦОАЫВПЪЧЫЦУ
ЧХТЛРЪЛМЬТФСЖЯЦЭМОДКЭГСЯЯЮЙТЮЕЮЗЧЩТЬЗЦГЬРДЦВЖСЖЧЬШЯРПЯЬНББЬРУОЗЪЗ
АЪКЬЯЬЭЗМЩЯЮЖШЙЬЮХЛМШФЙЫЮТЪДНВРУГХЛТЪЫББЫЩФУЖБЧМЩБУЭЛШЖЦЫЗХВРФЖЕ
ЖЬПЗБЖЬЪЖТАЬДЮЧБЦЦБЭБЯЯГЪЯЦФЛШЧЬГЛШЖЙСЕЭЕЪФАМВЩФДЩВФЧЗМЖКРЫЫЩФСИ
ЪЬСЪЭТЖЯЭДТЙЬХКШХШФОШЖКДЮЪЕАФГХВШПДМВЯРЫШДЬРАЧЦЩЯЬТЧЬЬФЫЦУЬСТБЙЦ
ГШДУЧЪЪВЯЧЖНДТЪЖМЫЬЬФСЕАЩЗЦГЬОЮХЩЩЭЭШДБРБЬРЮЭГЬЬРЩЮЦГУЬМЧПЯЦЙЕЦР
ЩЗГЬЭЬБМЩЯЮХЩВТПЙОЙУЬКФВРЫЙТХЩФЯЫРШЪЙПБПЯЙНЗБОБОЩЩФЕЕЖЬЧИЭЮЬЧЗОБ
ЦЦЗМЕЬНЙТЖЙШБНВЩЪЫЦЬЯЧБААЦЪЪПЫЬНЙРЩЫЩФЦЬЗФИААЦЫДБВЫФЙЛВАЧБШЮЬЧЗЭ
ЮЮСИХЩЫФВЩВТЩЭСВЮЪЕНДЫФАШБЫЗОТБРЧБОВРФЖЕЩРЗЫШЫЦЧБМЖУЧЮРЮГЭЗЪБЭЪД
ЧЦЖФВЪВРРЙЭЧЦСДШГАЦЕТЮЬЫДТЫУШДИБРЧМФАУЩТТЮЦЮКФЯЦЦБЪГЦГББЬЫФДТЧЬЬ
ЗОЕШЯЧЫЖУЩМЭЦЬЬЗЬЛЯЪЫЕЩЬЭЛЧВРФДТБЯФИШЖЮСЪШЦЩФЖВЬГЫКЩВЮЮЗМЮШЭГШДЬ
ЭЮЪЪЫЮМЫЯЙДДБЖЬСЭЭЬХНЮХВСЪЙЫЮЬХГЪЩЭЪКЬЬАЪБЩВРСДЦЩЫЫЙЦВРРЗЦЧУЩЮЪЯ
ХЭЛХЩСЪЫЫШБЪЖШЕЪЮЙТЦЩНДШБЦЪЪЧЪУЩЖЕЩТЗОЧЬУШЗЫЩЫФБЫГЬШЗГЬМЭЛЪВСЪКО
ВРЩБФХУЬЮРБЬФОЭЮБЮФМЯАСИХВЧЭЗХВЪЪВХЬДЪЮНВЦУЗЛДФЧЗЫГЬЦЗУЕАОБПЫТЪЙ
ШЦКСБОВПЬЗОЗЖФЮШБЪЩЮШХЮРЗМЯЯФКЬЯЮЭКЩДЖФЫЬРЬНМРЕЫЗОЩДЬФКВЩТЭЛМЬГЦ
ЗТАПЗДЫЦЦРЮЬЩЩИЙЫЕШУДПАБОКПЕАЬБФЕЩЯСХАУЩКШЦЫФЕЧЬУШБЦЩФРМЬЩЪЪЛЪЩХ
ЗЫХЕББББПЦУЮЫТХУРЖЕЭЪФЙШБЬОКФЫЩЪЖФВСРГШБЕФДЫЦЬКИПЛЩИЖЭТЭЪЫПЕАИЯХР
УПЗЯВЮЪСТЭПЗДШИЦВЮЬЬЪРЕЦЬЮЪЖШЦТЪЪЪХЙЧЭЦЬШЦЕУЕАСЙТКСЬБЛПЯЪДТЖКГЛШ
АЖЦИТЖЫЭГОВЕЦЗЬЦУГДБЖЬЪЖШЕАЧКЖЦШЬЮЩВЯЮБЧДБЦОЭГЬЫЭЖЬ

2. Разложить на множители числа:

(a) 626096267945161360999213545101

(b) 109496969908466287233052075274258336192505255078060015207855 7

(c) 7835367256432268879203812536069048450302477941522412874886454354969352959829714543953561 99

(d) 10729142495942877517042034321556208900255536279440720151874456399673459757745587701926275614138676723962200746110867653 51

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 366201976804770577216286516551344840424927915009615362301568760581292890075 29$
- $e = 17$

Сообщение:

- $M = 508133767835469050867420304429991895457383462618991528346027007116172963515 5$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 29268776418913536666138021356428967989 3$
- $q = 25110565755959215835740481431342250779 7$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 29839249504556914783462353792860647435649223506996111934601464963846982943336$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 18293660882983007543946595042771870993 7$
- $e = 5$

Зашифрованное сообщение:

- $c = 18385847502982586265857329924082937953$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 23277497991601569929474614061121893647 9$
- $g = 14385909574603073762724543629839758108 8$

- $y = 819463245565025076194454376254470598 71$

Секретный ключ:

- $x = 126253042397591086168259806214972964638$

Сообщение:

- $M = 617895147165414306886090859950607903 5$

Использовать следующий случайный параметр для создания подписи:

- $k = 473920738552800383338176844244507719 61$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 211161000776461736266864385869373178521$
- $g = 140125885465604323736997292673205041827$
- $y = 747105222159146562885379841853909672 90$

Сообщение:

- $M = 840167021492407167366887039841268459 32$

Подпись:

- $a = 100084793655299779945732863928177671332$
- $b = 123311538496691298149157658461680736952$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 827$
- $g = 211$
- $y = 110$

Сообщение:

- $M = 770$

Использовать следующий случайный параметр для создания подписи:

- $k = 263$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 8x - 2$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 32

1. (a) Расшифровать текст:

ЙБГЮЙЧЕЯКНОШСПВБООМДЙЛКНЗКЮДТЛЗКХАШКЛПНОБЗЮНБНОКЗЙКАЙКИИБНОБДЙБИ
КЯЛМДЮБНОДЮЛКМАКЖИЧНЗДНИПХБЙЙЧБНОКЗШПВНЙЧИДЮЛБУОЗБЙДИДЙБДГЮБНОЙК
НОШКНПАШЭБИМШДДЮЙКЮЙЧЛПХБЮНБЯКИБЙИПУДЗЯАБКЙУОКНЙБЪПНЛБЗЗДНЛМООШН
ЙАБВЙКЗДББПЭБВДХБЛКЗЙЧЕОМБЮКВЙЧИДИЧНЗИДЮКФБЗЮЖКИБЙАЙОНЖКЕАКИЮНБЭ
ЧЗКЛПНОКНОПЗШНОКЗЧНПЙАПЖДЭЧЗДЛБМБЗКИЙЧЛКНПАЛБМБЭДОЮНБМНОНЖЙКЮГЭБ
ВЗЛКИЗБЙШЖКЕЗБНОЙДТБЖКОКМЮБЗЮНЮБОЗДТПДЮЛБМЮЧЕМГКОМКАПЮКФБЗЮЖКИЙО
ПИМШДДЮЙКЮЙЧПЮДАБЗББЛКНОБЗЪЛБМБМЧОПЪМГЭКЕЙДЖИДФЖЛЭЧЗМГЗКИЙДКЯМЭЗ
БЙЗИЛАЖОБЛЗДЗНШБХБЛБМБАКЛПНОБЗЧИЖДЮКОКИПТБЗБЗКДГБМЖЗШТКЮДНБЮФББЮ
ЛМКНОБЙЖБЯАБВЭЧЗСКГЕЖЩОКЕНИДМБЙЙКЕАБЮДУБНЖКЕЖБЗШДНОМФЙИЧНЗШИБЗШЖ
ЙПЗЮПИБИКБИЮККЭМГДЗББЮМПЖСПМГЭКЕЙДЖКЮНБМАТБИКБНВЗКНШЯКМШЖКЯКМШЖК
ГЛЗЖЗДЯМКИЖКЛМКДГЙБНДИИКБЕЗЪЭБГЙКЕЮЩОПИДЙПОПЛКНЗЧФЗНЗБЯЖДЕФПИДДГ
ГФЖЛЮДЗНШЛЗФЭЗБАЙДОМБЛБХПХСЛБОМЙАМБДУНЖГЗКЙНЛЗБНЙПЮМПЖИДЖЖКЕАБЙБ
ЖЖЖДБНОМНОДИМШДЮЙКЮЙНЛМКНДЗЙБОБМЛБЗДЮКУОКИМШДЮЙКЮЙЭМЧФЙВДЮКОЮБУЗ
ЛЗФКЙНЛМОЙПЖПЗДЙЧЛИРДЗКЮЙЧПЛКЛАШДЮНЖМДУЗНПВНКИЭКВБИКЕАОИЛПЯУБЮЭМ
КНДЗНЮКЙДГЖКИЙОЧИДЯКИКУПОДЗНЙПЗДТБДКЛМКИБОШЪЛКЭБВЗЮАКИНЮБХБЙЙДЖЙ
ДУБЯКЙБЮДАДЙБУПЮНОЮПОИМГАЮЗДНШЖМДЖДСКСКОДЛБНЙДЛПЯУБЮЛДМКЮЗННЮКДИ

ДОКЮМДХИДЛЗФЛМДЭБВЗОПАВБГИЙКЪЛКАКНЗЗББЮЧГЮОШОДСКЙШЖКЖПЗДЙПЛИРДЗК
ЮЙПУБМБГИДЙПОПЛКЛАШЮЧФЗЖКИЙБЮНБЙДНЛПНОЧИФОКРКИЮМПЖСМАДЭКЯЯАБИМШД
ЮЙКЮЙНЛМКНДЗНЙБДГЦНЙДИЧИЮКЗЙБЙДБИЗБВДОИКЯКЗПЭПФЖПИБЙЙЖМКЮОДОИГЛБ
МБЯКМКАЖКЪКОЮБУЗЛКЛАШЙПЛБОМЙАМБДУУПОШЭЧЗКЙБНОМНЗНШЭБААНЗЮЭКЯПЮНБ
ЛМКФЗКЭЗЯКЛКЗПУЙКГЗКАБЕОКЗШЖКУОКПНБЗНКЭБАОШЖЖ

(b) Расшифровать текст:
АИЭВУОЙХШЗЯСХДАРЛШЕБПЖШЧШМГЫХНОЫЩЪЬГВЩБЛЙДМЕБЖЭМБРЖБМЯУЗШПГЧГЕЫВ
ХМЗТЮУЛБЫЭУАДЫЖСОДФБЗМЗЬХНЙЩПАКОБТВУПЕПЛНЙГЫХУЬАМГЧЖЖЭДЗГБЖЫЬАЗЬ
ГКРЮХЯКЛЗШФАИГШХКЛГЕЯЦАДТЯШАЫГАНГВШИУРИПФКПЙОГБНЫЪШЗГЪЕХЧЪЗЫВБЛС
ЦЫХЕЧШЬТЖАЦЫЖМЖЫЭУГБТРЧМЪПЮУЛЫЪХКЛНЫАНЕНЬБФОДЩЧКЦТТЧУЯЖШФАСЬЯБЙЖ
ББОТРЙЪЭШЖБТАЭАЫОЕУБЖПИНПАСЕБЛАШЦУНЖПГЗЙЫНБХГНЖХУНЖШДУКЗФБРЪАШЖС
ГГМДКБДЧХЦГЪПАКБЧЭЧКРЗЬШЖМИМШЬЙДЧДЙМШШЮБЛСЦХНВДЦЯУЦЫЧАНИЮФЭЧКГТЛ
ХЖБТХЦГИФЫШПЕПЮШРЮЬПНПУЬЫСПБШХУКДЧХАЛЙХЫМИЖЦАЙЙЮЧААЗШСААЗАШЛКЙЫФ
ВУЙГЕЬЦГЖПФХЛЙЫХКЙТТКЦИЭХШССДЬЧОДЫЦАКРЫЩШХЪЕШЮУАЮЧЖУПИХПТМЫМБМЪВ
ТДКЯЫПЧШАЧПЮУБДЪДПСФФГКНДЫЕБЯИИЛПНЫЬГТВЖПЫЬПАСЮЙМЧЪООВЪЖЭЙОДРМНК
ЩШЮУПДЦВУЯДУДЖМЩФЭЧГЧПВШПАЬПЦАЪШГУБЙМААЛЫВАКГШЪШСИДНЧТЖАЭЧФОДПЪЙ
СГПЕУРЖСФУЗГТЭУАЕШЩРГЯЬОЪМИЖДЗМЮЯГУВЮЬШРГЯФБРЖЗЦДКЯГПЩРГЫВППСЪЬШ
ЖГЫЯЕБЕНПЯФМЩШЧНКБПАБИДМБОПАЩГНВЙЬВКОЫХБЗРВШЛКЛГТЭУАИШЦЙНДПЪЛЗЗП
ФКУДЬПТАЗПККРСЪШЦРДЪБТЩГШАСГЖПАНГВШШЖЩБШЕЗГЖОБФОЮЧЕУНДСЧТМЖЫДШДЪ
ЬПУРШПКРПИЪЫПСЪШЮЛГГПИЧЪГПЯУБЙЧШКУИЖАКРЙРЫЦАЫХПНХЧШЦСЖБШДЧЖШМБЦЪ
ЙМЫЙЖВЫДСМИЪЫЛГГПДУАЫЫЕНПТТАКПАЭВНПТЩБПСЕУКЧМИПФКЯЙОШЧЛЙРАУУДЬПЗ
РЖТЧУОДНЧКЛТНЫВРЮЬШЖГЪЪСКПБТККОЫСЕХЖЪЧАКАДЪБЬСЗЖКЧМИЕРЧМЗЭЧХЪЕЪШ
ХАБЦШТПШПЮБЖНБЕУЯИПФФСЗЬЫРМЪЧБИМЪЗЕУБДТХУПГПАКНЖШДНИДХЫЧЩЙРГКЦЮХ
ДКУИЖЕУУДЬПФГОФБСВЕШЬЙСЭЬБЖМЯЬШЖЛЫЩБПЖГЭКЧМЧЫЕРЯЫСЕКЯЗТЧКРТСЭСГГ
ЧБОПИПАУЬЪЪЪЗГЗЭЯЦМОПЮЗМБЬХУПЙОГБМИЬШЖЛЫШЕЦРГЭЪТЙНЬБЦПШПЮБЖНПЯЦН
ДЪЫЧЪЧЕЮУЛЫБШИМЮЩБМАДХЫРГВЭВХЖЩШЕУАБЬПЦАЪШГУБЙБШХГЭЩБРХЗЫШРЛЗМБК
БДО

2. Разложить на множители числа:

(a) 783987262672439308376210077037

(b) 964631581597310875633715878491230014126050090909524722175657

(c) 573976995834504099835878139165874218791184234296014360764870562371454517749633762669691059

(d) 172624818983170990252125337014077041535597672487933562402559900111028214364725119868872000497848413904155334924106444939 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 474929738489377058962858038892198651864894616495421986250520522878496088644 97$
   - $e = 5$

   Сообщение:
   - $M = 193181175362197625999227804820525721803483421431728350076317697358310595628 50$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 259076782726371600862784751349195569803$
   - $q = 249745666969470018518749743263235749039$

   Открытая экспонента:
   - $e = 3$

   Зашифрованное сообщение:
   - $c = 298849483270528051646034845026614045682837862707854373816864420572190085835 17$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 114444507112209604898193856115307332459$
   - $e = 5$

Зашифрованное сообщение:

- $c = 766401300360472533979467130562610850 04$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 290105329531179979618226357294229894847$
   - $g = 177146708326866536095027773340611203799$
   - $y = 237127634061779069795744370572538784362$

   Секретный ключ:
   - $x = 337450181165540476133629840381976136 05$

   Сообщение:
   - $M = 815341119308293449703970330925052450635$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 281837762570657103409261029287111316811$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 172896658018982554243747704533632678843$
   - $g = 124319237821361785331132650752555544447$
   - $y = 904860181508500582675191261174728857 63$

   Сообщение:
   - $M = 164376169571253715573563488249965637785$

   Подпись:
   - $a = 117170064558359970496890638902450305 55$
   - $b = 167144275632652182202101741151625572238$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 863$
   - $g = 718$
   - $y = 669$

   Сообщение:
   - $M = 126$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 249$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 3$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 33

1. (a) Расшифровать текст:

ЮФБЧБЭЫЦАЬВЪЬТЭЪЭЫЮЭЪВВБЭЫЪФЬЬКШУВЗФСЬЭЧГЧЦЧЖФАЩЧТЪСЯЦЪВЩАЪУЩЭРК
ЪЭАЮЭЦЬСБЛАЫЬФЮЯФЩЯАЬАБЭРЭШТЯВАБЬЭТЯВАБЬЭЯААБСБЛАТЯВАБЬЭРВУБЭРКА
УВЗЭШДФЯАЩЭСЯЬЭВБЯЭЫЯЦРВУЧЪЫФЬРЯРЬЮЭЗФЪЬАРЭЯЬЭФЫФАБЭБЫАБЯЭЧЪЧАЛВ
ХФБЭЪЮКЮВТЖФСАЩЧФЭЩЭЪЭСЧАФЪЧЕКТУФСАФФИФСЧАФЪЧСЖФЯЗЬЧФХФЯБСКЩЦЩЧА
БЭЪЧСФЯДЫЧАЭЪУБКЮЭУЯВХЛФЫЦЬЫФЬЯЦСФСЪЧАЛЬФАЩЭЪЛЩЭЮВЗФЩЫФХУВЩЭЧДВЦ
ЬЪЧЬЗВЮЭАБСЪФЬКРКЪЧЬЮЭДЭУЬКФЪГФБКСАФХЧБФЪЧЬДЭУЧЪЧАЛБВБХФЭХЧУАЫЭЦ
СЬЕВЩЯКЪЛЕЩЭЫФЬУЬБАЩЭТЭУЭЫЩЦЩУФЯХЪЮЭУВАБЕКЮЯФЩЯАЬВНРФЪВНЪЭЗУЛЩЧЯ
ТЧЦАЩЭШЮЭЯЭУКЧАЩЪТЪЦЫЧБФЪЩЭЫФЬУЬБЗЧЭЬЭРКЪЭЭБЬФАФЬЭЬФЫЬЭТЭСАБЭЯЭЬ

ВЧЮЯЧЩЯКБЭЯЭТЭХФНЬЩЭЬФЕЮВТЖФССКЗФЪЧЦАФЬФШЬЯЭУАЬЪЗЮЩЧЮВТЖФСЭАБЬЭС
ЧЪАЬЩЯКЪЛЕФЧАЭСАФЫЧЮЭЦУЭЯЭСЪАЭУЧЬЧЦАБЯЗЧЬЮЭУЪФЫВЫФЗЭЩАЫФУЬКЫЧУФЬ
ЛТЫЧЧЭЬАБЪЧДЫФББЛЮЯЧТЭЯЗЬЫЧЬЯЭУАЩЯЧЩЭЫРЯЭАЧЪАЧДЮЭУРЧЯБЛЧУФЪЭЭРЭЗ
ЪЭАЛЬФРФЦВСФЖЛЮВТЖФСЭЩЯВХЪЧТЪСЬКФЧЦФТЭАЭЭРИЬЧЩЭСЫФХУВЧЫЧАБЭЪЧЗСР
ЯЧЬСЦЭЯКЬЗЧСАБЯФБЧЪЧАЛСЫЭФЫЭЬЫЭТЮЯЭЖФАБЛЮЯФЦЯФЬЧФЧЭЬЭБСЭЯЭБЧЪААС
КЯХФЬЧФЫЧАЩЯФЬЬФШЦЪЭРКЧЮЯЧБСЭЯЬЭШЬАЫФЗЪЧСЭАБЧЮВТЖФСВСЧУФСЫФЬСБЭЪ
ЮФЩЧСЬВЪЫЬФТЭЪЭСЭНЧЮЭУЭЦСЪЩАФРФАЪВЗШАЩЦЪЭЬЫЬФАБВЮШАФШХФЖАСЭЯФЬРВ
ЯТЧЭРЙСЧЭБЫФЬТВРФЯЬБЭЯВЧСАФЫТФЬФЯЪЫЖБЭРЭХЧУЪЧЫФЬЩАФРФЖФЯФЦЬФУФЪН
ЮЯЧАЭСФББШЧЫСАБЯФБЧБЛЫФЬАУФБАЩЭШЪНРЭСЧНЧЮЭАЪВЗЬЧФЫЬФБЭЬФЧЦРФХБЛЧ
ЫЪНБЭШЩЦЬЧАЖАБЪЧСКШЮВБЛСЗФРЪТЭЯЭУЧФЮЭБЭЫЭРЯБЧЪАЭЬЩЬЯЭУВЧАЩЦЪВЩЦК
СЬЗСРЯЧЬСЭБСЫУФБВЗЩЧЬЭСКШЩЭЫЬУЧЯАЪВЗШБФАЛФТЭСЭСАФЫЭЬЭБСФЖФБЫЬФЦС
АЧЦЩЯФЮЭАБЛАВХАЭЫВАЪКЗЪАЧЧАЪЭСЗСРЯЧЬУФЪЪАЬЖЪЛЬЧЩЭЫЩЯФЮЭАБЧЫЯЛЧСЬ
ЭСЬЭАБСЪАЛСФТЭСЪАБЧРЭХФЖБЭАЬФН

(b) Расшифровать текст:
ЮИЧПИЭЗАЭЮЩЛАЦДЫЗЪТКЯАЯШЕЩТЧУЛГЙФРВУЗГНДЬЙЭЦЬАКГФНФУЧЗДЩЮЭИИЬКФУ
ШЮКУКЛГКВУЗМУЧХЯШИЪТНГПЮАЬМБЗРВЩГГРИТКЦАВАКЮЬЕЩНОФИФЗЦПИЪААХИФБЭ
КЭЫКЮУАЮКГКЫЦЛВКЮВОФНМНУДУСДЮГЧЬЯЮЭЗЧГПЮНЗДОЕЬЯБББЩТЯВЖАРЦЫКЙЦИУА
АРАЦЙУАЕДЮЪЙЯГШГЦМЯЕЬУМЯМЕГЙЯУЬЧЕДВЧЙЕЭБЯФИГБВТЗЯЪФУИТМШРЛЦЭЧСВЮ
ПДШЗЙБХУЛЯБЦНЗЦЙЪЙНЭЗДПАЦДАЧИЭУЧРИУБЬКЬИШЪЪКДЖЗТПЯАЪРЛНИАЦНХШУНД
ЯОАХХЪЛАЦМБЙЯУЖДНДКСЦЙЪГИТНДУМЦЗОЦМУОЪТЛГЮЧТЗЯЭНРЛЯИЯУШВЮЩТЬВЛАС
ВЮЗАЖИАМАСЯГУЪЗИЪВЧЦМЯЖАЦМЩКЬХИУКШЙЗМСБХВУЧЙППГКХУДГКФАБМЮЭЦЫМОО
НВШЭФНМЦЗЧСЖЯБЫРШТБЩТИЪЛЕИСЦЮЯКБЮЗЙЧИЯЙУАЕХКЙБДАДДТЖЩМАТИУКЩРИТЗ
ЧТЗМЕКЗЫБДЯСИФКДПКМООКЖДЮГКЙДЯЙКЬЭКХФКЯЮЧЙМНДГЧВЮПЪЙКДЯЪСИТМЩУЖГ
КХЙСГКГЧЗЦОГЦЖБШЧОВУЙАЗЗЯЕЗУЕЯАБХИТБХРЙЯИАКЖДОЧРНЩЮАРИВНДТИУДЭНЛ
НАНЖИЭЮЦХНФЛЕИСЦЮБХЯБЮЭСИЩМЩСХЙЗЧТВЯЭВЧЛНЖАСЗЦНФУЙБКГУЖЯУЧСЬЙБУР
ЭЯМАЙВЦДЩЗИЬДЭМЮДИДБЛЫЖЯКБХПЮЧЦВКДЗЯИЗЧСНЯРЪЫЯБДЦЗИБЙЪТЬИБВКУЦАВ
РЛАМАЧВУПДКЫВБХУЮЮБЦШЛГКУУГУКЦТИЪЖЪЖВГЖЧНЛИНДНЯУНЧОЖЯБЫЛВШЙЪМЬЩН
ЪЧИГОЧЖСГКШЦЙБКГНЕАПХЬЯУНДХТЮКДКЫЦКДЗЯИЗЙЧИТЧФУЮЮВЦАНЧБЪСЙЯИЪРИУ
ЙЯЙЯЬНЯКМЯЗОПИЮБХУЙЯХЦШЗЯАШКВЮЛАСИКШЪЧХАМФКГТКХШЙБЮГПБЬНЮУБУЙЧЫМ
МЮЪЙЯЬУДУЖЯДВКЫГНЮУМББЭНЗГБУПИВКГЧКЩЖЪЦЯФКЦТЗВОЪЗЕЮОАССГКДАТАДАТ
ВИОАТЮЯЭЯУМЦЭБАМГШЪФИУБГНМНЙАТЯВКХРЛЩЗГФКЩЭФНЕЯЙБУЗЩГЪЗЭЯЗАЦСГКУ
ЦЬЦЗОНСЩОДХВЮЙЧСИФЗЪКЭЯПГРХЙООФИЭЙДЗИЬНДПЗУДЯНБЪУЪОМДЗЕФММЮЪЙВЙШ
ЙЧИЮБДПИЪБЛКДБКФУЙЩЕИПДФКФУКЩОАЖИЭЙЧЗТТМДБЬВЛАСЗЩЗФММЩБУКЕЯЯАХЛЫ
КЫПКЦЛАЦМЩЙАТЯАКЙКЕЮПШТХЭБХУИВЛАХВУООНЗЦКДЗЯИЗЯНЛЬКФЬМЯЯАЗИБОАЖИ
ЭЙЧЗИББЯЖНБЯЧЦЙБКГНЕАПХЬЯУЛАСИЬУФТЯЭЙАИИХЯАЗИБОЙЧИВОАЖИПНЭЙВГШДХ
НХЙАЗМЯЙЧЬЯФКГПБГШЦРММНЧЖБЮООРВЗКГ

2. Разложить на множители числа:

(a) 732148569571229435412609943819

(b) 11843938437125696620947513447632091037285223724564675188869l9

(c) 772294036684424966520861392185333579984851964959725734193064457472745912116004303402934703

(d) 13405923091275668122120219922303071594363875847873744928202280509076617221881916048272049628480088481370521155202141773 73

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 80634363521539880426488716784115261081752674533670489208903518632474274508793$
- $e = 5$

Сообщение:

- $M = 13611473768234731124184497314752871286442749720759777085091665026209592377748$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 335461816757051850064681838576377967819$
- $q = 205083791904079417012888412673837202517$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 539356070154132757062347434020718593024038060065555345531454644788770896743 62$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 270259592119260188540577987839860326739$
- $e = 3$

Зашифрованное сообщение:

- $c = 255469471428430579667301144946271817408$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 309274863905498600139853980521352960019$
- $g = 248614432998183248535850035974166415814$
- $y = 136985011522301627395183383913378115955$

Секретный ключ:

- $x = 387980994824894271190690049774472013 20$

Сообщение:

- $M = 260652829770680370554309053291154620462$

Использовать следующий случайный параметр для создания подписи:

- $k = 133512388789116648712645107628757329985$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 316371466177111598304673656329277776441$
- $g = 250212022142407570698271351660714446109$
- $y = 171049923888562536384271613109051700600$

Сообщение:

- $M = 131926281217448209261275761189511408087$

Подпись:

- $a = 105333200635882958288009515473347602879$
- $b = 313500066843171027380783817228023468032$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 929$
- $g = 472$
- $y = 101$

Сообщение:

- $M = 728$

Использовать следующий случайный параметр для создания подписи:

- $k = 723$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 3x - 3$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 34

1. (a) Расшифровать текст:

АШДДЮШЧЖСМЖСГШКПЦБДЖЧГЫЯБЫЧБЮЩШАХЯБФНХЫЕПКЕБДЯБШЬДЕБГБАОДБХШГЛША
АБДЯАШАЫШЯЦБДВБЧЫАВГВБГМЫЭДБЦЮДШАЫФБЯАШАЫШДЫШБДАБХАБАХДШИВГХЫЮИЪ
ЧГХБЬЕЭЕЫЭЫЭБЕБГХДШЦЧВБКЕЫАДЕЖВЕШЮПАОШЧХЫЩШАЫБФБГБАЫЕШЮПАОЯВГШЧВ
БКЫЕШЕЕЖЕБАБДЕАБХЫЮДЫДЕЮАФЫХЕПДХБСЕГЖФЭЖДЯБЮСФЫШЯБШЕБГЩШДЕХБХЮБЦ
БГЧБВБДЯБЕГШЮАКЫАБХАЫЭБХЭБЕБГОШЯШЩЧЖДБФБСВШГШЛШВЕОХЮЫДПДХЫЧБЯАШЖ
ЧБХБЮПДЕХЫЫФШДВБЭБЬДЕХАБЦБДЖЧГЫЯБЫВГБЧБЮЩЮБАХОВЖДЕЫХХЯШДЕШДЦЮЖФБ
ЭЫЯХЪЧБИБЯЦЖДЕЖСДЕГЖСЕФКАБЦБЧОЯЖАШДЯШСХЪЕПАДШФДЕБЮПХШЮЫЭЖСБЕХШЕД
ЕХШААБДЕПЭБЦЧЧШЮБЫЧШЕБФШЪБВДАБДЕЫХХШГШААОИЯАШВГБХЫАЙЫЬШШЫЯВШГЕБГ
ДЭЫЯХШЮЫКШДЕХБЯХДШЯЫЮБДЕЫХШЬЛШЬЯБШСЦБДЖЧГОАШЬЫЕЭДБЦЮЛСДПДФБЮПЛЫА
ДЕХБЯЦБЮБДБХЭБЕБГБШГШЛЫЮБКЕБХДШЦБФЮЦБГЪЖЯАШШЫФШЪБВДАШШХАЖЕГЫЦБГБ
ЧБЩЫЧЕПБДЧОАВЧШАЫАШВГЫЕШЮДЫЮБЬГЕЫЮЮШГЫЫЫФЖЧШБЭЩШЕДХБЪЯБЩАОЯХОЮЪЭ
ЯЫБЕГЩЕПКЫАБХАЫЭЫХДХБСБКШГШЧПАДЯШЛЮЫХБВБЦЮЧШЮЫАЯШАДБХШЕГЪБЛШЮДАШ
ЯБЦАШДБЩЮШЕПБДЮФБДЕЫВБКЕШААБЦБХБЫАЭБЕБГОЬАВШГШЭБГДБФДЕХШААБЯЖЖФШ
ЩЧШАЫСГШЛЮДДЮШЧБХЕПЯАШАЫЯЮСЧШЬАШДХШЧЖМЫИЫАШБВОЕАОИДВЖДЕАШДЭБЮПЭБ
ЧАШЬВБДЮШДШЦБЪАЯШАЫЕБЦБДБХШЕЖЪАЮЫЯОКЕБВЖЦКШХХШГАОЬДХБШЯЖБФШМАЫСВ
ГЫФЮЫЩЫЮДЭБГШАФЖГЦЖЖХЫЧШЮХБЬДЭБЯЕШЩАЫЭБХДХОДБЕОЦБГБЧДЭБЬДЕШАОЯАШ
ВБЭЪЮБДПКЕБКЫДЮБЫИХЧШДЕШГБЖХШЮЫКЫЮБДПДБХГШЯШАЫВБДЮШЧАШЦБВГЫДЕЖВЭ
БШЯЖФОЮДХЫЧШЕШЮПВГЫАЫИФОЮЫГЕЫЮЮШГЫХЪЕВЖЦКШХОЯХЯЮОИЭГШВБДЕИЫЯЖЩШВ
БЭБГШААОИХДВБЯАГШЛШАЫШДБХШЕВГШЧХЫЧШЮЧБЮЦБХГШЯШААБШЪЭЮСКШАЫШХДЕША
ИБГШАФЖГЦДЭЫИЫКЖЕПАШВЮЭЮБЕЧБДЧОАШДЕАЖБВЫДОХЕПБГШАФЖГЦДЭЖСБДЧЖЭБЕ
БГВГЫАЧЮШЩЫЕЫДЕБГЫЫАШДШЯШЬДЕХШААОЯЪВЫДЭЯДЭЩЖХЭГЕЙШКЕБДЫБДЧВБАШБД
ЕБГБЩАБДЕЫЯШДЕАБЦБАКЮПДЕХФОЮЦЫФШЮПАЧЮЩЫЕШЮШЬЭБЕБГОШВГШЕШГВШЮЫЦБЮ
БЧЫХДШХБЪЯБЩАОШФШЧДЕХЫЮШЦЭБЯБЩАБДШФШХББФГЪЫЕПКЕБЩЫЪАПХБГШАФЖГЦШФ
ОЮДЯАШДАБДАХДШДЖАОАЫШЯБЩЫЧЮЫГШЛШАЫДХБШЬЖКД

(b) Расшифровать текст:

ЕЦНЮЪЯРНИФДЬНЖСЪТЛЙЮЕЖЦЮЪЖЧЩНФЙАЩЭРЕФЦЮЯДЙФЙПКМПХЭДМЪЧЮЕЫЪЙГКЖЩН
ОЕЖУЛЭИЦКМИИБЪГШКЩИЗГЫНЖЪЩЙТЙШЯЛКАЬЪТФВЧЕИНАШЫПКМСМОШЙШЬТМИЪЪТФ
АЩЮЫНЗЩЬХТВЮУМЩНФДЯКШЮКРРИЯЙЧЩГЧУСЦАЭЕЫЫЭЭЙЖРАОВЙТЖЪГЙХЕЩЬРЫКЧГЙ
ХИЪЭЙУЖОТФКНИЬЗЦГУИФНЯЗЮПЦЯСЬЖТЙЮЕФГЗФЕСЧЛСЫЖЦЯФЙЙУЧЭЙЖЦЭЧЯХЧМЮЯ
ЙЛЙПЕПЦЭЯЖТТАЕЬЕГЖЪЩФНЗДЩЕШГЩЯСШЙРЙТУКЕЯНЩЙЦЕПЦИЭЖТФАДВМФИСЩЯЩЕУ
ЙАКМСОЙФГЭЖТУИСДТЙЦЧЕРЦАЭЬФМССГЯШМЭЙПРМИЫФЫБСИОРКЯЪЫНЭЯЩММЭЮЕПЧА
ЦКПРИЯЖРЬГЧЕЖХОЫЕЗШЙУЯПЧЖИНЙФГШЯЗХОЧЮСЯГЮЬПДИЪЖТЪЙШИЙУЭЦЯЕРНЦКЖН
ЖСВЙЭНИЩЕНЛРКМТЙПЫПЦУРЯЦШЙЩКПРМИЙТЦИСРЙШВОТХЫИЯВХРВЦЯЕРНЦЯМПЕЬЯЫ
УЗЩЬУШЙЕАЖААНВЗЦЛЪЫМНЭЪИАЫЭФЫМФМЦЕЗМИФШЧМЧШТЦЦТЩЕХХГШКЖРЯСВМЩЧЩЕ
ЖТЕФМТЙМЮЕЦНЖИИЦКРЫКЗЯАОКЙЭЖРЕПЛЙЭГТЪЛСВСЙАЧКВЩНСЖАЧЙЦЕЦЦЛЪАСНМЧ
ИАНЮЬЙФЦДЦДФЦЯЬЮТААЧИЬКЬЬЯСЩЕЬТПЩЭЪЗТЪГЧИЖМЙШИЖБАЩДМТЭЭЬЕГЖЪЪТЬЙ
ОЕОХУСГЧЦНЖЬЛМОЩЬЩЦНСВЕЦЖСЬРНЯЧЯЦДЯЪШФЦИДЬЖЩАНТПЦОЧЕКНИЪЩХЪЛЯХОЦ
ЗСДИХНЭБЧЖКЪЩТПЕЯГЭРЕФГМЛЙШЮПЦБФВМУЙДЫЙСЗЬУМКИЪЩСЧЙДВУШЙЭЙМЬЧЭИР
ЦЮФВРРМОЕМЭЛЪЫМЪАЧЬНЧЙБЕФЦИСДСГРУНЙШЕЪЩАЖРЪЙЙУАСЖФЦЭЪЫМЪЧЩЕТХКЬЕ
ХРЖШЬСЦМЮЩМЪЧСЬТМИЯОЙШАУДЙЩЕЪВАТЙШЯСЫНЪДЖЦЛЪЙМУМИЕЕУГОИАФЙЧОЦРРФ
ГМЩЖСЮРРКЪЩТПЕНТПЧЙРДТЪАВЪЙШМФГМОАЩЬЗЦЭЗППРИЦЗЯУЧВЕРГМСВМКЕФШМЪЕ
ЯЩЦШЙСГРШЧФЩСЦЭЩИУУУСАМЩЭСВАРТУШФУМЩЕЕУОГЕОЧЛЪРНФЛИЯЖХЙОДРЦЮЪВЧЙ
ОДБУШЙЕАЦНКСЙФХЯЬЬМЯМЪБТУИДИСГДПЕЖЦЛФВИЦЬЬЖТЧЯИИЫЩНЧЯЖГДЫКЦДГРАЕ
ЦЮОГТЙЙФГХЯМЮЯРГКЪЬЩУГЯЕОЦУЦБТФАЩЫСЪМЦЕЗЦЯЪГЧКГРЬПЩНЪРЙЛЙДЩЕШГЩВ
МЮЙСЪТРВЪШФОЖЪГФЯИЯХЛУЙНКСНРЪЙЙУНЪЗКНМЮЩТКНИДИЫИФОЦЦБСДСГЗОЗЗЦЗФ
ЕЕШНФВЗУВОЫФЫЮЯХХЪЙЬЕСЫИЦЕСНСШТЖГАБВМРВЦЗЙЧЙЭЙСГРОЕФЦНФДЖНЕЪИЦКГ
ЧЯЕНЖЪЪТШМЦКВТЛСЖТЩНИЪПКЛСИЦХАПДЙКДЮЬХДМЯЫФДКЪЫТУЮЯГТНЗЯ

2. Разложить на множители числа:

(a) 75890421652322496612513063849 7

(b) 82951609906558944862256539067735937524006761070367858814658 3

(c) 13491196083994064261449989941077915021869241014638049297031089368269787546631816185715866 03

(d) 75487231461496964845754812228974936616032684492541628863055575919306683671043868618630603917231619917311843927582502200 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 913641256103128304600077243039272796852258730754175608582852116778031424723 17$
- $e = 17$

Сообщение:

- $M = 800843663857531252203623829665275466640448792179395784297268036148141734136 34$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 173876235064643939086299980911675867483$
- $q = 297431964754962998093702120274631072259$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 509739602132053062387922651410597727259432170205835924989496346868277619159 67$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 179161902865873192245217113157162362259$
- $e = 5$

Зашифрованное сообщение:

- $c = 155575985507731695610726031510378372329$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 216672901646064485120781957990326194529$
- $g = 184338398335333149936180259674995982215$
- $y = 112570483764521811302860165658635349780$

Секретный ключ:

- $x = 48703316306413154197326376769932667497$

Сообщение:

- $M = 284204323700579080399235460223133 36330$

Использовать следующий случайный параметр для создания подписи:

- $k = 124901192548223484499387595976608567339$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 227860012581115920244107939046093798229$
- $g = 113016192029761509494848090475800422472$
- $y = 180779374590553661676522254790561024 00$

Сообщение:

- $M = 213518312203782103987597258657640663 18$

Подпись:

- $a = 540074041404588598995005309729412692 95$
- $b = 184471979332310902234232310350062834037$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 757$
- $g = 176$
- $y = 176$

Сообщение:

- $M = 126$

Использовать следующий случайный параметр для создания подписи:

- $k = 55$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 8x - 6$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 35

1. (a) Расшифровать текст:

СУИМРМОЩГЛГРОМЛСЙЖПЪПКГПРБМАМОЖПКГЙМНОЖЛЖУПИЕЙКЛГНСБХГАМРЛЖУЛЖХГ
БМЛГРЬАЕБЙЛСЙЛЖПИМПЪЛЛНГОПЛЖИМАПКМЕАЛФМВЖЛЖЕЛЖУЧГВСЦЛЩЗЖПБМОЯЙГЛ
ЛЩЗПРОЖХМИППГВМЬЯМОМВИМЬЛГЖКГЙАПГЯГЛЖХГБМЕКГХРГЙЪЛМБМИОМКГБМЙСЯМ
ЗЙГЛРЩЛВГРМЗХГОГЕНЙГХМНМПГОМКСОКИСЛМААГИЛГЕЯСВСГБМРМАОЖЧМЛЯЩЙАЩП
МИМБМОМПРСВМОМВГЛЖЦЖОМИМНЙГХЖНМИЕЙПКЛГЙГРПМОМИНРЖБСПРОЩДЯМОМВПГО
ЩГПАГОИЬЧЖГБЙЕЛМПЯГЕЛМЕВОГЗЖИОПЛМАРЩГНРЛЛЙЯСЖЛЧГИУНОЖВАЙЖГБМОЯМК
СЦЖОМИМКСЙЖФСАЩОДГЛЖГЛГЖЕШПЛЖКМГМЛЯЩЙАИОПЛМЗОСЯУГАИЖОБЖЕПИМКУЙРГ
ЖАИЕФИЖУЦОМАОУНГОАЩЗИИСЕЛЙНМПЙГЯЩЙЯГБЙЩЗИНОЙЯГЙМЯМОМВМААРМОМЗТЛП
ЖЗПМИМЙМАНОМЕАЛЛЩЗУЙМНСЦГЗППЩЙЪЛЩЗНОГПРСНЛЖИРОЖОЕЯГДАЦЖЗЖЕПЖЯЖОП
ИЖУОСВЛЖИМАЛГПКМРОЛХСАПРАЖПИЙЬХЖРГЙЪЛМКГЛАМЙЛМААЦЖГМЯЧГПРАМАИМРМ
ОМКРИЛГХЛЛММХСРЖЙППЖЙЪЛМОЕАЙГИЙМКМГАММЯОДГЛЖГЛМНСБХГАНОЖАГЙКГЛАП
ГЯПАМЖКАМНОМПМКБМАМОЖНМИИМКСДГВГЙСАЩГУЙРЩЖЕМОГЛЯСОБПРОЛЛКЩПЙЪНОЖ
ЦЙКЛГАБМЙМАСКЛГНМИЕЙМПЪХРМНОМАЖВГЛЖГАРМОЖХЛМНОЖАГВЦГГКГЛИНСБХГАС
НМВАЙМКЛГПЙСХЗНОЖАГПРЖАВГЗПРАМКМГЛКГОГЛЖГОГЦЖЙПЖКАМПНМЙЪЕМАРЪПЖЛ
ГСПНГАМЯВСКРЪРМЛХРМОГЦЙПМРАГХЙЛАМНОМПНСБХГАГУЙАЯГЙМБМОПИСЬИОГНМП
РЪЖЕЯАЖРЪПЖОМРСИМРМОСЬРКМЯЖДЬРБЙЕСНСБХГАЕПАГОИЙЖИРМЖЕКМЖУЙЬВГЗПК
ГГРМЯЖДРЪПЖОМРСЕИОЖХЙМЛЯСВЪМЛПГКЖНВГЛЪАМЙЯСМРПСВКМГБМЛГСЗВГРБМАМ
ОЖИРМАЖЛМАРЩЗЦАЯОЖЛАЖЛМАРЩЗМРАГХЙМЛВГОДЖРАЛГАМЙГРСВГАСЦИСИМРМОСЬ
РЩАЖВГЙЯМЙЪЛСЬСНМНВЪЖЖЛПЖЙЪЛМУМХГРЛЛГЗДГЛЖРЪПНОМСХСЦАЯОЖЛПИЕЙБОМ
ЕЛМНСБХГАМЛСЕЛГРИИМАМСКГЛПАМГАМЙЪЛЖХРЪЖМЯЖДРЪЛОМВГБМНМАГЦСНОЖИДЖ
ПЙМАМКМЙАЖРЪПИЕЙУЙМНСЦУОЖНЙЩКБМЙМПМКРЩНМРМОМНЖЙПЛЕЛХЖРЪЦАЯОЖЛАИМ
КГЛВЛРЩИОГНМПРЖРГНГОЪРМОМНЖЦЪПГБМАГЦРЪРЩСДМПИМОЯЖЙИЕИМАНМПВЖАВАМ
ОЛЖЛЖК

   (b) Расшифровать текст:

АЬШЭЧАЙЯЪМЯЖРЦЛРСТГХУЬЭЪВФГЫРХЪЖЬРМДУТЮМКАХЯЦЧИПТШЕЬШЪХУТМЦЩОЙЭЗ
ЪРЗЪРЛЕЗШЩКГЭУЯЦАЙШПХБИМТФЪЙЦЙУБИШЯЩНДМЪМГКПЦШЮУЦЫЛЧЮЧЙУБИТУЬЭЪФ
ХФОЖЩБШДЖВУФЯЛИЦЦАЫШЮМЭЛИЭХЕГТДУЯДПЯЩАЬШЪХФГПФТЪЫЪБЛНЛНЩМЫАЬЬЧЙГ
ТХСАЗЬУТНЭЫАМЯУЛУОЬИЕЖПАВШЫЩЬЖМПВЭЙХУЛАЙЬРТЧЕЧЙРБЛНЕМФУЦЪМЯЗЪЦЙЧ
ЯХЦЙЬИПЭХГКЖБЭЧГПРЯЕЦЩЬШЧИПТПГЫШЮМФРПСХХЖЪЬЛХЛЫЮВГЬХЦУЧЕФЮЪЭФЧЬУ
ЕЖЮЦЭЧИЭЬФФЭХУТЬГТШФЕКЖШЪЩЕПДФЦЭХЦУЯЭЧЫХХААУЦОАСШХФГТУМЯЫХБЬАЗША
ХЮЖЬРМЭАЦУФФКИЮГЮЛТЬШДЪТЩПАЬЧЬКАЪЬУШЯЖУЦЩЧДЧЬРЬЕЭЮСЧЙШТФЪДТСХЭУЦ
ЦШДЭЧЪПЪЙШШХКЭБШХЮЯНЬЧАЮПЫВЮЮПЩМЩЕШМЧЧРПАСАЦЬШХФЖПЫЮЭЖЧУЦВЭОРМЛГ
ШЪФЧЕТЕМХЖОЬИВЖНЬХЦЕФЬНЯЭЬУЧЭЕТПХЦИШЯЩЪЕТЫЛЧЮОЙЦВАЛУКЯЛХШЪДЭВУФЪ
ЦМЯМЗЙФЬЧУСТГПФЗПЮЙНЭМШЪГАМЯТЦЖЫАГЮЖХЦЩФУТХТЪЕЧЬРЪЯБЦШДЖНЬФАИЫАМ
ВЯЧЫХХЖЫУЧЦОЫЭХЬЖУЫХЩЙЧБТЯЭСПХДЙЖЬЩАДБАХГЖЦЫХРЩЭТМДЕОЮЪХЖУТМЯФЬМ
ЧЧДЧЙРГКШЮХШДПЫЧЩЩЭТПЭЙШПБФГПЫПЧДБАХЮЭЧАЧЧЩЭМЩФВШЪПГЙТМЛФЙШЩЛДЗШ
РМЭАЦУФЙЭЪУОЦЪШЮЙЬЖЦУФЦЕЬЯСАБОЬУАЙЬЫХФАХЦШОЪЩУЧЧЬЧУРЪЪЩБШДАХЦХЦЕ
ШСХФЖМЫЪДИПЫФЪЭФЬУЯКЕРХКЭХРОЭЛОЬЙАГЖЫХАЩВЦЧЯЛИХШДЖХЬУБЖФЮВДУЦПЪЮ
ЫЦЦШЪЬПЩПЦЪБУТАЪПШЦАЮТЩХЫЫПЫМВГМЦЛЕЙЬЮХХЖНЬПЗЖХЬЛЯЖНЬПЮЖХЬЛАБНРЧ
ЦЭУЯСЪБФЭПДЕХУЩЦЪОДЩЪЖЫКУЪЖБУФОЗЪЦЩЯЖУЫЧЕЮЧЬШДАХЬЙЬАУЦШФЖЛЬЛЯУУР
ХУИГУФЪАЭЬСАРФХХГЖЛЙУГКШЩХЮЙТТМЭЙПШЧЧКЪКШБЭЪЬУЩЛЯЬУЯВХЬФГФЧТИЕДН
ЬЕХЖЬЬЙНБСЭПГУМАГЮЖТЭХЬЯЧЦФЙГЫТХБИШЯУЧЕЫЭЧАЙТЩПАДШУУЪДПЫПЪЯМЫПЪЫ
ПЫМВГШЯЙЧЬШЪПЭЙЧУШНЕХЦФЦИПЭМДИШРПЙЫЪЦФЧЪТЫХДЪПАУАБМЬОВЯТЩШЕИШРХШ
ГЖЕЩАКФЬРБЖБАМЯЕЕЧЮЧГШРМЬАЦУМДКФЬКАЕПТХГКШЧФАЫШЯВЯЙЩЬСАБЧЬХДЪПЕТ
ЙКШШСАЪЕПВЯАЛЙТЪЖЛРПЯЭЧЦЩХЖЬУЕЛАПЫУЯЭЧТМРЙЖЦЬВЙЫУЩОПТЯЩАЙПЮЛЧПЧЙ
УАЩДЯФЧЕТУУЪЙЬЦФНЛМУЧЧЕЧЬШДФЦЬМЮЛЧУЦАЕЪРПЭЙЖАВУИЬРХГКПЮШЬЯХЬФЮЕП
ЫЬЮЛЪЯГЯЖМЦЛЭАЦЙПЯЭЬШПЗКШСЛЮЖХЬЛАББУТАЪПШШБИШЯПЭДПЫЦАВФЬУЕЙХБЮ

2. Разложить на множители числа:

   (a) 10180407838371690810446359184 11

   (b) 8467246035705725464126391740178264886604365835957592131545 31

   (c) 6559495044161336767922256100776719772963766344736919636673331218264005297159375174048339 71

   (d) 9990332375660553861302449528608118328243543971757383474313094559146336654432913477151118067458565629022308985369785767 23

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 62275667496225505867410321573951952164737252904062955828371936642580062720461$
   - $e = 5$

   Сообщение:

   - $M = 385821094270226513335528586947028302999247335172271793608324739478255845520 22$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 22336898999841349624268131819900730909 9$
   - $q = 19897803474747262746102544342036645822 1$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 24323781503358976664322077547605825910587297832696948515924906493132565446321$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 18634337391965558696107745122567362007 9$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 11928567859778602209729614114926995503$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 21686032446805865527367289903657176141 3$
   - $g = 14784437819735638308058616245321116810 3$
   - $y = 91492952062799546233686814027123338 96$

   Секретный ключ:

   - $x = 18409901699516956431126799173683683848 5$

   Сообщение:

   - $M = 10732059055876714387062001404206774566 9$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 18194103261143181393913608441861444165 3$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 26859423964122369025158978728895048358 7$
   - $g = 24594661725119754075234201709512046903$
   - $y = 17195768196077902639842145977110143726 3$

   Сообщение:

   - $M = 11366394874129918273791174692462238515 1$

   Подпись:

   - $a = 37459545326245621912803083958978293034$
   - $b = 21929723492689377474585838305958509542 5$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 1019$
- $g = 875$
- $y = 162$

Сообщение:

- $M = 504$

Использовать следующий случайный параметр для создания подписи:

- $k = 781$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 12x - 5$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 36

1. (a) Расшифровать текст:

ЫУЭЮЦАУЩКЯШЦУРЬЧЯШЦАЬЪБЭЬТЬПЫЬЪЦРТЮБСЯЭЮЬЯЦЩУСЬЫУЬФЦТЫЫЬЯШФЦПЮАУ
ДШШБМТУРБЖШБТУЮФЦЖКАЙБЯУПЭЬТШЮБЩЬЪЭЬШФЦШЪЫУУУЖРПЮЦЫЭЬПЩУТЫУЩШШЪУ
ЮАРЙЧСЬЯБТЮКЯШХЩЬЫТЮЬФЗЦЪСЬЩЬЯЬЪСЬЯБТЮКЬЫЫУЭЬТШЮБЩЬЪЬЫПЬЩКЫЬЫРЯР
УАЩЦДУЩУФЦАРУТЦФЪУЫШЫУЧЯШХЩЯЪЬХРЫУДРЯАРЯЪУЯАЬАСЬРЬЮЦАКЯПЙЩЬЫУРЬХ
ЪЬФЫЬЖРПЮЦЫЭЬРУЩЭБСЕУРРЯРУАЩЦДБЪЮКЦЦРЫЬРЫЙХЫЦЪЦЭЬЯЩУТЬРЩЖРПЮЦЫЬЯ
АЫЬРЦЩЯЫЩУЯАЫЦДУСЬЯБТЮКЯШХЩЬЫРЙРЩЯАЫЙАЮУПЬРАКЬАЪУЫЕАЬРЪБСЬТЫЬЫЬЫ
УЭЮЦШФЦАУЭЬЯАЬЮЬЫЫУЪБРГЬТЦАКРЯЭЩКЫМШФУЫУЪЬУЧХАЮУЭУАЩАШАЙФУЫАЯШХЩ
ЖРПЮЦЫБСЬАЬРЯУСЬЮЯАУЮХАКАЦЖУЭЮУЮРЩЪУЫЭБСЕУРЛАЬЪЬУТУЩЬАЙЭЮЬТЬЩФЩЬ
ЫЬПЮЗЯКШЖРПЮЦЫБЫУБЪЫЦЕЧЦЫУЩЬЪЧЯФУЫЩЦЬЫАУПУЦЩЦЫУФУЫРУТБШЫУЧШЬСЬГЬ
ЕБРЖУПЩСЬЮЬТЦУЯАБЭЧХЪЫЬМБТРУЮУЧЯРУАЩЦДЙЖРПЮЦЫЬЭАКЬЯАЫЬРЦЩЯЦЯШХЩЭ
ЮУЮЙРМЗЦЪЯСЬЩЬЯЬЪСЬЯБТЮКЭЮУТБЭЮУФТМРЯЕАЬЬЫРПУЩЬЧСЬЮЕШУЦАЮУАЦЧТУЫ
КШШПЮУТЦАПУХБЪЬЩШБЬАРЬЮЧЯШХЩЭБСЕУРЖРПЮЦЫЯАЩЦЯШАКБЯУПРШЮЪЫГЦЯШХЩЕ
АЬЫУРХЩЯЯЬПЬМШЩМЕЭБСЕУРАЬЩШЫБЩТРУЮКЫЬСЬМХЪЬШЬАЯШЬЕЦЩТРУЮКЬАРЬЮЦЩ
ЯКЦЪЙРЬЖЩЦРХСЩЫБЩЦЬПЪУЮЫЭЬЩБРШЮУЯАКЫЯШЬЪЬПЬЮРЫЫЬЪЭЩАКУЯЦТУЩЪЮКЦР
ЫЬРЫПЩУТЫГБТЯЮЯАЮУЭЫЫЙЪЦРЬЩЬЯЪЦЭУЮУТЫУМЯАЬЩШБРЖЦЫРЬТЙЫШЮЙАЙЧЩЬЪА
УЪГЩУПБРЦТЪУЫЬЫРХТЮЬСЫБЩЦХШЮЦЕЩЕАЬАЬСТЯЬЪЫЬМЯАЩЬЫУЭЬЪЫМЭБСЕУРЭЬЯ
ЪЬАЮУЩЫЖРПЮЦЫЦЯШХЩЯСЬЮКШЬЧБЯЪУЖШЬМГЬЮЬЖБАУПЩХЮУАЭЬАЬЪЭЬТЬЖУТШЪЮК
УЦРЫЬРЫУЯШФЦЪЫУСЬЩБПБЖШХЕАЬАРЬЧЪБФАУПЫШХЙРУАРЕУЪАЙЭУЮУТЫЦЪЭЮЬРЦЫ
ЦЩЯКЪЬЧЪБФЭЬРАЬЮЦЩЬЫЬЫЪЫУЫУЪБФЫЦШЬСТЫУПБТБУСЬФУЫЬМЩБЕЖУЮУЖЦЩЯКБЪ
УЮУАКЦБЪЮБУЯЩЦЪУЫЫУЦХПРАЭБСЕУРРХСЩЫБЩСЮЬХЫЬЫЖРПЮЦЫЦАЙЯЪУЩЪУЫЬПЪЫ
ЙРАКЯШХЩЬЫУЪБХЫУЖКЩЦПУХТУЩКЫЦШЕУСЬАЙТЬЯАЬЦЫЖРП

(b) Расшифровать текст:

ЭБСЖГЖЬНВЫВЖТИЮЭЧМАЫЪЦДМЛЧШКАЬЯЮБАЙЭЭНЕГЦХЖИЙЧБСЭЮВЭЪДБЧАДЯЖРЩМА
ЬГФИРЖЪЯПЭЭЧБЙЛБЯЭТЖЕЕМЗЭЖГТМЕГВХОЛЫЩТНВЙЬШКЯЕЧББМИРЕМОЫВХОЛЫЩХИ
ЬЗШГМАИЕТГВЖУТРАЫЖХБЗЙЖБЙБМГЭГЖЗЩЭНДЕЪЭОЙЭЧХПЮДЖТРАЕИЗСЙИГБСГЬАЮ
ДЮЗЭХРЖБГЭМАЗДАБЯДЖЯДЛЮЩБТЯЗБВНЛАЧХОЙЛГЬТНЗАМЙЙРЗЮМАОГВДЖАДГСНХБ
ХМНМЗЮММЯЕЮЛЛКЖЪЖЖЫЖХЦНЗИЦДГАЧХРНЖГЬНАЕИЗЗНЛЪЫЭЯЕЧЛРЖМНЫДАКГТМГЕ
ВШДЗЬЩХБЦЗЖВМЙЫЭЫЗМХЖЯПЙКЭЫНИИГВНЗБИБКЦСМВНОЖВЛБЖКСХБИФДАЗЗЗАТЗЖ
КИЫЪЬГГОЖИЧДАНФВЗХМАЬГТНЛБЗХМГГГЬТЙЖНХИЭКЗАДТЮВФДЩКСЗСЙЫРЭДЯЗАУН
ЬМЩХСАЯЩВЫЙЛЧХСИЫНХОГКСЬНМЦЗШЛМДГТНЗЗВТРНДЭТНУДЧЪПЦЛИОКЖЮУЬПЧБЧЭ
НЭЖЧЮЖЭЙЗШКМХЯЭМАЫАБЫАЫВХЗМИГЫМАЖВАГЙКЗЭНДЖЩХЕЯФКЮЖДГДЮАЛЖЭЫДААЕ
ЭМЩЧГБДИЖУООЛЗШГКЕМЧАДЯЖИООЙЮЪБКЙЫБФКВЭГАНЭХБЮКЙЭГЩГАЫИИЙГЗВЯПГЖ
ЪБКМЕГТПГАМИЙЙЧМВНЖХЯЮАЦДГЯПГЖАБЫВЪЪБЙЙЖЪЗМЦЮЕБРЕАРЮГЭЗЕХЙЕЫЩАТЮ
ИЕШГЭЗЕЭЙЛЮЗЮРНЖГТЗЖКСГЙЛФАМХГГБХПЖГЪЩБЙСЪЫРЙЪПТКАЖЭХЛТЛГУНММЩАЪ
ИБЬТНЖБЗЪРАЪЪЯПГЬАИСЧЭЪТЗСМБШПЙЖГТТИЖЧЫРЧЮЧЭЗВМБШКМХЭАРРДГЯННДЖМ

ФНБШЮРКЗЩШЖЕЙЭЗКЙЖШЮРОЭЕЛМНЙЪСТАЛЧБЙЙЭЧЮПОГЯЦДШЛГЮМКЙГТРОАВЫГЕГЫ
ХБЦЕЗГЧЕИЕХГМЛЧШСАКСЪЗЗИЪАСЛБЛХБЦРЮШРНМДШСЧИГЯПГЭЧЮПИЗБГМАМБХДНЮ
ВХОЛЗЧЮГГЛСЫЗЗЖЪТРЭКЪВЙГЫЖЕННХЧЗДЗЖЭСТЯХЩЬНЮМДАДЯЗЖВДЛЮММЗЕГЫХБЗ
ЮКВЫЭЭГАНБЖГЬОЖЛСХМАИГБКНХАШЙКЗЧШБЖХВЮИЬЪИИЙААЪХЕАДЗЛЛЛЗЦАНИЗБЪЛ
АЙАЪДДЗЦКБГДМВНЮЗЖГГЛФВХТЮЗЩЭНЬФАЮЦНЗЦЬПЧБЧЭНЭЖЪЕКЙЭВШБНЗБТЦАЕЪХ
ЖМЛВГСЯЮАВЫЬФАЮМАРЪУНЗЙСШБИЗЧЭРАДЧЪПАЛИШОЙЮКЫБЙЭЧЮПАПЖЮОЛЗЧЮЕЯЮБ
БНЭЮЗЬЗГЪАУНМДГТДИББШМИФЧЫРЧЮЧЭЪЗЙСШБИЗЧЭОЛЮЩЗТЭКЗТНЭДЕХЧАЖЭХМУЮ
ЮБТЯХЦЛРАЙЩЖДАЮЖШКЧЖГСЗЖЗЖМЗВЕЭАКЙРЕХЖИЮЖЪНЖХЯЮЛГЖИВЙЛЮЗЮРНЖГТЗЖ
КСГГЭЗЕЖЛЛХЭТМЙЫВ

2. Разложить на множители числа:

   (a) 1039431386702628955657869910603

   (b) 786620695432238427863703159759979043164110328054171335141881

   (c) 946124333009340688542118788298497088148506104021719413615344218327851554423500092494577963

   (d) 116681682161974366156599641471186783463813467044164385490733792399407012390978009258589685684824372945206210774861443314 7

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 906656133603183174886521250688843960380330221970875961778767857494156106439 39$
   - $e = 3$

   Сообщение:

   - $M = 1404514458473605230549193244489201508074731660993863124899906354563040733066 1$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 21053661335866675292196192203041545889 7$
   - $q = 33093387748830061982000503996203631874 3$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 525689740627202762933805416446379745444719620855790657756665767851689938526 30$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 152075048049834458665069252182168312487$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 132889509209913762631554770003591769425$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 25368607117040146943762592831456432 6967$
   - $g = 18299327927836904815411047902173965151 0$
   - $y = 20190972328480457248165782246409794046 6$

   Секретный ключ:

   - $x = 72723154071796512677406500536317993751$

   Сообщение:

   - $M = 34933286218695727782030925397903726429$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 75547107166835192394736753833786582259$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 330598251509493944670466062466936579433$
- $g = 277719083753087756337906742215867675945$
- $y = 131666138242392351616211407210773326374$

Сообщение:

- $M = 557907540816838026334929608388723972 89$

Подпись:

- $a = 860277783270581840610114436874461864 57$
- $b = 129611537435547640150998646510895868335$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 967$
- $g = 11$
- $y = 257$

Сообщение:

- $M = 654$

Использовать следующий случайный параметр для создания подписи:

- $k = 313$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 16x - 6$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 37

1. (a) Расшифровать текст:

ГВДГЯМАШГАГЧГУЭЖЯЬАЧЖЪТЗГЦЕЗКГЕГНГГЩВГВЪКГЕГНГЬМЪБЗЪЦМЪЕЗВЪЖЪЗЫЪ
ВЭЗСЖМЪЖЗВРЮГЙЭЛЪЕВЪЬКГМИЗЪЦГЦБВРЧЗСДГЧЪЕСЫЪЗРБВЪМЗГЫЪВЭЗСЦЦАЫСВ
ИЯИЩЗЪЦЪЧГЬЭЗСЖЖЫЪВГУЩВВСМЭЗСЖЖЕЪЦЗЭНЯБЭТЮДАУВСДГЖАИНЮЖБЪВЕЬЧЫЭЖ
СЗРЖЯДЭЗВЖЯГУЩГМЯГЮЩГЕГШЧЖЭБЦЭЕЖЯБВГУГМЭОЪВЭЦЪЬГДЖВГЗДЕЧСЪЪЬЧЗЕЫ
ГЩВИЯЕГЩЭЗЪАБЗЧГЭБЖБГЖЗЧЮЖИБЪВЧГЗЕЩЪЧГЕЪВЦИЕШЧГЬЧЕОЗСЖЗЪЦЪВЪЬМЪБ
ДГДЩЪНСЖГДЗСЧЕИЯЭЦИВЗГЧОЭЯБЗЯЧЕЩАЭГЗВЭКЪОЪЕЬГЗЩЪАЪНСЖЗЯЭБГЦЕЬГБА
УЦГЧВЩИЕСДЕГЮЩЪЗЖБЖГЦГУЭЧЖЪЦИЩЪЗАЩВГКГЗВЪЖГЧЖЪБЦРАЖВЭБЖГШАЖЪВГЩВ
ЯГЫМИЧЖЗЧГЧАМЗГЩГАШМЪЖЗЭЗЕЪЦГЧАБГЪШГДЕЭЖИЗЖЗЧЭЧЧГЮЖЯЪЭБДЪЕЗЕЭЛРЕ
ЪНЭАЖДГЖАЪЩГЧЗСЖГЧЪЗИЬИЕЭВГЗДЕЧЭЗСБЕСУЭЧВГЧВИЧЩЪЕЪЧВУЭГЖЗЗСЖЧЪШГ
ГЗЕЩЪЖЧЪАСЭМЧЭАЖБЪВЕЬЩЪЧЗСГЦПЧЭАЪБИМЗГЦВЩЕИШГЮЫЪЩЪВСШГЗГЧГВЦРАЪК
ЗСЧЩГЕГШИЖБЕСЪЮЭЧВГЧВГЮГВЦРАГЬИДЕБЭАЖМЗГЗРЖИЩЕСЯЯЫЪЗЪЦЗГДГЯЭВИЯЗ
ГЬЗГЦГУЦИЩЪЗКГЩЭЗСМЗГЖЯЫИЗЕГЩЭЗЪАЭЗЧГЭЬВИДЕБЖЗЧГЩЦСЯЭБГЪШГЧГЬВБЪ
ЕЭАЖИЦЪЩЭЗСЪШГАЖЯГЮЭЭЖЯЕЪВВГЖЗЭУЩЕИШЗРБГЮЕКЭДЖЧЪАСЭМЖЯЬАЪБИВЪГЗЯ
ЫЭЦИЩСБВЪЦАШГЩЪЗЪАЪБЧДЕЭЖАИШЬЬЩЪЖСВИЫЩЗСЖВЪЖЗВИВЪЦИЩИЖДГЯГЪВЪЖАЭ
БЕСЭЧВГЧВДГЪЩЪЗЧЩГЕГШИЦЬЬЗЪЦЖАИЫЪЮЖАИЫЭНСЗРЭБВЪДГЗГБИМЗГЗЧЪЕЩГЕЪ
НЭАЖЯЯЖЯГЕГГЦЖЗГЗЪАСЖЗЧЩГЬЧГАЗЫЪВЭЗСЖВВЪЮЗИЗЖЧЪАСЭМЖДАЪЖВИАЕИЯБЭ
ЖЧЭЩГБЭЬИБАЪВЭВЪГДЭЖВВГШГЫЪВЭЗСЖДГЧЗГЕЭАГВЩЭЗКГМЪЗЫЪВЭЗСЖМЗГЖЯЫЪ
ЗЦЗУНЯБЗИНЯЗГМЗГДГЩИБЪЗЖГШАЖЗЖЧЪЕВГЖГШАЖЗЖГЗЧЪМАЯГШЩИЬВУЗБЕСУЭЧВ
ГЧВИВЩЪУЖСЭВЗЪЦЦЗУНЯЭБЗИНЯЗЪЦЬЧЬЕЗЗРЦИЩЪНСЬВЖКГЩЗЪБВЪЗЯАЭЖЗЕЭЯЦР
АЗЕГВИЗГКЦЗУНЯЗРБГЮДЪЗЕВЩЕЪЭМГЗЧЪМАГВКГЗСЕВЪВСЯГЬЩИБАЗРЫЪВЭЗСЖЩЬ
ЗГБЕСЭЧВГЧВЗЯЩГЦЕЦЕРНВМЗГШЕЪКЭДЕГДИЖЗЭЗСГЯЬЭУЭВЦРЗСДГЗЧГЪБИДЕГЧГ
ЫИЪЪВШЪАЦГЫЭЭ

(b) Расшифровать текст:

ЧФВЮЗУТАДТЪДЫЫПФЮЬШСХХЮБММЦТЮЖМОЬИЮПСВМТЪНШЮЧИЮЫЮУЙКЭСПФСУЮПИЛВС
ГВОШАРТСФАКИУЮЗКТФШЛРИРШВФГЛЭЫОХЖТСЕХЕЮЖКЩЯЭЮУТСТДГШПЮИТМОШГОМРБ
ЮЙЪПЫЫППИЬЩРЛЕЮЫПФСЩЬКОРШИМПКЬЫППОШВЗФЪВДРФЛЭЫОХЖЫЮОМРГЭПЩЯЬИХЯН
ЕГХТЛЧБКТФМЗНМКЬЮДЛУГЩХШОЛОНУЛЫСЛОРЪДОВМУДНХФЯЫФЧРФЖЗПЪНИРЙЮЮЗФХ
ОСЫПМОЮЩНФЦЫЗКЙЛЦЙДЛУГЩРУЦУБХУУМФКЙРЮШПЪХЪЬЗШЕЧГПЪБЮИЗЭЖЫЪЗТРЬЫП
УСЫНПМФЬЫДМУШИЮШПЮВХШИСЫТЛСБИЮИОШЗФТРЫЮШМИУДУЦИИЮНШДЫЫАЧКАЫЙЩЯГЭ
НВЛЕШЗЧИТДМОЗАШУЩЕГЯЙЛУТЗФЙЦЩЕЗЩУГОЕХЕЮЖКТСВЫШУРХЕТПЙШВОМРЪЗЗЧЗЖ
ЙУТЕСДЕЪЗЮЬЖТЛБТФМДЯЫФЧЦИЪТЪЖЬДЛКСТДТПОЬИХЯНЪАФМДУДУЦСФТСЧЛТЫНОЗ
ЮЖРЙОШИЭШТХОКТЛЕШЭЙИБИКПКЧАНЕЪХГКФСЯДЖХЫХЪМЛЕХЖКФЫХБЗМФЭДДОТХЖФХ
БЭЪТЕЫЪЭМЧЛЗБРЩСЯЖКСНЭЫФССВШЗЮОШЭЙЛЕХЖКОИЬЗМПМБЮЖПНБВЙЛИБТДХХГЬР
ФЦЗЮОЩИСЧХФЛВТЖОЕЮЖРЩХБАФГЖЮЗХЛУХШЭЬЪШГРЙРШАРЙФВБРШПВЖКЙХМГГЧЛЙГ
ЗИЮЫДНПНЪДЕХРШЧХЛЯБЕРШССШЭИУВТУФИВЖХЛЛБТУСКЫВПМДВФЪСРХИМХЕБАРРШЮ
ЭКФЪВДГУСЦГРИЮЫДДФДАСОХЛТЛРЛЛВТКЙЮЕДЖПХМШРЧСТЗМППШБЙММЪВКУХГОМФП
ШГХЩЦЮЧТЛСТГПУСШВСХЕЫЫППИЬШСТЕЮИЩФЛХШКЛЪВДСЧЛИБРШЯШВПМУЧЪЗТЛВТСХ
ЖШЧЗТЯТЗЗРФХВЮПРЮЧЭТФЯДМХМЭЫЗШХХЛСХУЪАПЬСФЮНШФЭЮОПЛБВТГИЩЮДФСТГР
РФЮВПХБССНШДЫЮЖЙТШЗФХОХИОХЖХПЗЙЮФЫТНХМДУЛЦУЖКФИТЪРТЙХГГВОЯДЖХФЯЫ
ФГНТЫЩМУГЮПШСБШРИСФЮФГФЮДГАЛЫШУМАВДОХЛЬЖРЛЛВЫНУЛГЗСМОГЗСХНЮЮФГПВ
ЙЪСЦЮГКЦУХЪНПФМШСХОЭЫТЛСБИКШЕШЪППРГЕЗЩУБАЙТПЭЫРЩИЖЪРЙСЫТПХХЛЕТХН
ЧЮНПРВЫГЦСАЪМХПССНШИАЪКЩРЮГЗЮИУДСХПШГФГТАДУЩУЮЫПЛИОЗЮЮХЮИЗЦИАТФВ
ЛБЕТЙЛЫЗКЦИАЫГМФШБУОРОНФХХЛЗНЪЙШБМСРФБЗНЛВНЗШХЭДОЪСДЮШМУГЗСШЛСДХ
ЩИИЮНУИЭЗФЧЛЪАРТЛВЫГМССЭПИЦФЙКОДТБЗФЛХВФХЙШЭПГПЭЫДЛЕЮЫГЪЗХИСЧЛВГ
ЗМФЮЗНМКЬЮШТСТБЗКСАЙМЪЛУБЖМОЭ

2. Разложить на множители числа:

(a) 6703792535743327467606484881 73

(b) 878905246478308085063073674678641007779507036964353492769357

(c) 95392544687693588394060521430476414714246661676188850596971303420388116951937197861272014 1

(d) 1347266415821039052297551312317957839587180147074767694615678996003753490398480344588688651434667621713858237243036012319

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 67785079500367725220460334300408570178760650402190688948072881934638713619813$
- $e = 5$

Сообщение:

- $M = 4974175729694199236813107132891558228508052765416665147534926527238950433918 2$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 230027937753373712002213278241370039137$
- $q = 33852969654565945590006161142381272089 7$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 427248968157253534622754047817031693327119089709120465816138138641977681553 00$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 208799378738087126909515057793589503909$
- $e = 17$

Зашифрованное сообщение:

- $c = 159255668109418122677535487684689051105$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 28500034129475198137380448206774231654 7$
   - $g = 72090398684483048123754445202806970631$
   - $y = 21635768548144295839371043413083020 2322$

   Секретный ключ:
   - $x = 17772081312138121940839733800343219 6913$

   Сообщение:
   - $M = 13448593944854685198980909991929246 0870$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 21150801686107757792314651739715708 4711$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 27887711201810079400396421239528695 5699$
   - $g = 20275182313418978385725388081343401 5409$
   - $y = 19954392563712489543277405175755611 5329$

   Сообщение:
   - $M = 78037352550696988641096089756925370120$

   Подпись:
   - $a = 22348610170869041154047597347113008 9223$
   - $b = 18776771055025550654287297928477002 0309$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 727$
   - $g = 424$
   - $y = 590$

   Сообщение:
   - $M = 613$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 205$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 10$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 38

1. (a) Расшифровать текст:

ЙДЭНЕЛГЙЯГЖЩЕЖБЛЙДЭРВЖЦАЗИАЗЖЬЕЪЙЪЖАОЭЗАЖЗЭИЭЬАГДЭЕАЛЙВЖИАГЙЪЖАР
ЫАДЭЕЖЗКФЖКЪЭГАЪКЦИФДЛАЙКЭНЗЖИЛЮЭВЬЖЗИЖЙЛЕЭКИЭЩЖЪГАЕЭЩУГЙЪАЬЭКЭГ
ЭДЪЙЭДЛЖПЭДЖЙКЭКЙДЕЭЛЪЭЬЖДАКФПАККЭГЕЖКВПЙКЖЙГУНГЖКЖДИЙЙВЯУПКЖДГЭ
БРАЭЗЖЬИЖЩЕЖЙКАЪИЭЯГАЙФЪДЖЦЗДКФАПКЖДЕЭВЮЭКЙЩЛЬКЖЩУКЛКЮЭЕЭЪАЬАДЖЗ
ИАЙЛКЙКЪЖЪГДИФАЪЕЖЪЕЗИАЕКЩУГДЖАДАИЖЬАКЭГДАЙКЭДАЙВИЭЕЕАДИЬЛРАЭДВЖ
КЖИЖЭЖКГАПГЖГЦЬЭБЙКИЖЫЖЪЭВЖЕАЪАЬЭГАЩГЫЖЬКФЩЖЮАЦЪКЖДПКЖАДЭГАЙГЛПБ
ЗИАЦКАКФАЖЩГЙВКФЩЭЬЕЛЦЙАИЖКЛЪЙВЖИЭЖЕАВЕЭБАЙВИЭЕЕЖЗИАЪЯГАЙФЗЖКЖДЛ
ПКЖЕЭГФЯЩУГЖЭЭЛЯЕКФАЕЭЗЖГЦЩАКФДЖГЦЩЖЪФЛЮЭЕЭВЯГЙФЩКЦРВЭЗЛЙКЖЦЩГЮФ
ЦДКЛРВКЖГФВЖКЖЫЖАЮЭГГПКЖЩЭЭЗЭКИЛРЮЭЕАГЙЕДАГЖБВЗАКЕЙВЖБЬЖПВЭЙГЛНЖ
ДЖЭДИЭЙКЭЗЖИЯАГЪЙЭДЖЭЙЭДЭБЙКЪЖДИФАЪЕЖЪЕКВЗИЖЙКЖИЙЙВЯГДЖАДИЖЬАКЭГ
ДЖЙКИЕЕЖДЯЕВЖДЙКЪЭДЖЭДЙЗЛЫПЭЪУДПКЖЖЕЖЕЭКЖГФВЖЕЭЩЭЙЗЖВЖАГЖАНЕЖЭСЭ

ЯЙКЪГГЖПЙКЖЙДЭКФЙЖКПАЙКЖЫЖЙЭИЬОЩКЦРВЕЭНЖКЭГЪЭИАКФПКЖЩУДЖЫЩУКФЯДЭ
РЕЪЫЕЛЙЕЖДЩЛЕКЭВЖЭЫЖОЭГФЩУГЕАЙЗИЖЪЭИЮЭЕАЭЗИЭЙКЖГААЙКИЭЩГЭЕАЭЬЪЖИ
ЕЙВЖЫЖИЖЬЖЕЙКИЖЫЖЬЖЗИЖЙАГЙЪЭГФАПЬЬФВЕЭЛКАГПКЖЩИАЕЩУЪГЪЫЖЙКНЛЭДЭГ
ФВАЗЛЫПЭЪАПКЖЬЭЯГЖЬЭБЭЫЖКВАЮГЖЪГЕЖВГГЙПКЖЕАЖВВЖБАЯДЭЕЭЖЕАЕЭЙГУНА
ЪГЙКИАВАЛЙЗЖВЖАГАЙФАЙЕЭКЭИЗЭЕАЭДЙКГАЮЬКФЩГЫЖЗИАКЕУНЪЭЙКЭБДИФАЪЕЖ
ЪЕЙАГФЕЖЩУГЪЙКИЭЪЖЮЭЕЕЖДЖГПГАЩЖЪЪУЙРЭБЙКЭЗЭЕАЩУГЖЬИЭЕЙВИЖДЕЖЙКАЦ
АЖЙКЖИЖЮЕЖЙКАЦЗИЖРГЖЕЭЙВЖГФВЖЕЭЬЭГФЪЬИЛЫЩКЦРВЗЖГЛПЭКАЯЗЭКЭИЩЛИЫЗ
АЙФДЖЖКЕРЭЫЖИЖЬЙКЪЭЕЕАВВЕЯЩВЕЯФЗАЙГЭДЛЖЩЖДЕЭЗЖЙГЭЖЩУВЕЖЪЭЕЕЖЫЖЗИ
АЙКЛЗЖЕЖЩТЪГГЭДЛПКЖЗЖЬЖЯИЭЕАЕЙПЭКЛПЙКАДЖЭЫЖЪЯДУЙГНЩЛЕКЖЪСАВЖЪВЕЭ
ЙПЙКАЦЖВЯГАЙФЙГАРВЖДЖЙЕЖЪКЭГФЕУДАПКЖЗИАДЭИЕВЯЕФЬЖГЮЕЩУГЩУДЭЕЗЖЙК
АЫЕЛКФЕЖПКЖЫЖЙЛЬИУЕАЯЛЪЮЭЕАВЯЙГЛЫДАЗИЭВГЖЕЕУДГЭКДЖКОИЭРАГЙФЗЖДАГ
ЖЪКФЗИЭЙКЛЗЕЖЫЖЙУЕААЯЩЪГЭЫЖЖКЗЖЯЖИЕЖБВЯЕАЗЖЪЭГЭГКЖГФВЖЙЖЙГ

(b) Расшифровать текст:
УДЧИЖКВОЯДФВХЪАРМОСБТЪЗШУЗЖЦМНОГПЮАХДТБЗРЧМЖЯНЧХХМИВЦУЮТЩМШЭЭАЕЛ
ЯДЕИШДРВЛТОТЫОЯДФВЦЮЯРВЙЭАРЦСЮЛХЖЦМЮТБМШЛРЖПГВКЗМЧМЖВТБЖЙВТЯПУЯН
ХЯРДТВПИЭЦФЖФГЙУКРЗЙЖЖПЫСШЙРЗЙЖИРЮСФМЗЮУХОТГЖШУЕЕМЭБДЧРЮЗРЩТБОКЖ
ЖЮБЛЖПГВКАУАДЕЕШХИКВМЕБКЧЯИБНЧТВНФЧОГЛТЪРМБТБМЮМРБЖУКЖИХВБЧДТАВК
АТЭЮУЧТХЕУЭРСДТЖОЮЕЖЪФХЮПЭЗФБКЫЙЭДНЖСФБДЭЪХЮЖГЦМДДЖМЫШЗЧСХЪЖГЫХМ
КЦЙФЙРШТВИРНСХЯРЩЖЮМПЭСЭНГРПЮАЗЧЦМУЗАТТБМЩЙВБЛЧХХИРЭЕАОЮЭХХНФЕЯГ
ИЗЕПШЮРБПФБПМЙБОДЪРВПЪЯЕЛЗЗОЙЬЙРУЕАЪЧЗОЪПИЪЕЛЗЙДМБЙДЖЙЬБПГЖБЖКЮУ
ЮЗМЖЙАВПЗТЬЛРБМЫКУЗМЬДРЕЗТМЖЭМЪЙЙЦЕЫДЙЯТУКПНЙУКТГИБОДЪСЭДМЪХЫДГР
УЗБДЖОЮЯРМСШИФИЬЪМРЩМЫАРМАВКГЗВИЖРЦЮТДНЦЯЪПЖЖПХАРЧПЮКУБЙАОКВЙТДД
НЙУКУЖЙАВПЗМФБНГЦХИГРМЪКПММЫКУСХЗДФАХТКФДЧБЖХЩТЮЖРВЫЭДПИОТОРЧФХИ
ДГХЯДФРЖЫДУСРЛЙЗДТЭКПЬЬЭБОИХЯОКАЙВЙЗШТТКЙЕХВКФЩССЧНВФГЖКЖЦАБОВСЮ
ИХЖЖХЗЮЭЫГГФЕЙЧЮРЪУЮЮЗЩЙЭДЗДТЦЗРЧСЭКОИРЭБДЩИМЖКДТФБЕГСФГРЕТЬЙЖЧЙ
ЭАШЗТЬЯРЩЧТЧХММЫНТИХБЖРЮЗАИРЗЙШИРШТЗБПСЛФМДГХГАКЗАЮНДГНБОДКЕЮМЙГ
ЗЮЖРЦЙЫЮЯЗТТМЗБЕВЪЬЯСЭЗЖАРХЙЦЕСЖПЙБТБШЗЦТЯМЗЯТВКТГЗЮЭДМБЗКЭЛЬКУ
ЯЖЛЮОЪХВБУШТФКДРРЧЛУГРТДПЭУАКДВХЪКЕГРБЗСЕМХГЖЪЗЮНКААЭКПЪУЮЙТЧМЫН
УЧЙЫШКМЧБЗДЦТУПДГФЗЗРВУАКУЪЕЪВЗЗХФДФИРЛОСЕМЗБУВСЪКТБПХЙМИИЪЖПИКЭ
КФЕЦШОЮАМИЙКЪИХЙЮШМШЙПЭРВШОИХМБМЯЕГАФГМБЮРЭЩЫЪЖЪНЭБУЗПЮЭРДФХЮРЗЙ
ЗБУЗЖХНДГЙЬЭЭАУАДМБЩХМРБУЮОРБЖЯМХЖХШДУГПФОРБУЮОРБУАДЗКПТМРЖХШЪ

2. Разложить на множители числа:

(a) 325387795511600236380809943611

(b) 1180661851830322849591025402834347152720404425368458684758451

(c) 19414084503716948376319941285463985326514277758693349292853636345557117221250213100883693 11

(d) 13512242259365148621793048619984357322759047080444948559443300535157371654340065414027033839854013472187959513915956690 51

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 594834481397303623680048784156035406510807778381788268175509118836032704738 47$
- $e = 5$

Сообщение:

- $M = 424553688530143576064105735771329123316363767484663099490012969681522166271 52$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 27531578958767200024628633854729344 3499$
- $q = 32669829663520010593306477432451668504 1$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 55948906328710930791986445190361840617330671256680321085477648809731967875153$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 14971862113818014034045789778365662588 3$
- $e = 5$

Зашифрованное сообщение:

- $c = 87104347894364162700541466948910873990$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 337864069844938540102602393400118205701$
- $g = 64700200256598088619429893457823010715$
- $y = 16654761818457627767937154322505729505 3$

Секретный ключ:

- $x = 24394234571875471566822399242894292052 6$

Сообщение:

- $M = 28676992219453865947002802611954800108 0$

Использовать следующий случайный параметр для создания подписи:

- $k = 76619199700716864355092042074779469479$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 20796488612580025964460832780504681764 1$
- $g = 62697103713473464164960929734126074763$
- $y = 26401643246996603058369348001049761580$

Сообщение:

- $M = 10293487154688809402668104278176603831 1$

Подпись:

- $a = 13590455433323723618260453432486687239 3$
- $b = 17962156923254382606796571617350360444 8$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 773$
- $g = 239$
- $y = 558$

Сообщение:

- $M = 54$

Использовать следующий случайный параметр для создания подписи:

- $k = 603$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 8x - 11$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 39

1. (a) Расшифровать текст:

ДДТГКБЗЬЖВЬДЯГИВЕШЕЫТИЩЬВУЯОЕЙГЬДДЬЕЙИЙЩВДЬЖЗЬЗТЩЭВЕШДТМИЩЕЯМГЕВ
ЬДЯАЩЫЗКЪКЩЯЫЬВЖЗГЕЖЬЗЬЫИЕШЕАЖЬЗЬЫЕЩЕАБЗКВДИЕБВЯБВЯЯОЬВЕЩЬБЖЙУГК
ЭЯБЕЩЩЕЕЗКЭЬДДТМЫКШЯДГЯЕБЗКЭЯВЯДИЕШСЩЯВЯГОЙЕЬЫКЯЮЕЗЬДШКЗЪБЯМДОВУ
ДЯБКЕЫЯДЯЮДЯМЩОВИГЬДЖЗЕЩЕЫЯЙУИЬВЩЬЗУМЕГДШПБЯЗИБКХВЕПЫУЯЖЕЬМВИЕГД

ЕХЩИВЕШЕЫКИЩЬВУЯОЕДЬГЪЩЕЙЯЮКГВЬДЯБЕЬБЬЖЕЬМВЩИВЬЫЮДГЯГТЖЬЗЬШЗВЯИУ
ОЬЗЬЮЕЩЗЪЯЩСЬМВЯЩИВЕШЕЫКЩЕЩИЬМЯЮШМЪЕЗЬВЯЕЪДЯПКГЯБЗЯБЯЗЮЫЩВЯИУЩЬЮ
ЫЬДКВЯНЬЩИЙЗЬЙЯВГДЕЭЬИЙЩЕДЗЕЫКДЕДЯБЙЕЩЙЬГДЕЙЬГЬДДЬЮГЬЙЯВЯДЬКЮДВЩ
ЕГДЬЕЗЬДШКЗЪИБЕЪЕЕЛЯНЬЗЩЕЭЙТАЖЗЯЩЬЮГЬДЖЗГЕБЯЮШЬИЙЕЩПЬАДКЪВКЖЬЗЬБ
ЗЬИЙБЩЕЙЯЫЩЕЗЬНИБЮВЕДИВЬЮИВЕПЫЯИЬАОИЕЙЬШЬЫЕВЕЭКЕДЩЕПЬВЩЯЮШКИЩЬВУ
ЯОГЬДЫЕЪДВЩЮЪВДКВДДЬЪЕИЙЗЯББЗЬИЙЯВИОЯЙЖЗЕИЬШГЕВЯЙЩКЫЕЭЯЫВИЫЕВЪЕД
БЕДЬНЩЕЭЙТАЩЕЗЕЙЯВИЯИБЮВГДЬИЙКЖАДПШЙХПБЩЬВЬВЙЬШЩЖКИЙЯЙУИЕПЬВИВЕП
ЫЯЕЙЫВЬЬЫЬЗЭЙУИЩЬВУЯОКИГЩЕПЬВЩЯЮШКЯВЯЩЕЫЩЕЗЬНББДЮТЩВЬЬГКЭЯБЕДЕИЩ
ЬРЬДШТВЫЩКГИВУДТГЯИЩЬОГЯЯЙЫИДЕИБЫВЬЬЩЗКБЕЖЯИЯИВЬЫЕЩВЕЕЙЩЬОВОЙЕЯГ
ЬХВЯОДЕЫЕДЬЪЕЫЬВЕЯОЙЕЖЗЕПКЬЪЕЖЗЯДЙУГЬДДЬЫЯДЬЖКЪОЬЩЕШЗЙЯВИБИЩЕЯГЙ
ЕЩЗЯРГЯЩЬВЬВЯГЩТЫЙЯЩИЬЖЕИВКПВЯИУБЗЕГЬЫЩКМБЕЙЕЗТЬДЬЙЗЕДКВЯИУИГЬИЙ
ЯЙЫИДЕИБЫВЬЬЩЗКБЕЖЯИЯИВЬЫЕЩВЕДЬИГЕЙЗДОКЩИЙЩЯИБВХОЯЙЬВУДЕГЬДЩЕВДЕ
ЩЩПЯЬЕШРЬИЙЩЕЩБЕЙЕЗЕГЙБДЬОДДЕЕОКЙЯВИИЯВУДЕЗЮЩВЬБВЕГЕЬЩЕЕШЗЭЬДЯЬЯ
ДГЯДКЙКЖЕЮШТВЕЖЗЯОЯДЬЖЗЯЩЬЫПЬАГЬДЩЖЗЯИЙДЯРЬШКДЙЕЩРЯБЕЩЖКЪОЬЩГДЬИ
ГДЖЕГДЯВЕЙЕГИЩЕЯГЩЕЖЗЕИЕГЕЙБЕЪЕЯЮОЬГЙТБЕГДЬЖЕИВДЖЗЯЬМВИГЕЙИЬШЕЙЩ
ЬОВЖЗЯШЬЪХБЙЩЕЬГКИКЫКЭВКХИУДЕЫДЕЪЕЯЮЙЩЕЯМВХЫЬАЯЖЗЕПКЙЬШЮРЯЙЯЙУИЯ
ЗЕЙКБЕЙЕЗКХЕДЕШЯЭЬЙЪВЮКЖКЪОЬЩЮИЩЬЗБВЯЯЙЫИДЕИБЩЗКБЕЖЯИЯИВЬЫЕЩВЕЫЕ
ШЗЕИБЮВЖКЪОЬЩЫЬВЕЙЩЕЬЗЮШЬЗЬГЮЩЙ

(b) Расшифровать текст:

ЬЭТХЭХЛЯРЭЮЕЭТГЪЫГТЪЗУВФЮФБГШКСЛЦЪЖРТГПГФФБПЗЦШЮФИСЩЫШЯЦСЬТЕСТФЪ
КИШЫЪЖШПЫФЪЪЪЦЯАЫШЬЧЖОЪГЖЗЬПБМГЭЬБШЫЪЩЯОЪХЫПОЬСЧННАФХЩЬЭНМШВЭФЩБ
ШЫЪЧПЫЪСХНТПЫШФХЬСХЮЦЭЩЫФХЛНШЫШБПШБПЙЮЖПТЗЪВЦХЯШШЩЦЬЪХФШДШЧЦЛУЧШ
ЧХФНПХЧЖПШВЬИФФЮШНЪЬЦХЪЗЪУЬФЭЧУШГКТХШВУЬНБКЪЭЧЧЭЬПТПЕЪФХПЕИНЩЛУЧ
ТХШЙЮМЬПЕЗСДЪАЩЭВМЭЧЖЩБЗЪЫАПРФХУЕЪССГТДСЧЩСЗЬШЫХКЪНЯЬИЦЬЩЪЖЩМЩХЙ
ЭТШМЭЭЬЩПДГЬЯХЖДОЩНЖЮШУЕЙЩПВЩЖЦШЪЧЖХЫЯМЭЭЬЩИАЭЛЦСДЪХУЧУШЪВФЕФПЭМ
УСЯЬТЯЭТЭЛАЬЫЫЧЭЫЪЯЫКЭЖВЦЖФЦДБАЮПЬПДФЧЦОЛШЫЮТДЯРЦФЖПОЮТЩЯОНЭЪФОЦ
ЬФЭНЬМЪЪРГЕБЭЬЯЪЖЩХНЦЖЭЬЯЪЖЩЭЙФЙЮШБШЕЩПШЧВЪЦИЬЖЩПВЦГФЧГПЩУВЦХПЮШ
ЮПЬЪЛБЕБЧТХЦЭЩФЯЧФУМЦСЯОПШХДСЧХШЩЬШФШДЪХЯООЫЪМЬЖЭЬНЛЖРЪЯЫКИЦЯХЖР
ПЗФАБЦЦХАЩЭЙФВНАЫЫКЬТЮЧЗСЫЮОЖЬШЧЧУСЪШЦУДХЦЧАШШЩЛУЧТЮПЖГПЮЖЗЬТГЧУ
ЫЪЯТЫЬЕЙЦЖХЩЯЬЖПОЙЧАШАЦЧДНЕЬЧЭШХЯМЮСЧЮПДЪНЮПЗЬТШЧКИЫУОЛДПИЬЖЫШУП
ЬСЧЩПДЪПУЫАШЛЩЪЙЦШЭЬИЦЬЩЪЭНЕЬШЫЧЭАШАГЭУЫКОШУХЙСЛУТЕЪМГЕДЫПБПЬЭМЦ
ХФФБЦЦЪЭПОЬЖШПЮЦЛГТЬШЙЮЪЩФЛПЪПЦЖЭТХПГЩШТХЛГФЦШКОШБШКЭЖЯЬДСЧЩЦЖЧБ
ЬТЯЬПХФКЪХНФЖЫШЫЪВФМЮПЗЬПЭПЕЩШЖШКСХВЧАШЩЯЦАЬТГЖЙФЧЦСЕЧЫИПЫЪЧИЬФЩ
ФЯЧЭВЫЫСГСЦДЧЛЩЭВМЭЧЖЩБЗЪХЮШЗЪЦЩЪАШЫУТЕЪМГМАТЭВЦПЮШУТЕЪМГМПСЪЮЩИ
ЪФШТГЮПТЧЗЬЫЮШЖНТХПГЪЛЦГЦЭЖУЩЭЬПХМЭЭЬЩЫЭНЭЭЧЭСТВХЛДЬНЫКСЛЮЭЕСЫЦЪ
ЬФЫНЩЖШТБТДЭЗЖЛККВЫЩЭЮЪЮОИСТИШКОПИХЖЩЫФХЛНШЫТДОСХШНЪЦВПИТЭВЖКЪЧВ
ЦЖПШВПЩЭЦЫЪЛПШЭМАЩШУЬВЦЦЮПЩЗХЯШЙЮМЬЬФЮПТШЬЩШФШЪЮЪЫЬАЬПИЬЖРПЬЬФПЪ
ЦЯЗЪЩДЬГОСХЭДЧСТЪЭЭЬЩФЬИБЩЯЭЫШУТЬЮЖВЫВ

2. Разложить на множители числа:

(a) 92607014484185114230259856508 9

(b) 9727333088820907066799452065425464223447520656676828423411 53

(c) 10119284026823165928501277132496076524878486973397896834517468902487959543527589851687738 93

(d) 13563780361918641799019155894776887628549102394277873160127365452375355199742053398885961899769931958466431596118547457 77

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 100545755457749049086323771253610547460959515143049944187998611536323739313523$
- $e = 5$

Сообщение:

- $M = 237248126305266225869488544116943089112232578697103114749905900149794139528 07$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 18618093863709258884253667711882409477 3$

- $q = 194291375291381136066641806096071453907$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 248396817278357433555645744754827792947933329626954238593964650031360265496 20$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 139942232502981016833152857433482597831$
- $e = 3$

Зашифрованное сообщение:

- $c = 948925306170114249314405635908322086 25$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 307690544790292480301333955452547461233$
- $g = 302159718830482062440727979094072220911$
- $y = 167508945424133309573975567705863906364$

Секретный ключ:

- $x = 177370868234615358136263209956889618141$

Сообщение:

- $M = 258797756472866257956093425006424071934$

Использовать следующий случайный параметр для создания подписи:

- $k = 187928168498458341831319178481425215105$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 223044112470214656210791530170106126331$
- $g = 151429945161395855895033390141099544391$
- $y = 678492023287208903521501859799959971 76$

Сообщение:

- $M = 212071077597090349377942850432502988554$

Подпись:

- $a = 135229903022420340864423776143272891598$
- $b = 101506507875675521773537872501489358900$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 821$
- $g = 795$
- $y = 193$

Сообщение:

- $M = 350$

Использовать следующий случайный параметр для создания подписи:

- $k = 609$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 12x - 13$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 40

1. (a) Расшифровать текст:

ЮЕНЛБЕПВИВЖЯШМРОПЕПВЙВКХЯЮНЕКЙВКМЛОИРХВПКЕДФПЛДЗНЕФИООВНБУВЙДКВП
ВИЕЯШФПЛЯОЛГЕБВПЮВОФВОПЕКВМВНВГЕЯРЛПЯВФИЛКОМЛЗЛЖКЛКЛЙЛГВПЮШПЩОМО
РЙЛВАЛЕДЮЯЕПВИЕОВЙЩЫЗЛПЛНПЗЯВИЕЗЛБРХКЛМНЕДНВИЙЛВЮВБКЛВОЕНЛПОПЯЛМ
НЛЦЖПВКБНВЖМВПНЛЯЕФМНЛЦЖПВЯБЛПЩЯОЕИЩВЯКЯШЮШИЕБИЙВКЮЛИВВФВЙЮИАЛБВ
ПВИЕЮИАЛОИЛЯЕПВЙВКМНЛОПЕПВГВЕЯШМВПНКБНВЕФЮРБЩПВРЯВНВКШФПЛФПЛПРПЛ
КДМИЗИЕДЗНШИИЕУЛНРЗЙЕЮШИЗЗОРЙОХВБХЕЖЙПРХЗМИЗИМЛИКЛЯНПЩЙНЩЕЯКЛЯКО
ЗДИЙЛЖЛПВУЗПЛПВЮМРОПЕПЛБКРЗНДЮЛЖКЕЗЙОЕБЕДБВОЩЕЙЛИФЕРЙЕНПЩПЗРЙЕНП
ЩРГЯЙВОПВОИРХЖФПЛПЙВЦВАЛЯЛНПОБВПВОЩИЕЗНЕФИХЯЮНЕКЯЕБЕПВФВНВДМПЩЙЕ
КРПЯОЕДГНПКВОББЕЙОДИЛБВЖЛПЯВФИВЙРЮПЫХЗПЯВНБШЙАЛИЛОЛЙИЕУЛВАЛМЛЗНШ
ПЛВЙЛНЦЕКЙЕЛГЕЯИВКЛЮШИЛРБЕЯЕПВИЩКЛЫЮЛБНЛОПЕЫАИДАНЛДКЛОЯВНЗИЕЕДМЛ
БОВБШТЮНЛЯВЖЕЛЮНПОЩЗЛЙКВОЗДИПВМВНЩМЛНЛКЛПМВНБЯВНЕЛАЛКЩЯЛНЯИОЕЯДЯ
ЕИОМЛЮНВЯКЙДЗЛКЛМФВКККШЙОРТЕЙЙЛТЛЙЮПЫХЗЯШОПНВИЕИЕДМЕОПЛИВПЕХАКРИД
МШИЫЦЕЖМЛНЛАДЗНЕФЯЯОВДЙКЛЫОТЯПЕИДНРЗЕЙПРХЗРЕЙНЩЫЕЯКЛЯКРЕЮШОПНЛЯШ
ЯВИЕТКЯЛДБРТРМЛНЛАИВГИХЯЮНЕКМНЛОПНВИВККШЖБНТИЛЫНРЗЛЫЛПУЙЛВАЛПЛИМ
НДЮЛЖКЕЗЛЯЮВГЯХЛПКВЛГЕБККЛЖКХВЖЯШИДЗЕПЛПФОЛЮЛБНЕИОЩЕКФИКОЛЗНРГПЩ
РОМВИККВОПЕВЦВКВОЗЛИЩЗЛРБНЛЯКЛЗЕНМЕФРБФКЛЮНЛХВККШЖРАЛБЕИЙКВМНЙЛЯ
АНРБЩРМИЕКЙЕКРПРИЕХЕИОФРЯОПЯМНЕХВБЯОВЮРЯЕБВИХЯЮНЕКОЕБВЯХВАЛКЛЗНЛ
ЯЯИВККЛЖПНЯВЕМВНВБКЕЙЯОВКХВОВЙВЖОПЯЛЙВКМЛББВНГЕЯИЕМЛБНРЗЕПЛИМЗНВ
ОПЩКЗДЗЛЯЕЮХЗЕНУВЯЛЗНРГИКОХЯЮНЕКЮШИРГОКЛЮИВБВКЛБКЛЖНРЗЛЖМНЕГЕЙИЛ
КНКВКШЖЮЛЗИЕУЛВАЛЕДЛЮНГИЛЙРФВКЕВЕДИЛЮРЛКЙВБИВККЛМЛБКИАЛИЛЯРЯДАИК
РИКЙВКЕМНЛЕДКВООИЮШЙЕКВЯКПКШЙАЛИЛОЛЙЯВХПЩВАЛЕЯОВТЗНЛЙВВВПЛПФОПЛИ
МДИЛБВВЯЛЗНРГЕИКОЕОЗНЕЗЛ

(b) Расшифровать текст:

ЖОФРБУЛХЮЧЖХДЖЮЕНЯЖХЦВЬЮТЙЗЮЗЧЕРХХТЬЕЖОШПЛВФХНЛЮСЮЬВЬДБЖЛПУВТНЯП
ГТПАТТМИВЖЫЙВЮЗЮЕНКДЭМЙЮКЭИЛВЖГХЯЦНММФЩУЪТНЯСЮЛЮМНЮЖФЦТИСВЪДМВАЦ
РБЖЛЦОТТГГРЬМЛШЛЗАВЭФГПРАЗЯФЕЦЧТЖЛБЗЭЕРБЕЯФЙЯДШПОЫЕХСВБНГЧЯЩЖХПЙ
ДИЗМКДТЮХПДДЛХЛЫРУТКЯХЦЙОФРАЕИЦПЭТАЯУВФЛВФШВБЬКЭСШЦДЮПЛВЭХЗЛТЭЫМ
ОЯДБЙЙТЗЫЯОГТЛНМЯНШСИМЛЬЧКХКАСМЯОШСИУРШСЯБЗЬЙКЮПЛМЛЮПЮЖКМДХЗЛБЗЗ
МОЩНМСЛЯФЧЯЯЬУЭЙЙЦШЪМЖУЭУТЯЯТЯТБЬЗЬЧМЩУМРЛЯФСЦЫЙМШУНЩКЬЙКЩЗУТЛЮД
ЧЗИЮХЫСЙЦПСЯОГТЮУЛЧЗЬТЖВМЧПЛЮФТСЛЬКЪКВГУЭИНЦЛЯЙПБРТМФТЭЫЙХЦФТТЕЖ
НХЦПЦСХФЩУРВЧХЫМЮНРЮЗУТЙЯНЮЦВЗЧДФВЭЦАЙЙЯПАХМЦЩВПМЩУМРЛЩУВПФЩФВАВ
ФРТУЛЬЕЮПЛВЖХПОУРШЛЙЦЩЭМЙЩНЮХПЩДЛНАЯУГИННПФФВЪМАПЛУКЗСБЦАБАФГРТЬ
ВАТХЖЛВЧЮИЕГЗЫАОГДЮБПЯЩВТДВЗАЙЙЯПШМСДЛЪОВЭХЭЙОЯЦХХПЮРЪТКЦЩЭТБЩУЖ
ММЬКЭУВБДЮИВЬРЭТПЫНШУЕЙХВООГТЮРРЫОАИЯЙЗЯФВУРБЩЛХКВЙИНУВЖЛЮЗЧЕШЬР
УРЕЫРУИМЯМЮНКМОДЙИНЖЬФХЬРЬРЕЮСЮЩЛХЗВОГЦКЪФЛЬКЭОРОЧХЕНДЖХФПЫРЭЙХЦ
СЮРКЩФБЦНМПИММБРЪЛПЦСХФЩЯЖХПВЫДЬРЛЦЕЮУЛУЗБЧАЭЖХФГГЮТЙГЯДЛЩНДМТМУ
ЖЩВТПЫРХЙХЦДЛФРЫДШЪЪГРФТИЧПЮЕШГЮАЧОВМЯТАЯДЮФЗИФЮЦЗЯЗФЙНЙФМЖВЙЗТЯ
ТБХЪЖЕЗЧЯТЯГРАМИЯПЮЕНКУМОЛЭПХБПЯЙЭЫЕГРВЖВИНХРРВДШИЛЭМЪРЛЧПЮЕЛЬЗХ
СВУКЭСШЭРСЩЛХКВАОЬУЪТЯЯПХХИЩЪЪТЙВФАТАЯЖТЦЩАРСТИНЪХЖЛЬКФЙНЧФМЖВЧЗ
ТЯТБХЪЖЕЗЧУРМЯПШРЫЩПХИЯГЮХРРУРЫМКЦФТМБЮРХЬВУЭАЧЗУКЖЯДЮЩШЦКЦФЮУНЩ
УХРВФРЯХМЯТВЗБЦИЮСЯЯФЮЦМЩУВАЯВЗЬЙКЯДБОЕЪЧЮФЛЙРЕТНЯЪЮЖОЦГГИВГУФЙИ
ЮРЯТДУРЫМХНГХЛФЩПЮЖЛТПВАОЦГШХПБЭЬЦЛУТШЭВЭКФФРФРЬСЗЯПХЪБЯЕФПОЩСАТ
ФЩСАТФЮХСЦЫЙМБОДЬРЭУНЯЩШЦЯАКБАЙЯКЮЦИЯИШЖЯВФЮФЛЮХЬТЖАУЯТНГДБЙЮДЖХ
ЦОХЗЫСЛГЭСЧБЦЪМТСЩШХФЛЭСХФВУЗФЙКУСЮПЗЩЩВТЮГЗСЙЯБЗЬЙКЩПХЦВБФМЦЛШД
ВФГЦСЮЙДЧЛТЕВЬРУТ

2. Разложить на множители числа:

(a) 6185381729746265751139666430677

(b) 679814447923933272392236348869959465498066567623425844336471

(c) 19744385188373736402922046611028607640008133918621464167647270082609532678017024542773756 29

(d) 92761988152568222422954671038508103729768182725105617828829870411804236879294527566749804226463821599267635114877979158 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 898788399733606011759067832623652987179009528900854143895639094293070975930 91$
   - $e = 5$

   Сообщение:
   - $M = 73476630075656860593192601819246826457170181443057996394464223183995336992750$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 23622270645536192104037090437661836695 7$
   - $q = 25419627613091422262880591174986873000 9$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 95908086226109588969777620763938806452767126848191637693119278700248167435 12$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 28867020200419335685553491240929028634 9$
   - $e = 17$

   Зашифрованное сообщение:
   - $c = 41553956959906573083884672224425708303$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 19209116746751585257783220390490261106 1$
   - $g = 17636917149591780791405055301099594014 6$
   - $y = 62807696467778060603038121280563169208$

   Секретный ключ:
   - $x = 18769714179969947612007433683136217524 2$

   Сообщение:
   - $M = 17937123257942555280525381774668076681 7$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 12909024226083124232520791478688968227 9$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 23808060646584781706674594352792997240 1$
   - $g = 32687394967672076629066261324586730910$
   - $y = 11565188106146678126584437253122883948 2$

   Сообщение:
   - $M = 20599658971705027381415230968140871471 2$

   Подпись:
   - $a = 55798199353620168236309247319277093332$
   - $b = 21651237716692898197772657831153585925 6$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 521$
   - $g = 202$
   - $y = 319$

   Сообщение:

- $M = 235$

Использовать следующий случайный параметр для создания подписи:

- $k = 23$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 17$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 41

1. (a) Расшифровать текст:

ЩЕЯСХИБЙПТЮЩХФУМЧМФЦПШЩГШХУФХЕСИЪЛЪАМУЪУХМУЪФЮТГФПСЪПЦХЩЧМИХЙТЦМ
ЧПИЪУКПФМОИЪЛГФЛЧМРЦМЩЧХЙПЮШСОТУЩЪЯСЦХСТХФПЩГШПХЩУМФСФОЕИЛМШСЩГФ
ЛМЕШГЮЩХХФФМХШЩЙПЩЦМЩЧЪЯЪШЙХПУПУПТХШЩУПЮЩХОЙОЛХЧХЩЙМЮТИЩЕЯСФЬУЪЧ
ШГСССХРШЩЩПШЩФЪЦПШЩГССФОЕИЛЙМЛГЩВШСОТЮЩХПОЙХТПЯГЦПШЩГСФЮТГФПСЪЦМ
ЩЧЪЯПФЪЩУЮЩХЛЙМЛГФЮТГФПСЦМЩЧЪЯПФСФОГИЙМЛГЦМЩЧЪЯОЦПШФЙШМУМФХЙШСПР
ЦХТСОЦПШФУФМССХМЛМТХЮЩХХФОЦПШФЦМЩЧЪЯЙЦМЩМЧИЪЧКФМЦХМЛМЩЮМУЪФЪЮПЩШ
ХФШТЪНЙЦМЩМЧИЪЧКМУХЩШГЛЦХЙМШФПЮЩГФМЩЦЪШСРЦХШТЪНПЩХФЙЧУППЛЦХЩФМЩТ
УСЪЛЦХФЕЬМЩЦХЧХЬЪЛИЪЛМЩШХТЛЩФМЯУЩХФОЦПШФЙКЙЧЛППКЛММКХЦЯЦХЧЩЦХЛРМ
КХШЕЛУЩЪЯСХЩВШСТУХРЦШЦХЧЩЬЧФПЙЯПРШЙММЯСЩЪТСМЙУМШЩМШШХЧХЮСХЕЙСХЩХ
ЧХРУМФСЧМШЩПТППЙЧЪЮПТМКХИЩЕЯСМЛЧХНАМЕЧЪСХЕИЩЕЯСЦЧХЮМТМКХШХЙФПУФП
МУЦХТХНПТЦМЧМЛШХИХЕФШЩХТПФЮТШЙХМЦПШГУХТЕИХЦВЩШЩЙХУМФУЪЮПТХСЪЛНХЩ
ЦЧЙТЕЩУМФМШТПЪНФМЙЦМЩМЧИЪЧКФМШЙХЛПТКТОШЦМЧИЩЕЯСПФСХЩХЧХМЛЙПКТХШГ
ЛХЙХТГФХУМЛТМФФХФСХФМЭХФСХФЮПТОЦМЮЩТЦПШГУХЙХЛФХУЦСМЩМШЦШЦХЧЩХУШФ
ТХЮСППЦХЛХОЙЙУМФШСОТЙХЩЩМИМЦПШГУХСФЛЧМЕСЧТХЙПЮЪУХМУЪШЩЧПФФХУЪЩХЙ
ЧПАЪПЛЧЪКЪЩВМЛМЯГЙХЧМФИЪЧКШТЪНПЩГЦХЛМКХФЮТГШЩЙХУПЩСЙШМУХПИТМШЩАП
МФЛМНЛВЧЪЯПТПШГЙУМШЩХЙМШМТХРЦМЩМЧИЪЧКШСХРНПОФПХНПЛТУМФШСЪСЙШЩХЧХ
ФМКТЪЬХРПХЩЛТМФФХРШТЪНИХСХЩХЧХРОУПФЪЩЪЛЪУТШЩСПУЙХШЩХЧКХУЦХСОТШГУ
ФМЩНСПУФМШЮШЩПМУФХШЦХЧПЩГИВТХФМЮМКХФЛЧЬКХРЛМФГЦХЪЩЧЪЦХЛЙМОМФИВТС
СЧВТГЭЪЛХЧХНФСПИПЩСЪТХНПТПЙФММЮУХЛФЦХКЧМИМЭШЮРФВУЦЧПИХЧХУПЪОТВШИ
ЪТСУППЦПЧХКУПЦХШТМЛФПУПОФСУПЛХУЯФМКХИТХЙШЩЙЧХЛПЩМТПУХПИТКХШТХЙПТ
ПУМФИЩЕЯСШСОТУФМЦЧХАРЦМЩЧШТЪНПЙМЧФХСХУЪЦЧПШКФМЯГШТЪЯРШФЮТГФПСХЙО
ПЬТШСХРФМКХФРШФШТЪНИЪФМФЦЧЯПЙРШХЩШТЪНИВФМХЩКХЙ

   (b) Расшифровать текст:

ЖЫТЭЙЩАКБЖГЪТДЕСЖФЮДЙОЦККМЪПНЗАВТНХПЬЗКЪГИУБРЛЕХОБЬЩХДДЖИЙЯЗОЕЖЙ
БЛЫЙЗКЙККЭФПГТОЙГВОЖЖПЩТДОМЮННГЖЬМПИОЩПЗГОЬУККРЯВОГРЕЫЙЗИБМНЫМЯР
АЗКБТИЕОУМЮЖМЩСНГМЗТЛЮОЬХОДПЕРЙЗЬЫМУБРУХИФНЕЛЙГМГМЗБПУЖЙЮЗДЬБДЯВ
ЗКЙЕКРЙМЬЯЫПЫПЙЖДЛГВАЙМЬЫЙЮМЦБЧЙЮЕГЙОЖЩГТЭЙЕЕРЛЙЖЩЛЗКИЫТЭЙМГЧНЮК
ЬННЛАКИВЮИЯЖЙМЖЪСОХЖОЧЖЙЖЩТИМБЗСДАМДСКЕСЖТММХЯОПЗИЕЦКЙМГЬЮЪОЯСЮФ
ВКРЗЪСЫЦКЪЩЕСЭФЙЩСБИМЮЖКДЖЙЙЗХЛЕННЫЕЯХЮКЖВМНЗЗЬЗКЙМЩСКВХЙТЙЮЖГЙЗ
ЗЖЙЙЙБНЗЖАЗНЕИКЪЖДТФЫЯЗМЙЗРЕРЙЮЯЬХЛЗИЕМЗКЯТПЛЙМЯЛЮЮВЬСЮЗТЯЪБЙЩИП
ПЯЯГЙЙЖГЕЦЯЗЧВЖЭЗБЕХЛКГГТЕГОЬУККРЯСБЪЩВТЙБПГТОЙМЩСДМХЬСДВЛЯОММЙЕ
ЖЖЗКЬСАЖРЖТНЗЯИЦЮЮЛДТЕЗУЕЦБМХЯПДЖМЪИНЫМЯЩНЗЙЫЦЙЗГРЙЙЮКЕЗАЗЯЯЦШКХ
ЙТЭФАИЙКЖЖЮСЗБИЕЦКЙПЙТМЗЛЖФЮГМЙТМДГЩЩКЛКДТЯБГЯЛЙБУЫЕЧЫРЕРЙЮМПМЭБ
РУХЛЮОЬИЖЯВТРКЪМЗТОЗКБПЗБЛИЙЭАЛГЙЙБГБФБКРКЬЮЪОЯСЭФЙЕСБКИЕПШГМЛФЙ
ПСЮХЖБУБСДЬПЙПУБРЙАДЫМГСБИОЕЕПЭЖВХШЗУЕЦЖДЖЙЙМЛСЗЙЛЗСЙФИРЖЙППИОЭС
ЗКАЖЙМЮАЕИСБЛЕЗАБАИТУБЛЬСДБПЙМСЗАЕЕБЭЙЖТУЛЖЩХБЬВКОКЕГДИЙЛБЫЙКЪЩБ
СКЫГДСКИОЕЖКЭЖВТНЛРЕОАЖЖБЧАЫГОЙМГМГМЙЗБЫЖЗДПЕЦБПБЬФНБКИКБЖМХОПДЖ
ДТЕИКЛМЗЗАДТЕИГЗЖКЧАЬХОЗАРМТЮЬЩТЮКГГТЖЗЙЕИЖЮПЯЬЮЪОЯСЧЕОЮЧИЮГЙХЮБ
ВЬПНГДЫЯЕЭГДАЙЗХИТОРПКЕБКГЫЙЯЗПЙСКЫЖВХШЭЙГЙЙЕГДЙБИОЯЦЙЗЬЩХБЬВПСД
ЮЦКЦЖБГЪТЙКХЬЦНЮКУМЖЗКЬСАЖРГСБЗХЬСШЖГДФЮБЙЯХШЗПЕЕБЖЛЕОКДИЯЙГЕГОС
ДЗКЗАББАДТЮЖГЫФПЬМЪТКЪЧЬХОЫАБФБИМИЦДЖГШЯЗЗЛЕИММБЕЗКБЛЬКБДЙДЙНЕМЙ
ФЙИОЬИНГЕДМЭСИЯФТФЛЬЖКАКЖЭЗБПУХЛЗИЕННЛАЯЙТЙПЙЖКЫЙЕЖКГОКЗЙСГАОМЮН
ЕХОБЛЕРДЙЯТПЛЙГЗЖЙЖГЮУЙФКГЙВЭСКХКЪЖЬРПЯГИОГФАВЫОЗЕДМИДПВМОЮОЙЧМЗ
ЬЕУЧЛЩГТДЭЙЙТЯЭЦДЙЯЗАЗЙИЮЛЯЕЧДЖЯЛМЭЛТМЗЮИИСАЙНЬЦМЗАЯЫНМКЗТЖЗАДЙН
ГМВАЖЗЙЬЦЛЗПВЙКРГДАДОНЕЩЮДЙЕИЙЯВТЧАДМИАИЖГДУДКРУУБКГДОПГМЙТМЗЗШЯ
ЗЭМЩТЗЮЛЯЛЮЮПЙСКРРЕХКРЖДМОЮЙЯМЙЗБЫУКЭАЯИКЕРЗЙЭЗА

2. Разложить на множители числа:

   (a) 441768441900809982741855205753

   (b) 1299828466613119789218972447055692481182269194074061339639633

   (c) 661585301352131590941159272956846201133994605521584906368934851768015782753564786197182861

   (d) 1413047313015780519854681234972947854549301716533322435857834084066898126255254922900039087644938153177968066450689423789

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 80169409941626342862354558785115769996589202527899194944355617472503846110793$
   - $e = 5$

   Сообщение:

   - $M = 75770509416430651680389763831555648404465321035529109035434775961275592583962$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 3028257383957730346110274071591351902 57$
   - $q = 18779434950707259801827784407399962876 1$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 14189054139158459434889398120894559240453832948401806048018224978241293285890$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 21156138175099542763580144818904370795 7$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 19858128735063810516819881597954561864 0$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 22412110868087771135866443143740947 5741$
   - $g = 17705276606788710249872172155271747 8615$
   - $y = 20219618371025540384055673992141886 2513$

   Секретный ключ:

   - $x = 26176443677019738663805837805003234268$

   Сообщение:

   - $M = 17595818451081703646379398034985584 2807$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 19754833624664026804929905765027826 1559$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 28260997266099021147140398571476230 4421$
   - $g = 11187129650879900300873425585663014 2255$
   - $y = 99223899600612896446343168916618355748$

   Сообщение:

   - $M = 78174642838960671509654263865811974 24$

   Подпись:

   - $a = 16906571120182263867216832494281884 9690$
   - $b = 76762923976810870611153661280327477434$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 577$
- $g = 387$
- $y = 339$

Сообщение:

- $M = 397$

Использовать следующий случайный параметр для создания подписи:

- $k = 97$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 9$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 42

1. (a) Расшифровать текст:

ЮИФШЗГЦШХЕЮЬГВЭХБТЮЩЯЮУЮЭЩЭХБВЮЩЬЙШЪЬЧЫБЬЭХЯАТТБЬЮЬФХЫХБЪЧЫЯЮЗХЬ
ГФГЬХИМВЛЗВЮЦШЫЮЭХФЫХЗХЯЮВЮЬГЗВЮТХВХАЮВВЮЫХЯЮВЭГЫЮВТХЗЫФЮАЮЦЭЛЩШ
БЫЛИГФЛЬЮЬЯЕЭГЫЮЧЭВМФХАХТЭСЫШЧЪЮБЬХВЫШТЮБВМХУЮШВЮЭЪЮБВМЗГВМЬХЭШЧ
ГЬШЫШТХЫХЫЬЙШЪГХЕВМЫЮИФШВЦХЫЮБВГЯЫШЯЮУЫГСЮЪЮЬГБЭХУГЪШСШВЪВШЕЮЯЮФ
ТШУЫБМВЮТКХЧЦЭБГУАЮСВЮЮСАГИБМТЮТАУШЯХАХТЫШТБМВЮЭЮФЭГВЮЭФАГУГОБВЮ
АЮЭГНВЮЯЮЕЮЦХСЛЫЮЭЯЫТЭШХБГФЭЯЮСГАЭЮЬГЬЮАОБТХЫМШЗЮЕЫЯЮЬШЭГВЭЮВЮЫЪ
БМЮЬЮШСЮЪЮЯГБВШЫЖЛЭЮТЪГЧЪГВЫБТИГСГШЧФАХЬЫГСОЪЭЭЛЩЯХЭШХЬСГАШШЪЗЪЮ
ОВШЕЮЩХЧФЛЬЭХЯАШБЭШЫББЮЭЪЮВЮАЮУЮЭШЪЮУФЭХЬЮУЯЮЧСЛВМШТЪЮВЮАЮЬФЮБШЕ
ЯЮАТШЦГЭХЗВЮЯАЮАЮЗХБЪЮХЪЮУФБЮЮСАЦОБЭШЬБВАЭЭЛХЮСБВЮВХЫМБВТЬЮХЩЦШЧ
ЭШЗШВВХЫМШЧТШЭШВЬХЭШСЮТХАЮВЭЮЧЭХВЯЮЮЯЛВГЪЪБАЮФЭЮЗХЫЮТХЪГЯАХФТВМБ
БГХТХАШОЭХБЬЮВАЭТБХТЮЧЬЮЦЭЮХЯАХЧАХЭШХЪЯАХФАББГФЪЬЭЕЮФШЫБТВЮЬБЮБВ
ЮЭШШЗГТБВТШФГИШЪЮУФБГЙХБВТХЭЭЮБВМГБВГЯЬХЗВЭШЬБЫШТХВББЭШЬШТЭХБЭЛЕ
ТШФХЭШЕЯХАТЮБЮЭШЬЭХЪЧЫЮБМСГАЭХЙХБТШАХЯБВТЮТЫШЬЛХЙХСЫГЦФЫШЯЮБЭХЦЭ
ЮЩЯГБВЛЭХТФАГУГТШФХЫТЮАЮВЛШТКХЕЫЭСАБЪЮЩФТЮАЭИХЩГБФМСЛЯХАТЮОЬЛБЫШ
ОЬЮХОСЛЫЮЮЯБХЭШХЗВЮСЛСВОИЪЭХЯАЮУЭХТЫБЭЬХЭЧЭХТЮЫМЭЮХТЮЧТАЙХЭШХЯЮФ
ЪАЮТЫОАЮФШВХЫМБЪГОШЭХЯЮЗХЫСЛХУЮГЬЛИЫХЭЭЛЬЮБЫГИЭШХЬБСХБЯЮЬЮЩБВТЮЬ
ТЛЯАЛУЭГЫШЧЪШСШВЪШШТШЦГЬВГИЪТБВАХЗХВЬХЭЭЪАЛЫМЖХБТШФЮЬУЫГСЮЪЮУЮЮУ
ЮАЗХЭШВШИХУЮТЮАШВЮЭЬЭХЮВХЖСЮЫХЭЯАШБЬХАВШШЦХЫХВБВЮСЮОЯАЮБВШВМБЯЮА
ЦХЭЭЛЩБВАЕЮЬШФГЧЭХОТБЯЫМЭОТШЦГЪЮЬЭВБЫСЮЮБТХЙХЭГЯЮБВХЫШБВЮВЫОФШБЯ
ХЗЫМЭЛЬШЫШЖЬШВШЕЮЭМЪЮЯЮФЕЮЦГЪЯЮБВХЫХЬВГИЪЯАШЯЮФЛЬХВЯЮЫЮУШУЮТЮАШВ
ЭФАХЩЯХВАЮТШЗЯХВАГИЯАШХЕЫЮЭТЮАЮВШЫБГЧЭТЮВТЮХЩСЮЫХЧЭШСЫУЮБЫЮТШХУЮ
ББВЫЭЪЮЫХЭШШГБВАХЬШЫУЫЧЬЮШЭСЮЫМЭЮУЮЗВЮЦТЬХБВЮЮВЖЬЮХУЮТШЦГТЯЮБВХЫХ
ЫХЦШВЬГЦШЪБЗХАЭЮЩСЮАЮФЮОТХБХЫ

(b) Расшифровать текст:

ПФХЗБЦЦХЪЬХЧНРЗПЩХФОУМЭОЫЧЩТЫИШГШГЕШАУРЖХЩСЪДХЙПЪЖХВЧОВТАКЬИЙШРД
ЙКДНЦЗМЭШОХЯЦРУСМЭУЮДТХАОМГВПУЕУЮКДЬИБНЩБФЭНЩЯШЭУЮКЩВУХЮМЭПЬЯСЦЧ
ШЗПЫЧЪЗУЮКЫИУЦЭСМУМУЮЙЧУНЧВШНСЪЕЮВФЯЛЩВБЫИСБШЮИРГХЪЙПЮПФЖВЯЦЮЗХУ
НЧВШНШЭЖХЪХСДПЩУНЗНЩРФТЦФНДЬИБНЩЫВЬНЭДЪВТСЯУЦТЩИШЩРИЗМЦНЭЖМЬКСВИ
ЯФЬЯИМЗДВРЮКЦИКХЦЪЕЛГУШЮТЭТСЗМВПЪЕГЫУЯКХЫУОЬЫЦЬЮИЙЮНФДХГУЬХУЩНОИ
ШАУЧЦОЯЗЧЛЯУЖЬВФЮКЪАПХРЩГЩЩЗЪЖФЦЦЮИТНУЫЛФЯИЪЙЧЯЧФЬФЩПРИТФУШХФЦСЪ
ЭТЩЦРЯТГБРКЪФЙЬНКДТФДСЯИЪЬЧЦЙЩДХЮКВЙЧЩССМЮГУДЬИБНЩИШЬЖСЬМГЦЮЕШЧН
ОИШГНКЗФЦИЪЗШГШЫМГЩМПЗТЦИЪЙХИЧФЬШЭШККМЫШОЮЧДИЯЛТМЭЧЛЙЯКФЖКБУШДХА
ХЪВОЮКЭЯФЮУСИКЬТЯЕШЩШОВЛЦРЭЬМЬБФСШТКПШАЦИЪДХЭТСЙХЮИЪКФЯОЮКХАНЩДМ
УВЮИШЭУСЬЧЦСШЯФВНЧЦФЯПЪЕГЮШЧИЙФХЯЮГАУЩВНЦФЬЬХФУЫЕМИШЫЕПЬНДВТВЬЯЬ
ШГЗПЕЙЬГНИЙНЪЮХЛЦЗЦЮМУПЦКШЮТСПХХНРЯЙЫСЪЕХХМШННГАЭЙЧЯЦФЮМУПЪМЭЭЧС
КПЯЧВЖЩЦХФКХХШЫЕМЭКЩВФЫУЫВЛЦЗЦНУБМЯЖЪЭХУНУАХФЮФЯЗЫЯШЮТЬИЛЮЖЯЮМЬШ

ГТМЭКЩЗРХКДЦЦЯМННЛЦЭИЯШЬНБННЦССЗФЪЙСТГУЦЫИУЮКДЦЩЯЛСИЮЮШОТПВБЩЯШЫ
УЧЦСЯЗЬЯУЦТФЗМЭУПИЦЯСЩВЩНЦФЗМАУЩВУЬЬЮИШЯСЩИЕВЙСЕТЯЦИЕМЧРЩДЧЯЗЮЯЙ
ЮКУЗСЯСЪГКЯХЩВЭЦНГНЙВЧОИЙЬЖЪЕГЙШКЛТТУЭМГАКЬЯЛЯСЩИЕВЧЪЕШУКЧЦПИЦЪЛ
ЙЦЬЦИЕУХЯДЬЫЧЪМХТКЬЯНЮУЬБЙЩЗЧЙМБКОБПЫУЮИЧМСФЭЧДЙИВЦЬКГИИМРФНУЦТЭ
МФДЧЗЖТЯФЪЖТЭАЭЕПЭУФЙЧЯЦЩВТЩЦИЬШАУШЗПЬЦОИРАУСЮПЮУЦВЛЯИРЕШИЧЪЫВЬХ
ЩЯФУВЮНУЩТЯМЪВПЬХЦЮШЧЮЙЦХИСЩЯПЦИЙАХЪВОЮКЭЙХЙКЫМЪФУЧИ

2. Разложить на множители числа:

   (a) 4785115135866163486179319819 01

   (b) 4873097877335469241691612133218980108788741665437730723840 77

   (c) 8233756866740196050245334251866929339559421133294511496392298410321921173531260243748500 49

   (d) 8063095995498138529550710034229974664849986675809547821527977263221029975613948556577857714715004295224096283793228954 89

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 727301985768803897237586554205776643283920713303764694048096772396315858251 29$
   - $e = 17$

   Сообщение:

   - $M = 484085797675728047043703946238920250784955750399250910787868180805329968754 59$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 335359560806361755171912305792312716829$
   - $q = 247083979046561760102666376522149988129$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 283902093798324995285972132850845917740122764774783105663993181471284719369 99$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 241441596910166945748693909070238597893$
   - $e = 3$

   Зашифрованное сообщение:

   - $c = 199794938025099367019539932776370159889$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 276377398762707066497310481969125524947$
   - $g = 677472609857117577379926262443164608 09$
   - $y = 102492356756100832868125966020349177728$

   Секретный ключ:

   - $x = 570539806899272994188925865333423361 06$

   Сообщение:

   - $M = 235935002772460960067663087190746777413$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 211384167369814740167920889992745653217$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 282199756453053894712218893874484492919$
   - $g = 488799278433140342166006807056392597 17$

- $y = 25102079347080739533129945716804543804 1$

Сообщение:

- $M = 175939161880945970884962648172842063413$

Подпись:

- $a = 213482799303015743190105297955817963586$
- $b = 164910976683704266221469310740539669181$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 877$
- $g = 184$
- $y = 257$

Сообщение:

- $M = 63$

Использовать следующий случайный параметр для создания подписи:

- $k = 817$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 11x - 4$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 43

1. (a) Расшифровать текст:

НЗЕРНАГРСЭФУФДХУОЗАУСТРУКФЮСТРЖРНИНРПЙЩЗОКЙДРНКНКДЭСЗТЗЛФККЙЕДТЖ
ККДЕТПКЙРПРФДЗЩНЩФРФМРДГЭНДРНПЩНЮУФДЩФЗНЮПРЙПЗСТКНКЩПЭЗЕДТЖККРЦК
ШЗТХСРУФХСМКСТРЖРНИНПЗХФРОКОЭЛДРСТРЪФЗНЮСРНПРДТФЮСХУФМКУМЙНЗОХМС
КФПЪФЭДКЖКЪЮОРНРЖРЛЩЗНРДЗМУЖРТРЕКХУФНЗОХПЗЖРФЗГЖЗТИКМТХМКСТОЗЗФЭ
ОРЛГФАЪМСТРЖРНИНРПРГТЫУЮМРОПЗПЗСЗЩНЮУЩФРФЗГХСЗМНКДПЪЗЙЧРНХУФЮЗПЗ
ФЭСЗТДЭЛПЗФЭСРУНЗЖПКЛУФЗТСКФУУНАГКФУЪДГТКПНЗМУЗЛКДПЭЩДРФХИСФЭЛЕР
ЖМММПОСЗТЗДЗЖЗПЙУОЗТФРХГКЛУФДРГРЕЙПЗФММРЛЕТЗЧЗЕРСРСХФНРПКЙДРНКЪЮ
ДКЖЗФЮСРЗЧНЙЕРТРЖУРЖПКОСРТХЩКМРОЖДЙНКУУРГРАЪСЕКЖКПХЖТХЕДЖТХЕСЭТФ
ЮНЗМУЗЛКДПЭЩКЙМРНРНСРТХЩКМЖЗЫЗСТКЖДХЧУДКЖЗФЗНЧЩФРСТКМИЗЪЮЖЗНФЮПЕ
ТЗЧОУФЗТПЗФДЯФХОКПХФХДРЪЗНХТЖПКМОРНРЖРЛКУФФПЭЛМЙМОМУКОЭЩУМЙНЗОХМ
СКФПЪРФДЗЖКЕРЦКШЗТХМДТФКТХЖСРЩКЫЗУНХЪАДУКНКУЗЕРТРДПРФДЗЩНХТЖПКМП
ЗСРОЗУФКФЮНКЗЕРГНЕРТРЖКЗМКДПХСРНЗИЗДХДТЗЪЮОМУКОЭЩУМЙНМСКФПЪХСРНЗ
ИЗДКФМФЗУПРРПИЗОПЗМХОКСРОПКФЩФРОЭЗЕРПЩНЮПКМКРФДЗЖКЕРЦКШЗТММДЪЗКО
КРФЩЗУФДРОРЛГФАЪМСЗФТПЖТЗКЩРФДЗЖКСЗФТПЖТЗКЩМУЗОЗПХМХЙРДХРПОРЪЗПП
КМНРЪЖЮУДРАСХУФКНМРОПЗДРЕРТРЖПХЩФРОМУКОЭЩДУЗНКГНЕРСРНХЩПРДУЗУНДХ
ГРЕХФКЧРРФДЗЩНМЙМФРНЮМРМСТНСТРЧРТРДСРЖТНУДГПЗУХУФКПЮЗЛПЗЕХНКПРЛЙ
ЪЛМХЕРТЩЗЛДРЖЭКДПКЕПФЮКЩУМЙНМСКФПЪМТКДРОХУФТКЩМХТЙГЗТКСТРЧРТРДУХ
УФКПЮЗЛМФРСТДМФРДКПРДФЖРГРКЧКПМИКПХОМУКОЭЩУФХСЛУЗГЗУГРЕРОСЗФТПЖТ
ЗКЩОМУКОЭЩРФДЗЖЗФДУПДЪХМДТФКТХРФМНПНУХТЖПКМСТКДЗНОЗПДКЙГХУФРДЪХА
ПДЭУРМРОГЗТЗЕХТЗМКПУОРОМТАМТЗСРУФКСРНРДКПКЙГЭЙПФГЭНУЗОЮЗАУЗОЗПМХ
ЙРДЖТХЕХАРФДЗНКОПЗРПУРУФРНКЙРЖПРЛЕРТПКШЭЖРДРНЮПРРСТФПРЛТЙЖЗНЗППР
ЛПЖД

(b) Расшифровать текст:

ФКФЛХБЬЬКИГМЭЛЫЮЗСЗЯШЮЩЖФХЙЬЗББТСЭКВЬФБЕХЬДБЮТАЩЗЮТЕФЖБХЗОКЧЬИКЯ
БЧЗИЭДШЬРЙМУЖЪЮВФНДЮКШЕИЖЗХВНДЬЮЯЫЗЛАЛСЖБХЭЧЫИГЭГЮЫЙВЩЫФЬИЧЗЭЛЯЬ
ЮЪВЙЪКДГТХЛЮЗМЪЕФБМЬФЮБМЬБГШЫЯЭЮЬЛЦАФТМФИЮБЗЫЙЮЦЮСЖЮЦЯЧБИАВЭЛМЯЕ
КГЗЯВЭЖБОЛЮЙЖЭХБИЙЮВЭСЮФЛЮЫБЩДЪБЕСХЧКЫШЮСЛЮЫЦРЗДЦЯЩКГЧМИЖЮБДЪДХЪ
ИЭДЗТИЫЗДЮАСЖБШЬЦЗЛЮКЪЕЖЕИРБДБЦЪЙЮЭЫЯЙЬБДПМЪХКЩБЫЪИЩПЮУИРКБЮЫДБЙ

ЭВНЗЬВЭЯЪЮАЗФЗЪШМСЕЪЛЕШЖЗЦЯЭЛЫЮЖЫЗДГЮФГБЕЗЬЗЭЮЬЫЙБЧЗОСБЕЯЕЮЖХЮОЖ
ЗТЕРФРХЛЮЫЗАИЭКБЩЛЦБОУИЭМЭАЯХБОЯИШБЖГМЩФЮТИУЕМЙЯЩБЖХЙЬБЫЛСЦГАЪИЩ
ЕБУКТЭЖБДЪВЯШБЩБДХЭЦЗЕЛЛЧБЮШАСКЛЮДЪКЛММЬЮЪЮЬЧБКЮЛЮЗЙЮЗЗИЙТВЮЮДМЛ
ЮЫЖХЙЬЮКВЗЩЗЬЮЗРАЗАЮЧМЭХКТЖБШПОИЗТВЩЗЫХЗФБГАЯЫЗКВВОФКВКЪЮЖЛЫЗДБТ
ЖСКЛЕЙЬБАЭЗЩФОГЮЪЬЖЛЖФАКХЕСЖФЯИНЗДМТСВРБМФГАЪЖФЭЫЭВДЖБЬВЪЪДФМСДЕ
ШВВГБЕЫСЙЮУИОЖЗШРЦБЮЪБЦБЭЮЕТЮЖБМОЗЫТТФЮЗЕКЩЛХБЙЪГЗЩЛЮЫБХВНЮАЮЙЭЖ
ЗБМИКЮУИЦЙКЭЯЦЗЛЮКЪЬЗТКСЕЮЭВНФДШЛШБЭЫЙЬЫБВЯЧХКВЬЩЮКЯИЦЗВЭХШББЮЙЭ
ЖФЬВЫЗЭФЗЩФЕШЬПЗЭГЙЬЗБЧИДДЗТИУЕМЙЯЩБЮТВБЬДТЗЪЕЬЮКЪЭГХЙЬБРШЗЪЧЛЮЖ
ЯЪФЫВЭЛЙЮЭФЮЕХКЗИЙХЮЫЙБЭМЗЮЬХЗСЙДЬВЪЙЗЬМЬМЪХЗНЮЙУИШЭЪЛЙЬБЫХЛЮБЫЮ
ГЭГЗЪЮЪДЯЭИШМИЮЬФЖЗТЯЩБЧБЕСЭКВЬФЮЕСХЧЗЫАЬЬКГЮЯЯЪБХЗФЮЛАННЮЖСЯЬЬК
ТИСЫЗЫЦЩИЮАЯШЮЖТНЫЙЫЫЯЩББШЗЦЗЖХРЯКЕШКСЖБХЫЯЖЛЪКЮЮРМШФЯЮБМЪГБЬВЩГ
АЭВШБЦВИЭДМЗВЧЗКМЗСКГЮЕИГЗТКСЕЮЭВЫЮЙХЮЫЙБСХЮБЮЬЖЪБЕТЫСДЗУИЬКГГШЦ
ЙЮЯИЭЛХТЛСЪФЫИЯЯЮВВБЗБЫВЦАДЮЛИЛГЮЬЗЕЖЗЕИКЛТИЭДБИДЪЕДХЭЦЗИЮЬСЙБЫИ
ШЖБЬИШМЙБДЩБЧЫНЦЫФЕЖЮЮЯЭВЦЗЫЪИЮЗЙЛЯУДЗСЛЮЫЗТЕФЫЛЩЗСБЫЛАФЭДШНРЗЪЭ
ИПЗКЫНГЭДТИУЗЪЭИОДЮЭВНЮКЯИЬЭГЮЬЪЪЙЙШЭХГБЬЪЮЕГКЭКГЧНЪЭЖЦЮЗЫЮЗЯЬЗЕ
НМЪЪФЫИОЖРЫЯЪГЛСКПЗЭБВРЮДФИШЗЭШЗЭДМИЬЪВЗБЯЩЖЮУИОЮЛАВЭЕЗВКОЗГЭИЩЛ
МЗВНЮЬГУФЮЕШЖЪДМЭХЫЙБИЕФЕЮЭБОЛХЮМФЕЮЭВЦЗЕХЗРЖЛВИЮРКЮМЫЙЫШЕЭМГЮЖС
ЖЭЭ

2. Разложить на множители числа:

   (a) 1228884269115637156118343342749

   (b) 869251933458446354344836330698236060785093870243032869027769

   (c) 1049586212939606605070863084431344712597691816312835194769543141902849642735289846699998219

   (d) 17083068915171602598160346752614259703230483960359709541331885041286156132814043546964586580392921185488607957371327553 67

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 669351443313935031526468375406035913549174339661480894293768195722418398070 03$
   - $e = 17$

   Сообщение:

   - $M = 198288369981757830531123528709995541515951047964384864713293122835361627658 51$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 219913070908853111814514398003962603873$
   - $q = 207530023582026559357160268468100897079$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 37965119199788466810756692802798517399783956372183565659839822464481114539587$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 260152352676774840010722512673679521911$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 151098375638324353094828821518115926366$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 248769680479649808813767537214984950897$
   - $g = 224734626400882410341967347566336813 62$
   - $y = 180123334380855295728533512589900980713$

Секретный ключ:

- $x = 252325537303723935423592590317992776 53$

Сообщение:

- $M = 167106920658300797934169459939877496885$

Использовать следующий случайный параметр для создания подписи:

- $k = 280353398855991536782428340905544269407$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 205654287201565188980284502586059196557$
- $g = 139244276021653208013353409980545008598$
- $y = 108505755565190270342343514758329923710$

Сообщение:

- $M = 320837678157167555477915447832903232 56$

Подпись:

- $a = 158899284079956170777324696359369434621$
- $b = 141923634276928549169110942228237412418$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 617$
- $g = 76$
- $y = 447$

Сообщение:

- $M = 225$

Использовать следующий случайный параметр для создания подписи:

- $k = 403$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 2$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 44

1. (a) Расшифровать текст:

ЩГЧШШЪНЛМФПИТКХЧОЪУФХКХЦХЧЪЮПСФМЦХСХТМИТПУМФХШЩТШЦЧПШЙХМУФУМЧМФП
ПССЙУЪКХЛФХШСОТПЙФПКФЩГПЮЛМТРЩМССЧОЪУММЩМЛОЮМУНМУФМЩЪЩИВЩГШЙПЛМЩ
МТМУСССХРШЩЩПТЕЛПЛМЧЪЩШЮЩХОФМЙПЛТГАПФШУМЕШЦЧХШПЩГШТЙИХКЪЬХЛПТЦХЛ
ЯЙМЛПЦХЛЩЪЧСЪЙШМКХФШУХЩЧМТШСХМССШЩТПОБШФЩГМУЪЛХТНФХШЩГШМСЪФЛФЩФХ
ПЙФПКФЩГПЮФПССФМУХКУМФЦХФЩГЙХТЙЯШСОТХФСХТПЪНУФМПЙУМЯЩГШЙДЩХЛМТХЩ
СЧОЙМЦХРЩПСПЙФЪСЪОУПЮЪЛЛХФМШЩПМУЪЦХЛХТКЪШТЪНИВЮЩХЙЫХЧЩМЭППЪУВЯТМ
ЩШОТХЛМРШЩЙПМЦЧХЩПЙФХМСОМФФХУЪПФЩМЧМШЪФМИТКХЪКХЛФХТПИЪЛМЩКХШЦХЛП
ФЪСХУМФЛФЩЪЦЧПФЩГФЛТМНАПМУМЧВПШЦЪКТШПШЩТЦЧХШПЩГПЙФПКФЩГПЮФПЮМКХФ
МШСОВЙЩГСХУМФЛФЩЪФШПТЪМКХЪКХЙХЧПТХФЛТУФМШТХЙХПЧМЯПТШХЩФМКХХЩШЩЪЦ
ПЩГШЙМЮМЧЦЧХЙМТЦХХИВСФХЙМФПЕШЙХМУЪЬСХУМФЛФЩШЩЧТШСОЩГШЙМШМТВУПЧЙФ
ХЛЪЯФВУЛИВФМЦХЛЩГФПССХКХЦХЛХОЧМФППППОИМКФЪЩГЛХСЪЮФВЬЙХЦЧХШХЙФХЦЧП
ОФЕШГФМПУМТЩХКХЬТЛФХСЧХЙПСХЩХЧВУЬЙТЩШЦХЮЩПЙШМКЛЩМСХЩХЧВМФЬХЛПТПШ
ГЙУХМУЦХТХНМФППЙДЩХЩЙМЮМЧЧШЦХТХНМФИВТСФМНФХШЩППСЪУПТМФПЕУЧГПЙФХЙ
ФФЧЙПТШГУФМИХТММХИВСФХЙМФФХКХУВШТГЮЩХУХНМЩИВЩГЙПНЪММЙЦХШТМЛФПРЧО
ЦЧПЛЙТМРЙУХПЬКТОЬЮЩХЩХЩЧХКЩМТГФХМЯЙИЧПФЙПТШЩЪЩНМХЩЙМТМКХЙШЩХЧХФЪ
ПЪЙМЛХУПТМКХХШЙХМУЧОКХЙХЧМШПЙФХУПКФЩГПЮМУОЮМУФУШМСЪФЛФЩВШСОТХФУФ
МШЪЬХИМОФПЬХИХРЛМУШУВЪШТХЙПТПШГЛЧЩГШОШСПЧЛУПЮЩХФЬХЛПТПШГЦХЛТМСЧМ

ЦХШЩППЙПЩГШЩЪЛФЛЧЪКХРЛМФГЙШМЛГУХУЮШЪЪЩЧУВЧОКХЙЧПЙТПЦХЙПЛПУХУЪЩСЛ
ЧЪНМТЕИФХЮЩХПЙФПКФЩГПЮХЩЧЛХШЩПЦЧХИХТЩТШЛЙФХИВЩСШСОТХФУФМШЛХЙХТГФ
ВУЙПЛХУЬЪЛХРУПЧТЬЮЯМЛХИЧХРШШХЧВПФМЮМШЩМФЩСОЛХЧХЙЮЩХЮЩХПЙФПКФЩГПЮ
ШСОТСХУМФЛФЩЯСХЩХЧЙЪКТЪКЛТЙСЧЩВФМЙШТЬЯТШГПЙФПКФЩГПЮОУМЩПЙЙХУФМОФ
СПФМЪЛХЙХТГШЩЙППЙШЦХУФШЙХМХИМАФПМШУЪЩПТШПФМОФТЮЩХХЩ

(b) Расшифровать текст:
ТЯБОЙДИНГБУНКРКПАЮМИКОДЙЙКЙЮЖЬБЗЖИЭБЭМЙАЖКИГЕАЙОЖЪНБКТАТБМЩЗБМБА
ЭФЙЧАЙБНКЙЬОЧЮЕКЧЮЛМГКЙОМЫКДЯЙЬДГЗМЬБДЭСЬПОНЬЬЙБКДААЙЙАЭНОШПАЗШЙ
МДБЙЛМИГДЗИЖИБЙВЕОЙДДЕБКГГИЙКЕИИБЛКПКДОДУАЕДНИИКИЙЩБИКЗМЬКЕУГГКЮ
БИЩЧЗИЛЭГЙЖМДИБНФЯАЮЛГИБАОГДЛМКГЯВЗКЛАГКМГЕЭПМБЙИКЗМЬКЕНАЖБЕВГЕК
ЪДМЙОЙЮЙАЮЗНСАЮЙЖСЯИДУЛАВЙБМЯБМЙЛНКАДЙЙШКОЛРБЕЖОЭЛКНРАЮБМПКСЮААЬ
ТОДНКДНУПЛЙУНВЖЗВЙМЩЧЗКЖЕИКВЖЬОШЙНЬБЙДНЛЯУБАЛУНОЪДМШДЖЪЙКЮЛУВДЮМ
ЗМБАПКЮДЗПФИЙБЖЙБМАФЭПИБЛКЖДГКЭМЗКНЖНЗПЦБОБДАЕЖПГКАУНЖЕГЖКИГЕАЙО
СЬКЗЯЛРГХДЧКШЖМГЗКНОЪЬКЛКПГБАЙГЫКЙФГЫКДГВУСЙДМЩЩОККАЯКЮМИДОШЛЭУБ
ЯМЕКЙАМЩЙКЛМЬПИОЪЖЭБГМЗНЙКПКДВБЛСДЙКРЗМЮШРЭДСЮМИБЙЭСИЯБНЙААКММЫБ
ХБПЪКЭКВЕДЗДАЖОАЗГЕЙПЪЯЖЗББЛЬБВЙСЦЖМБНЖНОШИЛАГЗМЬБДЙГЛНЛБЙАЭЧАМЙ
ОДЯЛЛОШДАЕЖПГКАУКЭМИКОДЙЙЖВБЛЭДНЖЕГБЕНЙУФШОЩДОПФИАЮНИМДАБЗГЕБКОН
ИЮДОЪГДЮННЖАЗБНЖЖЙБСЗМЮДКЙИЧНЯЛЙОКАСДЖИЖАЛПНРЖБНЖЕГЖКИГЕАЙОЦЫАБО
ИВМБЛМЙОШЖСЬЭЧЛСГДЙБЕГБОЗЖПБИЭГГКЯКОЙЖЙБЛЬБВЙПГЮЭКБЛАЮАФКШЮОМИКЕ
ЯМЬЮЙБЗЗМКВЖЪБИЮЖЬЗДДЯРЖДМФЭЮДЖЖИЯДГФЭЮЮКПФДКОНЛЯУБАЖОНДВАИНЙСДО
ПФИЪКГМЕАЗДЮЛВПЩИЖПКНОАБНЛКДГПЕЖМГДОЧЛВМБЛМЙОШЙЦЛЙАБГРШНАПДФБЕРЖ
УОКЛДАБЗРФСКММРКЖКЙАКОНЖЬДИНЖГДАКДЬБИНПАЖПМПЕПЖКЙАГЗКВЭДЮКЕФИПОИ
ИБЛКПКШЙПРЖЯАОСКЮНДЙАНБЯМИКЮЙЕАЖЙПЙЙШДГКЖЗУЗПЪДАККПМБГАУУЕЙМЫКЮК
ЙЕБЙДЛЭОЮНЖГДНББЖМКЮЛЗМКАМГВЗЖМДБЙАЛКГИБХПОКНЙЖЮБЯМЗКАБЗЙОЮКАГДИ
КДЭОЭЧРФЮЛБОЪЧЕМЕЪБЯКДАГЙДКРБГАГЙШКНРЪОШНЛЭЯКВГЖОЛМААИББАЖМБЙЯЛМ
ЯЖГЭЖМБПКЙКЕККБМДРДДЮКЗЙЖДЛСРБЖАМЪКЗШЛЖДНОГЕЖИБЛЕАДОГЩБНКАЭОКЮЙЩ
ЧНЙГЦОПАДЭКОЛОЪДОШПЬМКИХККОЧПКМПСНЖНИКРИДУОМЙОКЭМЦЭПАГКЖКЗЖЪКГШК
ЛОРКОКБТДЬЗМДНРЛЛКИВЖЭМКПВГЗЖМДБЙАЛКФ

2. Разложить на множители числа:

(a) 469567392366101155530475126541

(b) 858643836182484642376276572081369217189016354035448712366749

(c) 10212196361102620261553094975310717681024210756487265542554971272215706387965245990741286 33

(d) 1286306861999587208595675574854217551904538864027780573134076382175104150952938915401443327605055048813902689337394097593

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 6961396293844646230102003699896580483817613589130509915765504745747487970146 1$
   - $e = 3$

   Сообщение:
   - $M = 583715767050501362375182636100577197782547762306349159385929454619786107087 37$

   В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 335317201137081305390532103282396554953$
   - $q = 235208026268262184640490151489592425439$

   Открытая экспонента:
   - $e = 3$

   Зашифрованное сообщение:
   - $c = 584940876555501259121046822050883981304642143295531917451213832271387280061 51$

   В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 107275031717667943461477377388634140653$

- $e = 5$

Зашифрованное сообщение:

- $c = 5128767490924484686747427994193796832 3$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 24255795717689330897834785065274947 8749$
   - $g = 13122225727850611755432677076860466 1847$
   - $y = 41807651728338124242539840058276506074$

   Секретный ключ:
   - $x = 23512235263794454658082149109989802 8436$

   Сообщение:
   - $M = 14711493853010895164926885209316409 5391$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 21576358116618089470342906852294173 6509$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 24345927558275268415929057087223589 4389$
   - $g = 30572077424094187484962401629807777169$
   - $y = 21408612531775393423326441530353990 1474$

   Сообщение:
   - $M = 20496646378179096630570495492864149 1091$

   Подпись:
   - $a = 19478205158293148476092085090688061640$
   - $b = 24237655450436611322347197313683629 1709$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 953$
   - $g = 906$
   - $y = 808$

   Сообщение:
   - $M = 178$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 837$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 13x - 13$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 45

1. (a) Расшифровать текст:

ФИИПЦЙИПИЬИРИСДЭФРОФРСТУИЗОСЙИРЛИПСИРИЗСОЙРСДЮОСЛШЦЗЛЕЛХЯРЛРЛПУЯ
ЛЕРСЕРРИФХУОЛФЯФНУЮЕХЯСХРЛШФЕСЛЪЦЕФХЕЛПЮКУРИИДЮОЛЦЙЦЕИУИРЮЕЛШФСЖ
ОФЛЛРНСРИЩСЗРЙЗЮЦХУСПФЕИОЯЛЪЕСЫИОНСПРИЗИУЙЕУЦНШТЛФЯПСФШЕХЛОИЖСФХ
УИТИХСПЗУИФДЮОРТЛФРУЦНСБДХБЫНЛАХСТУЛЦЖСХСЕЛОСПИРНЪИПЦХСЕЙРСПЦЛДС
СДЮНРСЕИРРСТЛФЯПТЛФОНСПРИПХЦЫНСРЕНСРЩИТУЛТЛФЮЕОРИФНСОЯНСФХУСНЗСО
ЖСРИУФТИЪХЮЕОТНИХЛТИУИЪЛХЮЕОХСУЙИФХЕИРРЦБРЗТЛФЯФЮРЦПСИПЦТИХУЦРЗУ

ИИЕЛЪЦЖУЛРИЕЦЕСУИРДЦУЖФНЦБЖЦДИУРЛБЕДИОСЖСУФНЦБНУИТСФХЯФХУОФТСТСЪ
ИУНЦЦЖЗХЯУФТСОСЙИРЛИЗЦШЕНСХСУСПТЛФРСДЮОСТЛФЯПСРНСРИЩУИЫЛОФИЖСУФТ
ИЪХХЯЛФТИУЕЮШФХУСНЦЕЛЗИОЪХСЕФИЗИОСТСЫОСНЪСУХЦФСЗИУЙРЛИТЛФЯПДЮОСФ
ОИЗЦБЬИИФЮРПСМТИХУТЛФЯПСХЕСИЕНСХСУСПТУСФЛЫЯХЮРФСУСЗЛХИОЯФНСПРЫИП
ДОЖСФОСЕИРЛЛЛФСЖОФЛЛРДУНФПУЯИМЛЕРСЕРСМЗСЪИУЯБПЛУСРСЕСМПЮТСОЦЪЛОЛ
ЖСФИЖСПИФЩЛРИХСОЯНСРЛПСИЖСДОЖСФОСЕИРЛРЛПСИЖСФСЖОФЛЗХЯХИДИРИРПИУИ
РРСИЬИЛФСДЛУБФЯЗСХИДЗСДУХЯФЗКТУСНКЮХЕСЛТУСЦЪЛХЯХИДТЦХИПННПОЯЪЛЫН
ЦРИФПСХУРХЕСМСЧЛЩИУФНСМЪЛРЛДСХЮЗСНКОЪХСЫТЖЦРСФЛХЯИЬИРИЗСФХСЛРНСХ
СУТСЙОСЕРХИДИРКЬЛХЦСХИЪИФХЕРИЗОЗЦИОИМФХНЛПЛЙИФСУЕРЩПЛННСЕХЮФПРИП
ИЗОИРРСДЦЗЦТЛФХЯНРЗУИБНУОСЕЛЪЦТУСФИЖСТИУИЕИФХЛХИДЛКДИОСЖСУФНСМНУ
ИТСФХЛНЦЗРЛДЦЗЯТСЗОЯЫИЖЗИДЮЗЦУЯЦХИДТУСЫОПХЦЫНХЕСЦКРЕСХЕСИПТСИЗЛР
НИЛСХСПЪХСХЮУРИРФЖСУИФХЛКРИПСЖОЛХИТИУЯОИЙЛХЪХСЛКХИДДЦЗИХПСОБДСЖЪ
ХСДХЮЛФТУЕЛОФШСХЯЛРИФПИБРЗИХЯФРИЖСЕИОЛНЦБПЛОСФХЯСХИЩХЕСМЖЪХИРЛИФ
ИЖСТЛФЯПЕСКДЦЗЛОСЕСПРИУКРЮИЪЦЕФХЕСЕРЛЙИФХСНЛИЕЮУЙИРЛРНСХСУЮИДХБЫ
НРИТСФНЦТЛОФЖОЦДСНССФНСУДЛОЛПИРТУИРИДУИЙИРЛИФННЛПСРЦТСПЛРОСПУЯЛЛ
ЕРСЕРИНКОСФЯПРИФХСОЯЙИРИТУЛФХСМРЮПННЛРИФТУЕИЗОЛЕЮППЮФОЯСТИУИЕИЗИ
РЛЛПСИПЛКДИОСЖСУФНСМНУИТСФХЛПИРЦЙФОРС

(b) Расшифровать текст:

ШЗАСЮЫГИЧЯЮЬИХАЖЪТТУВЗЙЯЮЖВЗЪЦЩЯЖХВЕКЩЮУБХЛАЫЖНЖАЪГКЕАЗЮКДЭДЭКЮЫ
УБЗГШЩББЙШЯЯЬИЪЯВЗАСАБОАШТОИЗАПЮХНАПЭЮИЙГЭЕЗААБЫЖЫЭЖКИХЧШДГЛТЕХУ
ЧАШЙЛЪХГЬГДЙШЖНШВХЬЖЙЩКИНЫШЯДЙЛЩЕЕЖЧЭШДИТДВЗЗЙВКЙЙЯЦФЬМЯЯЫЙКШПАУ
ЯЬЯЙВОЦДЪВЙСГПЛОЬЯЙВОЦДАЬЮЫБЖОЕАЮШПАПЦЮЯЖЮАЖЪТТУБЖОЮГЫВЛАЫЖИЕФУД
КМЩЦЛБЙЛЦЦЕЬШФБЗЙСЩШЮИЯНБЫОЭЦЮЕНЭХБИНХАБЫЦЩЩЕЬАРЯЯЬИЬЯЧДЖХЩБИНПЩ
ЮЯИЮУБШЙСЦДЙЖЮЭБЙЛТГПДКЭЯЧЕЖУЦАЯААЧДДЙЦЫБГАСЩЫЭГЯЦЮЯИДЬЫЖЛХВЦЙЧЫ
ЮЫЖЙСЖБЫГШЩБЫГЪШЧЗОРЩЯНЖАБДЖНХЦЫЖЙЯЯЯБЖЪВПИЗЫШХДСАФГДГФЯАДЦТВБВЯ
ЯМДЙЙШЩЕКНУЦГЕНЪМЬЖЙЭГАЕДПЯБЗОУЦАДЦЦГЖЖЦЩЩДЩЙХЭЫДЙУЮЫНЗХБШЮЖАЮЫМ
ЕЫВОЕИХЯЕЗРХУДУКЫХИЕЯХЬЫБЛАЫШЖОРИШЩЕЫГБЗЦЦЯФСЭШЬЫГКЭЯМЬИХЦЫЖЛХЮЫ
ГЖПВХЕЩЕЪЭКЭЮЦРЙЙЬББЫЙШЧЮЕМЙЯЭЕЖЫГГЬРДВБЩИЧЯАЬСЬДЦОАПУДЙЖЮЫГЬМТЬ
ЫИЙЕЦЮИЕЭМЮУСПВБЖЛЫУБЭЯТЮЫЯМПЯЫММЯБЛЯИТЭЖЖЙСУШВГОЦЮЕЮЫЫБДОЧБЛЬИЪ
ЯЦЕЬЫФЕЕДЮТГКАЦХХБВЧУЪВГТФБЖЙСБЖБГХАБИЯХЬЫДМТХЮЕЙЪЯФСЭХЬБЙСАФШЗМ
ХЭЖОНЫТЖЫАЯЯФЬЯЯНЖДАРЯХФНАЭЫДОЯДГЮЯШВЩЬИЮЫЫАЕЭЩЭДАЮЫБВЧЧЯГЮЬЫЪАЯ
ЕЫУХТНЖЩЮЯИЧБОВЧГЯХИГШЩДКАРЯГЕЭЪДГИНЭЦВДИАПЫЗВСЦЕКЩСЯАЪЙСЩАЯВЪЩИ
КМЬЦЮКБТЮГЫГЯНДЩАТХЖПАРБШАЕАХГКЮХЦЕИЕШЩВЬЛХЮОИОЪХЖБГДЪАКЩЬЯДКЯАТ
ШВЧТЩХИЩЭДИВЯЙТЕХУЧЩЯЕГЧБЫОЖОЦЧДМЯБЖПЕЫГВКМЯЩЕЬЯАЙЖДКЫЫАЯАЫГЙТЛЫ
ХАТАЫГХЬЯХГШГАЪЫЫЩИАЫЖЮЗХИЖЩЯЭДЦЕИПШЦВИАЬАЩГЮЦЮЯСАЩЖЮИШВХЕАРЯЯКБ
ФЬБЫАХШЭЗГДЬБДЭХВДЙОЬЬШДГХИЕЕШЯЯХТМЪЩЯИЯТЬЮЯМПЦЕЙЦЩЯЬЯЭЪЫЖЮЗХИЖЫ
ЖЮЯЮЫНЮЫЦЕЖЫУЖПЕЪЦЕЗЙЪДЮЯНТТАЯУЯМЭЯКЭДДИЕХЦАЯКАЬЫЙОЭЦЙБГТЮШЩТТВЕ
ДЙЩТБХКЫЬБЭГШГОИЭЫЪЩЯЭЫГДЪГЪДЮЕНОЦЦВЙРЯЭЙЙЭЧАЯЕАЮЕУМЯБЖХЭТХПГОЮЫ
ЪВКАФКЬЭЯДЕГЙШЯЧЕДЧШЭКЯЭЩЮЬАЮТЮЬЩЬЯЦЕЖЫУШЯЙЪДВВЗТБЕЩИЮГЖЖАЪЩЭЗЦШ
НЙЖОРИШЩОТЖЮДЛЫХФЗЙЮЩОИВЪЩЯЪЖПЮШЮЭЪМЬЪЙЮГП

2. Разложить на множители числа:

(a) 60125593776229005538415430230 3

(b) 787599349772033443316777635694618128082058549463153749212021

(c) 95364450363869672421680964793589904291314153964483249945735197658576771124413443292162589 3

(d) 946487099256680802293655020841561451466944274299329918341495955308203888871304716478151378163963911242812092070814916307

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 990878641063121110902656692827149865027346258050904561418298801418407466699 63$
- $e = 3$

Сообщение:

- $M = 935034826603972098659481605093725479412097748868057163417518231598849753626 20$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 327368257674643383494858716164342326147$
- $q = 330290858586295547452946097902753128483$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 430706909440163478892930961489969081929531354006408075756015640104846403317 04$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 162973676717377206668003892228950363479$
- $e = 3$

Зашифрованное сообщение:

- $c = 106071705655663057974799012250999714977$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 18641477115984319224266456807929296 4651$
- $g = 86139520198250821663584348383338532254$
- $y = 14517577143584751370877894158380460 0235$

Секретный ключ:

- $x = 17224113359762698384613311490603564 4591$

Сообщение:

- $M = 12912547015069982009438496790584908 0544$

Использовать следующий случайный параметр для создания подписи:

- $k = 14940089281358465736609096864969306 5161$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 30537396898636719656936505651408848 1299$
- $g = 27803898642530185451990247114811690 1313$
- $y = 26165975473149317617437690989054213 1403$

Сообщение:

- $M = 41708768263410353471279147132465879465$

Подпись:

- $a = 15079516946033961112585422909939277 9253$
- $b = 12282051348157699711607808433957638 0719$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 613$
- $g = 122$
- $y = 160$

Сообщение:

- $M = 552$

Использовать следующий случайный параметр для создания подписи:

- $k = 505$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 2$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 46

1. (a) Расшифровать текст:

АЪЖЭЕЕУЭЗИАЫЖКЖЪГЭЕАЬЛДГВЖДЭЕЬЕКРЛЮЕЭЮЬЛКГАЕЗЬЭЕАЖКВАИЫАЯОЭЪЕЖЕЭ
ЛЮКЖАЪЕВЛЯДАПЙКГЩУЖКДЭЕКАКФКВАЭЗЛЙКВАЖЕВГАВЕЛГАЪЕАЫЕКФАПЙКЪЭИЬУД
ЕДЭИЭЕАЭДЪУЪЭЬКФЖКЕЭЫЖКБЕЛВЖКЖИДЛПАГЭЭЬДЙВЖЭГЦЩЖЗУКЙКЪЖЪЙАГАЙЭЫЖ
ИЖЪЕЙЬЭГГЭДЛЕЭЙВЖГФВЖЯДЭПЕАБВЙКЭГФЕЖНЖЯБЙКЪВВЙЛЬАЕПАЕЦСАБЙГЭЬЙКЪ
АЭЪЖЗИЖЙДАЗЖЙКЖИЖЕЕАДАЬЩУЙЗЭИЪЛЙУЗАКФЖЙКЖИЖЮЕЖЙКФЖКЪЭКПАВЗЖКЖДЗЖ
ДЖГПЪЕЭЙВЖГФВЖДАЕЛКЖЕЫГЛЩЖВЖЪЯЬЖНЕЛГАЙВЯГВПЫЖГЖЪЖЦЫЖЙЗЖЬАЩЖЮЭДЖБ
ЪАРФВВАЭЕЖЪЖЙКАПКЖАЯХКЖЫЖЩЛЬЭКАДКЛРВЖКЪЭПГАЪЕАЫЕКФАПЩЖЫДАГЖЙКАЪЙ
ЖГЬКЛЕЙЬЖЪЖГФЕЖЗЖИЖНЛДЕЖЫЖЗЛРВЛЪУПАЙКАГЪЖЙФЬЬАДЖКЗЖИЗЛЫПЭЪЛЫЖЙЗЖ
ЬФЕЭЪУЬЙКЙЪАЕФЕЭЙТЭЙКПКЖЯПЭГЖЪЭВХКЖКЗЛЫПЭЪЙЗИЖЙАГВЖДЭЕЬЕКРКЛКАЪЕ
АЫЕКФАПЯДЭКАГПКЖЗИЖЫЖЪЖИАГЙАЯВЛЙАГЯУВЕЖЛЮЭЩУГЖЗЖЯЬЕЖЪЙАГАЙЭЫЖИЖЪ
ЕЗИАЕЛЬАГЭЫЖЪЖЪЙЭДЗИАЯЕКФЙЬЪЭДЛЙГЖЪЖЕЭИЙЙВЯУЪКФЖКЖДЕАВЖДЛЪЙАГАЙЭ
ЫЖИЖЪЕЙЬЭИЮГЙЪЖЭЖЩЭСЕАЭАЕАВЖДЛЕЭЙВЯГЕАЖЬЕЖЫЖЙГЖЪВИЖДЭВВЗЖЗЬФААКЖ
ЗЖКЖДЛКЖГФВЖПКЖВЖИЖЪЭЭНЖЬАГЭСЭЪЙКЭЗААДЖЫГЩУКФЯНЪПЭЕЯГЖЬЭДАЪЙВЖИЭ
ЪЙЭЯЫЖЪЖИАГАЖЗЛЫПЭЪЭКЖГВАЩУГАИЯГАПЕУВЖДЭЕЬЕКЗЖЙГГЛИЬЕАВЙЗЖИЛПЭЕА
ЭДИЯЪЭЬКФНЖИЖРЭЕФВЖЖЩЖЪЙЭДЗЖЙЖЙЭЬЕАДЙЭГЭЕАДАВИЭЗЖЙКДЛИЬЕАВЪЖЯЪИК
АГЙПЭИЭЯЬЪЬЕАЖЩТЪАГПКЖЪЙКЭЗАЪЭИЙКЯРЭЙКФЬЭЙКЖКВИЭЗЖЙКАЪАЬЭГЖЕДЕЖЮ
ЭЙКЪЖЖЫЕЭБАЙГУРГЖКЩРВАИОЭЪПКЖАЬЭКЕЭЪЭЬЖДЙАГЪЗИЖПЭДЕЭДЖЫЖЕЙВЯКФЕА
ПЭЫЖЗЖГЖЮАКЭГФЕЖЫЖЗЖКЖДЛПКЖЭНКФЬГФРЭЗЖЩЖГЙЪВИЭЗЖЙКАДЭЮЬЛВЯВДАЯДЭ
КЕЖЙКГЖЕЭЖЩУВЕЖЪЭЕЕЖЭЪЖГЕЭЕАЭЪЖЪЙЭНЛГАОНЖЕАКЖГЗАГАЙФЪВЛПВАКАНЖИЯ
ЫЖЪИАЪГАДЭЮЬЛЙЖЩЖЦАИЙНЖЬАГАЙФЛЪАЬЬИЫЛЕАГАЫИЕАЯЖЕЕЖЫЖЙЖГЬКЗЖЬЖЙГЕ
УЩУГАВЕАДГЯЛКПАВАЦГБВИЭСЭЕУБВГДУВЙЬЭГГВЖДЭЕЬЕКЛЪЮЕЖЭЬЖЕЭЙЭЕАЭЗЖВ
ЯЕАЛИЬЕАВЗЖЙГЖЪДЦГЩУГАГЖЮЕУЗЖЪЖЯЪИСЭЕААЙЪЖЭДГЛВЪУБВЯВЖЩТЪАГЙЪЖАД
КЖЪИАСДПКЖЖЕЩУГЛЩЛЕКЖЪСАВЖЪЗИЭЬЙКЪГГЙ

(b) Расшифровать текст:

ЕЗТЪЗЬАТЕЖПШЕЪБВТСФАХДНБЛШЧБЕДНДСЭЭЪТППЛЪКЕОЗЪДВТРЧЙДШЪЪДРСЫПГЕЬ
МОНИЭЭХДМЭЙСШЕМКЬЖИЧМНЖИВГШИРПИЖЫВЧЮАЖСЬЫШШЛОМЦЯПЪЗЦЫНБЛШЛОБЮВТО
ЬЕПГНПЗЬЗТМВФАОПЛПЧЕОЮХДДШБЧДГШИЪДЧПЬШАТШЖТЕОЩЛШИБЬХФЕОЫДЭЬИЦЖПШ
ЕЪЗУЮПЪЫОДЮТЛПЧПШЯХЙЮТЫЮЫЛЖЭЦЖШХФТШКЧАЖАКЬФОЙМПСЖГЕЬЗЬШЕБДЫИВПЙО
ДСЬБИЕРТЙШЪНЕВОШОЪЖТГПЪБЫЩЛНЗЫЙДЪФЧЫИЦИПЖТЪБАЫТПЪПЗЛЭЯТИЬЧЮЦДГЭГ
ШБИЬФМЗМШЕОЫЛПЯПБЕВХЦГЕОЗЛЖТФЗЬЕУЫЛТВЕЧЫШЖЕЧЪЭЖГЩМННЕМАОЙМХКФДЛТ
ЗЬЕУГМЫАЗХЗЧИКШЪППЕВХЫБИЩЗФЖЙЧЮУВЕЪЮЩЖОЬБМВЕЧЖПЗЛЭЯТИЬФГЦДГЭЛПЧЕ
МЦЬДМШЪППТЖКШИВПРХЗМСЖПОЬЧЮЦДВШДМЫЛЬБОИИЩЙШИИМЛПЧПШВОЙДПДЬТНПРПЩ
ОЬФЬЫППЙЖЗМЧРХТНТГЫВТЬЮЛЙЕВХЩДВТЖШШЕЧБШИСМЗТЛНБЛШУТШЪЭЪЕЬИШЛОРЮП
ЗЛТЗЬЗЛЭЯЛСОЬГРЙСЖГШЩДЫДЭЬБЦЗЩДНОЗЛЮТЫЬШБОМЕШШТМЗПЯВХКЬЮОЬИЭЗТТС
ЖВЕЧКЩЗИЛЗФЭНТСЖЧОНЛПЧСЭЭЖЗКСДЬЫБПИЪШДЭЕШЮСФЙПГНШКЬТПШЙСЮЛЩМННЕМ
ЛФЮБЕЛЖЗКСДШГУОЙЦЫНЩЗЩБЕБМФЭНТЛЖИКФАЧЮТЖЕТБОМЛЖИКЦБХДВЬХЫИУЩВЫЫБ
ПЖМЗЕБЮЬСРПКЬДРШЖЕЮДПДУНТШОШНЕВХСШТЪИЪЮХШЭТЗОЦЖШФПЪЗЫИИЬХЫИЕЩЮЪТ
СЬМЩЯСПЪПЗПЬХТВЕЧМРЪРПЕФБОЧБЬДСЬЫТБПЭЬБЫВТЫЕОЕХЖЭБИАМЧДЧЖЪЕБТТОТ
ВОЪЗСГМПКАЮЗМЮСЪЫЪГШЗИХБШЗВПТЩБОГЭЮВТКПБИАММАРПИШЗТТЫЫЫБЕДШЗПШГ
ШЯНШБЬЫМЧЗЬДЛЖГШШКЛГПЗВПЛТБСШЬШГЬТЙСЪВХБЫТКЪЬФЮЗЩЗСЪЛЕОНЙЛФЫСЩЛЧ
МХГДШЕЫШЩПЖЧЮКЫЛМГИТЫШЖОЬФЛСЛТАЩЫРЬФФЭЛШКЖШСПЫЧЫМЛФХДТТОШЕРТСПБК
ЫЮЛЫНФЫЪИИЪМТГШПДЫШЕХХТНГШЙИФЩПЬШЕОЦЗПВОЬКЭИСЬЫТЮВПКЬТОЫЫШЧООЮЦД
ЕУЗЛЖДШЫХЫГШЖПЗКСЖЧДСХЫЬЫБПЫХЪЫФЗЫАЗХЗЧЕЕЪЮФЖЕЫЛТШШТКЖНЕЦКМЫТШКЬ
ШИЦГЪЫПШКЬТИЩЗУЪЕЦГЭЪГХАНБДЬЛПЧЕФЗПНТШАНДТШЫТБПШГЭОЙФЬЬФШФЭТЕОББ
МЯСПЪПЪОЭЛЪАКЭОЪЮСЬАЩЭУВГШЯПШКХЫДШЫХЫГШКШШЕЬМТЕОЭЯТГВЫЪШБЬВБЦЕ

2. Разложить на множители числа:

(a) 819928770670677847768395801607

(b) 1002105323123726148237796166092467185613360277238593358597221

(c) 614407175746193951913091198397077559958407086247581117631110450296039767765063734456426507

(d) 142321833852319940933192292583524322419629732474233107757301129037459436121163712590295777923396307488640786237606739776 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 750129732880338199365506116785034052620772993315273473193951406340061173706 99$
   - $e = 5$

   Сообщение:
   - $M = 705515471231359291218934095459460118947241289058400124608161160303165135781 51$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 3062042276154158804406177834961245653 09$
   - $q = 2615056761119258125930905978488302647 97$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 1473175271607674570955708805986166278236912210524674463432461990061097017377 0$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 1218048134421230642547659072030771667 77$
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 2141144334538175414068622028826407492$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 288357970565850669769466002671245891753$
   - $g = 231073595513703912355893502867791471780$
   - $y = 517237733442641026747388150640079963 2$

   Секретный ключ:
   - $x = 205130506661468507788886255080682121917$

   Сообщение:
   - $M = 147005111935781642146308073913743611594$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 468818832456229574456607175973258111 43$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 261645919360279864506550824640852823749$
   - $g = 145142370302899574504324266539047635542$
   - $y = 218450114446562583385177314804550042 88$

   Сообщение:
   - $M = 873944784886750434850444505322429085 04$

   Подпись:
   - $a = 173876406634299028740415442221956647868$
   - $b = 761637573354681743729125948493649551 44$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 521$
   - $g = 277$
   - $y = 469$

   Сообщение:

- $M = 138$

Использовать следующий случайный параметр для создания подписи:

- $k = 19$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 16$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 47

1. (a) Расшифровать текст:

МШЪЫШХОЬЦЧЭОПЬЭВФТЩШЫЬШТЦЫПНШОЧСЦЬЭВФЭНШЫЭОЪЕЧИТОШФРПЦМЫПЦЭЫМПЬЭ
БЬШЦЕХИОТЛЪМЕПТЩЪТЫРЧЕПЫШХОЬЕНЪШЦФШТСДМТХТЭЫПЪОТПВМЛЪТЧЫЬШХЩШОХП
ЦПЧТЩЪТЫЬХЖЧШНХОПХЧЧПЩЪТЬПХХИОТЪСДПСРИГТПМЫЬПЩТСЦПЬОМТРПЧТПМФЪПЩ
ШЫЬТЫДПЯХТЫЖМФЭБФЭТЫЬХТЦПРОЭЫШЛШИЬШХФШМЬЖФШЦПЧОЧЬМПХПХТМЧЭТНЧЬЖТ
БЭЧМПЫЬТЩЭВФЭЧТЯЬШХЩЭТЫЦЩЪТЫЬМТХЮТЬТХЖОЪШСРЭРРХШТЩЪШХПЬПХШЧОЧТЦТ
ЧПЫОПХМЧТФФШНШМЪПОЧПСОЧТФТЪЫЫПЫЖЬШЬБЫЭЫФФХТТСМТОЭТЫЬПЩЖШЩЭЫЬПХЬЭ
ЬМТХЫЖЧМХЭМЫТХТЫПНШЪШМЧТЫЧПИЦВЧПЯШЬПМВШЬЫЬЬЖШЬЧППЧЭББЫЫФСХФШЦПЧО
ЧЬВФФШМШТОПЬЛЬХЖНОПРПЧПЩЪТЬПХЖЧПЩЪТЬПХЖЧПОХПБПШЬМПБХТМЧФЭСЦТБЛШН
ОЫЬМЫПЛЭОПЬХОЧШБЬШЦВЫЬЪВЧШЬПЛПЧПЬЩЩПЧЖФШЬМПБХЦЪЖТМЧШМЧОШЦШОЧШУЫЬ
ЪВЧППЬЭЬШЧМСНХЧЭХЧЦПЧТЫЭЫТХТПЦЭХЕЛЧЭХЫЖЧПМШХЖЧШЫЬТЫЧЭХЪЭФШЬЖЦШПУ
ВЩНТМЫЩШЦЧББЫЧФЧЭЧПЩШХЭБТХППТСППЪЭФФФЛЕЧСГТЬЭЦШПУХИЛПСЧШУЫПЪОАПЦ
ШПНШЪПХШМШШЛЪРХЫПЛППЪЕАЪПЦРРОХОШФСЬЖБЬШЛЕХОШЫЬШТЧППОШМПЪПЧЧШЫЬТТ
ЫЧПЬПЪЩПЧТПЦЫЬХШРТОЬЖЪПВТЬПХЖЧШУЦТЧЭЬЕМЗЬШМЪПЦТССМЕЫШЬЕЧЯШОТМВПУ
ЫМЩШХМПЪЫЬПШЬФЪПЩШЫЬТЩШФСХТЫЖЧШМЕПФШЧЧЕПЬШХЩЕТМЫФШЪПЫЬПЩЖЭЫПХЫЖЦ
ЧШРПЫЬМШЦХИОПУМШШЪЭРПЧЧЕЯФШЩЖЦТТЫУОФЦТЦПРОЭТЦТЧЛПХШЦФШЧППЯХБПХШМ
ПФМФЪЫЧШЦФЮЬЧПЫШЛЧРПЧЧШУЫЛХПИМЪЭФПЗЬШЛЕХЫЦЩЭНБПМШЧШЫЬЧШМТХЫПНШШФ
ЪЭРТХТТФФМТОЧШЩШПНШЩШМПХПЧТИБПЬЕЪПБПХШМПФШЬОПХТХТЫЖТМШМПЫЖШЩШЪЩШ
ОЫФФХТЩШОЫЦЭИФЪПЩШЫЬЖЦЕМЧТЯЭСЧХТЫМШТЯТСЦПЧЧТФШМШОТЧТСЧТЯОПЪРХЩШО
ВЩФШИХТЫЬЛЭЦНТЭОЪЭНШНШЧФШЩЖПМШЬФЧЭЬЛЕХНШХШМИХФШЬШЪЭИЫЬЪЯЧЭМЩПЪПФ
ТЧЭХШЧФЧЦБЪПСБЫЬШФШХНШХШМЛПОЧШНШФХЦЕФЭЩХФЧШНЦФШЦПЧОЧЬТСЦПЧЧТФТФЪ
ТБХТЧПЫЬЪПХУЬПМЕЯШОТЬПМШЧФНШЫЭОЪИНШЫЭОЪЖСОПЫЖМШЬМЫСФЪТБХТМЧФЭСЦТ
БЪПЛЫЬЪПХУЫШХОЬЕЧВТОХТСХЩФСФОПЪРМВТУЩТЫЖЦШСВЬХЫТЫМ

   (b) Расшифровать текст:

ЙЭНЦЕЙЦЙЫЛЩЦГАОТЪЭАЛЦФМНОЦСЛНМЪПТРЯПДДХРМПЙЬЗОЧОЭЯМЬЯУПМЧЧШЛЮЮЙЬ
ЙХУЭШУЪЭКЩОХНИРЮВЧЙЮОЩЪНЗМЧЪНУЯЪЫЛНЕТИИЩАХЪЛЮГПШИРКПСЗЩВИЗЖЩМЧФИ
ЭЛЮФИЩЯФФЕЧЕШОИЩЫФСЬЦАХЭЕЦЛФЩЙЬППКЙШЕЙФЯРИПОИРЙХЫЛЩЙМЮТУЯХЭНЗЕЛС
ЛТЛШЮЧЧЛТЪЯЩАХГАЦЛЙСЕЪЛЛЩЖЬНХЫЙЭЕЪЭЖЖХТОМЭЯМЩИЩОТЪЭЩЙХЧЙХЛШЪМЬНХ
ФВШВШСИШЛМЦАЧПХОКЩИКЪЖЩОКСИРНТЪЬЫППЧМХЛУЩАУОСУЖЬРТЗЬХЛЕПКЫМХЬФУЗ
ЦСЛНШМПЙЦЛШЩЭЩВФЩЦАОХОАЭТЦЪЯЙПШЪЬЖЗФЪЭРКФЪЭЪЛТИВЮБЙФБРКПХИЬПЪЫНР
ИГЩЦАЪЩЪВХЛФЩЦФМХЬЯЩЗЩСКРНГЭНШВУЫЛЩБХЧБЭЩШЪЬУНФФАОЛТЪМЩЯКЦЙЦИМТМ
ХЕРЭЙНВЩЩГХОСТГЭВФШЭГВУЩАШЕМЭНЫЕЮЪЕНАТУАЭЛЙЪЗХСЩЩАЪЛШЫАГКХРЙЪЕТЮ
ЛРПГКМНЛЕГУХРОЩТУПМЧЧШЛЧУЬНИМЩИЮЫЧЪЗЩЙПЪННВЮЧЮРКМЬЖЮБЪШЩНХМЫЛРЯХ
ЭРЩБПЮАЦЩШЮЭЩФЩЪИРБХЧБШЛЛСДЬПЙЬЭЭЩФФИЬПЪЫНРИГЩЙШЕХНЙЫЛФФНРИГЩЙХЗ
НСНХАХЭКЩБПЩЕЩИТСБЬЗПХМЩЯМЮИУЗЙЪВЫДПЧГТРУЧАШКВХЮРКМЬЖПНЪПГАОЦЪМЩ
ЮХОНХППЦИРМЧСЯЬПЙЧАЭБЙФБРКПСЙМЛЧЪИУПМЧЧШЛМФЖУКШЮОЪПМЧЧШЛМОУРМЧСЭ
ЩОЬЪЯУПМЧЧЬПЙЪЯНЕКХНРОГЫЙПЗЪЫНРИГЩЙЧКМЩГРЯЯСЭРОГШЬЦАХЬВЮЙФЪЯНЕНС
ИУМХРЕЮМЩСЖЗКВСНХППЦЙЙБХЫОЬЗЕЮМУЙВОЙЬМХЧЧТРМШМНХПШМЩЯМЮЙЧЙХТИЩЮЪ
РАЭЛИСФЭЩОПЙЦЛЙЯЬРДЛСЖЗКПЦЛЮЮТСДЬВУИЯРОЩФЖУБНСМЭЛПУМРЗЧСНШЛРЭОЧЙ
ВФНЩАЛЫЛРНЙЧНЧЛНСИШШРРГЫВСЮЙЫЮЪРЧХЕЧПГТОСЪДМНФЩАХЛТЧАСОСФДЬЛЙСНШ
ЕССМЦЕДЮГНЛЧЗИРЯВРЯЮПФШМНЛМПЙЭЙФЭЕЩЯФЩЙОЛЦЪЛЮЗУФКЩКХПЗЧШМЕАЩЮДЮЙ
ЧМХРОЧВУФКЩПХЧЕЮВУЪННВЮЧЮРКМЬЖЩБФЦЙШБТСБУПЙЪЭЬЗХШМЦРЮСКЫВЛЫЛУКЩИ
ГНЛМЩИЖВУСЛЖАХЭКЩБЦЪЯФПМПЙЦЛШОУУМХУЕЩКФЪЗЮМХЬЯХРЙЭАЧКМЩГЩЗОЧГЬЩЦ
ЬЙЭЕЙЩЦЧЕУЪАЧРЙЭАВЕФЪЭШЕСФЮЩЯХЬГЦЕХЩАШБМТИЩОЩФЭЩЖШЦЙШВЙСЛШЛШЮГЮБ
ЮФЙМЛШЮЙЫЛНЩЙЬППФНЩЙЪЫЙПЛИЩЙЧЯШСКЩИКЧГВПХНЖОЛЧУОЧКМСЙЬПЙЮЧЬМХРКЫ
ЕСЬЦЭЕМШКЮХМЦВХНМЫЕЩЖСШАШКХХМЭВФЪЩШВНСЖУКХЮЕЫШЩЪЗЪЛТСГЬМВЮЦНПГЭТ
ЬППСЙЫРНФИХЛФССОВФСЛЦЯВЭЖЮХЙОМРЙФСИУЯВЮЛРТФЯЖЪВЦСЖУДЩЬОМЗПФКЫЛПУ

2. Разложить на множители числа:

   (a) 405184747253239773431811450653

   (b) 57497821975980622710018207552315761774908425762593411558137 1

   (c) 1289029223310726277356411798781935715279539099054574291898709087816568424148866202620311139

   (d) 1884491193698050484999335660845225802816367357752793566740810443014020990611170762319158774246742062918357677699344556007

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 40461863496422569218171430867976954336990343497499168916539558938941129545031$
   - $e = 5$

   Сообщение:

   - $M = 19645825569974276772653374097975368902493929455432265488018991294864751787702$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 232190079044220395214002109456821755819$
   - $q = 250897792054495036993696828207429882937$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 166448438907712423134516328610923563168058394601472348211476206348886276812 32$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 217412174913181730241855943740745882399$
   - $e = 3$

   Зашифрованное сообщение:

   - $c = 155528087648302211055655240993963186521$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 211951355878968608483076283857322965871$
   - $g = 121674301615150352380780001861645261242$
   - $y = 78506788486832666964165788246667251152$

   Секретный ключ:

   - $x = 279755414740225230730436525103202 93$

   Сообщение:

   - $M = 95959323881680956395963103055165253768$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 10707983600244115971637803798227451547 7$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 209051172062882968799807408718554780189$
   - $g = 75023748767143813197237870588731216677$
   - $y = 19108727727684670621157520240631833979 3$

   Сообщение:

   - $M = 23829389473371622298560727498996637448$

   Подпись:

   - $a = 19818859912910186183947040731574610090 3$
   - $b = 86294350447015358965062441442444882809$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 821$
- $g = 471$
- $y = 543$

Сообщение:

- $M = 565$

Использовать следующий случайный параметр для создания подписи:

- $k = 229$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 16x - 2$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 48

1. (a) Расшифровать текст:

ЩЕЯСЦМЩЧФЛЧМПЮЙМЧПЯГТПЙШМЪФШЧОКЧИПТПУХЯМФФПСПЦТЩГМИМТГМЙМАПЦХШЪЛ
ЪФПЮМКХФМХШЩЙПТПЛЮЩХЪНШТЙИХКЪЮЩХЩМИНПЙХКХХЩЦЪШЩПТПЪОФТТПЩВШЪЛЧГЩ
УФФМЩФМЪОФТСЩХНМХФЩСХРССИЩЕЯСЩВПЦХОИВТЩХКХЦГФПЭЪСХЩХЧВРЙВУФПТЪЩМ
ИЩЪТЪЦФЦХШЩХТХУЛЙХЧМОРЮПРЩЪТЪЦЮПСШХЙШМУФХЙМЯМФГСПРХФИМШЩПМКХЩСПЧ
ШЦХЧХТФЦТПЙФШМИПОЪУПТШЙШУХУЛМТМШЬХЛШЩЙХЦЪКЮМЙШУХПУЙХНЩВУИВТХЧОПЩ
МТГФХЪЛХШЩХЙМЧПТШЮЩХЦЪКЮМЙПХФИВТПХЛФХПЩХНМТПЭХПЦХФТЩХКЛЦЧПЮПФЪЦХ
АЛВУФМХСОФФХРФМУХКФМЦХЛПЙПЩГШШЩЧФФХУЪШЭМЦТМФПЕХИШЩХЩМТГШЩЙЛМЩШСП
РЩЪТЪЦЦХЛЧМФФВРИЧХЛКМПОИЙТТУМФХЩЦМЩТПППЦГФПЭЯЩЙЯПРШЦХЦХШЩХТВУЛЙХЧ
УХШНЛТСЧМЦХШЩППЦХЩЧШТКХШЪЛЧШЩЙХУФМПОЙХТПЯГТПЦХСЪЯЩГШЦЧХШПТШЙМТГП
ЮФМПОУМФФВРЙШЙХПЬЦЧПЙВЮСЬЛХУФПЮМКХФМЩЦХРЛЪЦХЯЧЕЛЮЩХФПИЪЛГЩМИМПОК
ХЩХЙТЕХШЩЙЯПШГХЛПФЦХКЧЪОПТШЙЧОУВЯТМФПЮЩХУФМИВТХЛМТЩГХШЩЙЩГШЙСЧМЦ
ХШЩПЦХЛЙТШЩФХРОТХЛМЕПТПШТМЛХЙЩГОМКХЯРСХЕИВТХФМЦЧПТПЮФХХЫПЭМЧЪЛХТ
КЩЧМИХЙТЮЩХИВЙПТШЩЪЛКЛМШТЪНИУХУХКТМАМИВЩГЦХТМОФХЩМЮМШЩЙЪЙФШЩХАПЬ
ОЩЧЪЛФПЩМТГФВЬХИШЩХЩМТГШЩЙЬФХТЕИХЙГШПТГФХШХЙМЩХЙТУФМХШЩЙЩГШЦЧПУЧ
ГППЙФХЙФМПИВЩГМРОАПЩФПСХУПЦХСЧХЙПЩМТМУЬХЩПЦЧМЛЙПЛМТШСХЧЪЕПФМШХУФ
МФФЪЕЦМЧМУМФЪЙХИШЩХЩМТГШЩЙЬФХЙШМНМФМУХКФМЩЧМЦМЩЩГЙХХИЧНХЦШФХШЩГМ
МЦХТХНМФПЧОУВЯТМФПУХПИВТПЦЧМЧЙФВЦЧПЬХЛХУХЛФХКХПОСОСХЙСХЩХЧВРЦЧПИ
МНТШХИБЙТМФПМУЮЩХЛМЙМТПСПРКХШЪЛЧГЩЧМИЪМЩЩМИСШМИМКЛМНМХФШЦЧХШПТКХ
ЩХЙШГЦХЙПФХЙЩГШЙСХУМФЛФЩШСХУХЩЙМЮТСОСЦХШТМХИМЛИЩЕЯСФЯХЩЦЧЙПТШЙИФ
ЕЩМЦМЧГХЩЛВЬМЩФЪЙЯМИТКХЧХЛПМЦХЙШМУЪЙПЛФХЮЩХЦМЧШХФОФЩФОХИМЛХУШСЪЯ
ЩГПОЙХТПТЛЙЪЬНЧМФВЬЦХЧХШЩЦЧПЩШЩСНЧСХЮЩХПЩЧШСЪЧХЮСПФФМЙВЩМЧЦМТХЩЛ
ТЙМФПСЫХУСМИПСИМЙЪЛФШПТЪЬХТХЛФХРЙХЛХРХЩСЮТШФМЮМКХШСОЩГЙШМЦЧ

(b) Расшифровать текст:

ЕЬГШМКЩЩЫЖДХГЖЩТЦТЕЬКУЭШПКГЯЛЪЖЬУХШРЫЩЫФТЦЫШЦГЮЯЫТНЦВЖЧОУЮТЦКСЯЦ
ЫФЗЩХТУЩЯВОКЬХТЧКХЮТЯСЬУТОКЪЯЦЭЕЩУЧЕЛЬТДМКЩЮЦБФЬЯЧЫЗЧИЫЩРРЦОПФЫВ
ФНРЯДОЪАЫЙЛЬАЖЫЩЪКПУТХРЫУШХЗЫАЪТМХГЖЫЗЧИЫХКРВЩШДУВТЬЮЩЦОШИТГЖЫУР
ЦЬЭГЬЧТЧЗЭБШЬКРЩХЫУРЦХЖКЕАШЫНУХШМНЪЯПЦХЭБТЦЗЮДТФТБЬЖЧЭУАШМЗЩЩЧЫУ
АЯЪРЗЯГМШОЪМЩПТУТЪХКЯНБПТУШШМТСЩМЫФБАТХКРВХШГЬХЭМРРВПЯКХТЯНРЮЦХТ
РСЮТВХЪЩФЪКШЩЪСЖРЬТЫЮРЦСОЗЫДХТШУУЫЬТУГТХОЫЯРПУАУШЧТЬХЭЧРЫЩФЬРРГП
ЦПЬГПЧУЫЦСЦЗАЩХТПУДСЧНРЯЦЧЗЬБПЧГББНЫМЬФШШЦЦЗПЪПЯАЪТДУЬТЩТЪЯФТЙПЦ
ЫЬРРЙПУПБФХЭСУБПФТУВЬФХРЯЪШФЯГШХРЫЦЫФРЩНФШДЦЮЧЕЧПЯБПМЦХМПСБЙФТДЬ
ГТОДЬБПАУШШХШЖЦЮТСОБЧТФРРВПУЩЯЯЛМУТЯХШИЦЭШЧДЬЙПХДЦШЛЭДХФХЧХЩЮЫМЗ
ЩНТБУАБТФМЮЦЫЬКЩВБТФЭБШЫЗПЭШХКАУЭОРФЩОХУТЯХНРЫЫШЧЗДЭЭРКШУШЪРАЩХЫ
КЯЫСХОЫЦЫЬХЭЪЧВГАПВФДУЬПХДЭДЫЬКАНШЮКДЦЪМРЖЦХМКХТЭТНЦУШОДЬБПАМШЮС
ЕДЩЩППОБЧТФКЬЮШЫДУКПЧГЙЬОМХЪВХЖПЙЭТЫДУИЦТУАЦЧЕРШЬПЧЭПМХТЙЬЬШЬРМТ

ЭЦЕЬПМЩТЬИПЦНРЫТЫФЬЬЪЭМЬЭШУПЦЫЧМЗЮЦМШЩШЦЩШНЬГПЧШУЮНМРХХПЭЧРГМЭЕЩ
ДТВКЮЯФТЛЖЦЫЬРШДЫЬДЩЦЧЧЭЧФШЪЬШЭТМУУТЕХРШЫМШГЙЫЧШДУЮЧШЛЦШЛПСБФБПД
ЯЩОПНЭЯОШГЮШЦТДШБЫЧРЪЫЮЬПУУМЕУЬЫШУЪЭЫПТДФЮШЩРТТШБУКЯФШНЬЮПНРЯГШХ
РЫЦЫФРЩНФШКХФХМПЙЖПНРАЯМЪКЗЦУЫДЦХШЦСЮЩЬМРЮЮШНРЭЯОШГЬВЬЪУАЩМТЖЫЯЛ
ЕНЬИЬШДУВЬЖРЭБТЛЭАЩТШЦЦЗПЪКХЯЪППДЪНСЮЯЛЭЖЦЬМЛХЫГШМЫЦЫЯЫКЩНЧШЗЩП
ЛШСЙГЫЬДЬЩБЬРЬЮТЩТЦФШЬРРЩХТУКУЫЬТУГТЬЮЪЦЧЫФЬБРПУАУШЦСБФБПДБШЧХОУ
ЮЫЩЗЮУШНРРШНХЖБАШОЖУЬЖЧДФЮШЫФКЦНШДТБЭНКЯИПСНРЙПЛНСЯЪШЖЦЦЫФЙЩЯЧЦП
УВРТДЬВЬТАШЫЩШИЦУПВЮХИПЦФУТЛШЕЭБТЧЗЯЯЬМЗЕЬБЬРУЖХЩРЯУШПОБХПХХЦИЬШ
НМХТПЕЬЭПЧРЯГЧШДЦЬТЩРШЫШЦХТЦХЭУЭБШЫКЩЯЧЦЗЫЮПСПЩИЬШРАУПБФКАЭНЩУУЩ
ШНЬФБЬРЫЦЯШЩБЯЛДУЫГЖЫСЮЩЫМКТЦЬПНГЯЛЪФЦЬЫФУРЯТЦФЬУЪТЫЪЩМПНУЬТЦДЙХ
ЬТДЯЦЩШУЩДВХКЯНФЪРЪЦОМ

2. Разложить на множители числа:

   (a) 4942001331732203802078415253 69

   (b) 1094318485040658914306696992498571627155375485191887731952387

   (c) 1286923566560511366121607174029594117691396675628386295758727034415435727499521241174038703

   (d) 1415270579753939799126791441340983782815717416336729448204988232312389556095005429097503498737560418384356429876834111151

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 10166218528739194482347947240565353953884559891783008725179219773023783407498 1$
   - $e = 5$

   Сообщение:

   - $M = 31234998774552363773776938935148359544975077476535211834526103513128881014747$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 30625937788311447057330733281749917142 9$
   - $q = 33887746680926637354205736288956931305 3$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 995507677851475418137598120988776920663600436513573189322629641408656617662 1$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 21854957466525273042828392418520195087 3$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 34626632657670173897064192130773157881$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 32701298642970937894312845952621047214 7$
   - $g = 16546453751270090700787195622851069092 2$
   - $y = 15773026597427277997350604364705172472 8$

   Секретный ключ:

   - $x = 14414874575328802254274047083732191687 8$

   Сообщение:

   - $M = 31049917326818116352321998862562793086 7$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 24851262386580171434571428713791944441$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 23926535092068076742628070106243451345 7$
- $g = 98954268842427561772307542483913719 97$
- $y = 68384543013043898962332234890878793660$

Сообщение:

- $M = 19421418145913649247972868713221419 3999$

Подпись:

- $a = 38898753421549410976456916456540606105$
- $b = 23460263763304865335776418818725269 4545$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 929$
- $g = 475$
- $y = 909$

Сообщение:

- $M = 242$

Использовать следующий случайный параметр для создания подписи:

- $k = 525$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 11x - 10$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 49

1. (a) Расшифровать текст:

ФРЛУПФРЧШРПХЖЩДЧНШНЧЫЛУЩПЙНМХЦЛЦФЦНЛЦММДТЫЦХЭЦЪНУЙГУЦЧЫЩЪРЪДЩЦЧЪ
ДКЦЙВЩХНХРХЦЧЫЛЯНКНЛЦЧШНШКУТТЪГЩФНУУНПЪДТЦФХНЩЪТРФРЧЫЩЪТФРКЩТШРЯ
УЦХКГЭКЪЙЫФЛЫРПШЫТЩНТШНЪШРЙШЦЩРКННКУРЮЦЩКНУДРЯЫЛУЫЧГСЩЪШРТРЭЦЙЦЙ
ШУРЕТЙНММЪГМЦУОНХЩЪШГСЭШГЯКНЯХЦЙЦЛФЦУРЪДПФНХМПФЦРЭШНЙЪПЪЦЯЪЦЪГРЩ
ЙШРХЦФЪЦЩКЦРФХНКРЩРЪНПМНЩДКФНЩЪНЩФЦРФРЦЩУЫАХРТФРПСЯРСЪЫУЫЧЪНМФПС
ЯРСЪЫУЫЧМПХНАДУРЪГЯЪЦЩЪНЙОРКЦЛЦТЦОЫКНУЖЩЦМШЪДХЪЫУЫЧГТТРПКЦУРАДЦЪ
КНЯУЩКНУДРЯЯНУЦКНТЧЦМХНКЦУДХГСРПЙШЩТЦНМЦЙШЦМЦУОНХЦЪКНЯЪДЧЫЛЯНКЙГ
УКРМХЦКЧШРЧМТНКНУРТЦМЫАРЦХЦЪКЦШЦЪРУЩРЦЪВНЭУХНЩТПКЙЦУННХРЩУЦКАКЙШ
РХРЩЪШАРХГЧЦЩУНМЦКУРПХРФАСТКГЩЪЫЧРУРПТШНЧЦЩЪРКЧЦШМТНХШЦМЧЦАНУЧШЦ
КЦОЪДЧЫЛЯНКЦЩЪУЩХЧУЦБМРЦМРХЩЩКНУДРЯНФММДТФЦСМНШОУКШЫТЭЩКЦСШННЩЪШ
РШЩЩФЪШРКУНЛЦЩКРМЦФЛУЫЙЦТЦЛЦЩЦОУНХРКРМФЦНМЦЙШЦНЩЦЛУЩРНЩЧЫЛЯНКГФЦ
ХМЫФУЫЧЦЪШНЙРЪДЦХЦНКЧЦУДПЫХЦФЫМШЦНХФНШНХРННФЫХНЫМУЦЩДЩЪУЙГУЦНЛЦЙ
ШХРЪДПХНЫФНЩЪХЦНЫЩНШМРНРХНФЦЛЫМНШОЪДЩЦЪЩФНЭЩФНСЩЩЫМШДЦЪКНЯУЩКНУД
РЯЩФНСЩТТЧШРМНЪЩХФЩГПХЦКПКЦМРЪДЩКЩНФЭЦПСЩЪКЦФЪТЧЦЩФЦЪШРФЩФНАХЦУР
ЙЫМНЪЩЧНАРУКМЦФЩКБНХХРТЫКРМНЪДЩЩФШДНСРКХЦКХЦСЧЦЧМДКЩЪШНЪРУФНХЩЧН
ЯУДХГФРПКНЩЪРНФХЦЯДЖЫФШДРРКХЦКХГЦЪТШГУЩДЩРУДХЛЦШЯТЦХУНОУЙНПЧФЪРР
КЙШНМЫЧЦЧМДККНУФНХКННТЦФХЪЫЪРЭЦЧЦМЦАНУТННТШЦКЪРЧНШНФНХКННУРЮНЧЦШ
ПРУФНХЙЦУДХФНХХНЫПХУМЦУЛЦЩЪЦУЧНШНМХНЖХНЩУЫАХРЦЪЮЛНШЩРФХРМЦЙШЦСОН
ХГНЛЦТЦЪЦШГНТОНЪЩФНХЫЪНАУРФШЯХГНФГЩУРКЦУХЦКУРФНХЩЦЩЪЦХРНЙНМХЦСЙН
ППБРЪХЦСЩРШЦЪГЦЩЪКУНХХЦСЧЦЩШНМРПУЦЙХГЭФЪНОХРТЦКЩЦЙЩЪКНХХЦНФЦНЙНЩ
ЩРУРНЫЩЪШАУРФНХАКЙШРХАКЙШРХЧЫБНКЩНЛЦЪНШПУФЦНКЦЦЙШОНХРНЦЙУНЯНХХГС
КУЩЪРЖЦЪЩФЦПКХЮЧШНМКЦМРЪНУДЩЪКЫКТШНЧЦЩЪРЛМНЦЩЪКУЩДХНЩЯЩЪХ

(b) Расшифровать текст:

ФГЮЛКСЦИЩАФЧДШПЩТДПДШУКТЫЦШЭФШТШЙЭЫШАКТАЛЫЗЛХШНИЛГШУБЭЫУДЛЩЦЭЦЮХ
БЧЭКШГЛЬЙТШУВПКЫИЬБУЫЛЭДУЫЭЦЯФАЛЯОИШЭЬКЗЯБШИФЮЭЬДХБЙБПНДВЫВКОПУН
ИБОБГТОЮЬБУЫШГМОАНГЙЩЮЩЮЧСЖДАБЧАДВЮЛЮВЩУКГЛЭЗРКСВЙФФСДУРШРЩЭОЕРЬ
БШШСАКЙЮКЫКТЖНЩИУШТДЛЩЕОУАЦЖЙДЮОЧЛЬАЛГЛУПЮЭЩЮЖЦЖШЯИЗШЦЦЯЩЫРВУЧЕФ
ЫКСБТЩНРБСЯЖФЮВЮБПЫЭЦМЛЪЭЦОИШЦГШЭДИЛБЫЮОЭЧИФЛЬКЙБЦВЖЩСРББХБЧГШЙЮ
ИВДЦБШЫЖЩАЮЦЕЩФСЯЙРЫУЩЮЛГЫДФРЫУЦОУЫФГМФДШЯУЛЭРЫПУЛЛЪПРАЙЩЙДЛРЩЙО
БШЗЙЛЕЩЮДТЕЛБДЧАЦХДШПШЯБЛАЛЫКТЖЗЬЯФДСЯЮОЕВГКЛШУЦЖФЯЩВЮКШЗЮЛЛДУЫД
ЗЫШЫЛФЧАЦССЭРБЧСПЬДЖФЯЛЮАУЕЧЫКЙБКЯИУГФХПНАСЫКСБРЯЗВКОЫЛЩЦЭЦЮОЕФЬ
ЛФСЗЦВСЪУЭДЮХЗБДУХЧГМЛЕОЬНТБНУЙЬАРБЧСПЬЦКУФБЬККШШЫГРБТЩКШГЧГДСДЛ
ТБЗБЦЯАЩЫНЭБУАОЫЛФЯФФЛЩЦЭЦЮЩХБЬБНЕВЩГРЫЗЩОРЫИАККЮБЖЮБГМЦЙОИОШЦИЮ
ЧУКДГКЯНШПОДНЛГКЩБЩХОХИЛАФЮНТЖШЩЗЧАФУНРБЦЦКХГИЩЗЧВЦЯОУЖСЭЙЛГЩЫПЙ
БИЯМОЕБЮФКХУЯЭБЕРЯОИБЦЯООЮЧЯОУШЙЯДУЫЭЦЯФАЛЯОИШЭЬНЛГКЗБТБЛШЙБЮФЫК
ЙЧФИПШЫСЩНВЯБУАИАФШЙРБТЯЕРБТЮОЛЦКЦЙЧЕЛЮБИЫЧЦЗЛМЛХДХЮФЭЛФЭФЪЙФЦФЫ
КТШУХЙШЭРАБЭЮВЮЩХЫШЕДХГФЙБКЛЛЭПИГЛЭБУЫХДЯЭШИВБСАШЯИКЫИЮБУЭФГКЦБТ
ТЧИЮФХМЛЯСЩЮУЭЩШИОКЩВЧХЮЛЮЙБЬИЯМЭАОЦИЧХФЦЕЧЖХБПЙЫЮУЭЦЫУВИХБКЮБЧШ
ТДЮФЧРЩЛЩЦЭЦЮИОХЩЗЦСТЫПОДРШЗЛЯЩДЖНХУЭБУВФАКШКЩЪДЛЦФТЗЙБЦЯАОШЮУЭЦ
ЫУАККБЮЦЗРБТЮБЧДИЯДТВФХЙФДФЭЙФХШЯМОКУЯКШАЛФКФЕИЯМФЕОЬНФАРШЗЧДТЮБ
ЧХФЪЛЦЫФТЧРАФУБУАФЪНИБЛЪНТШШЬДИБЧГДФАРЯЙЛКУЯАФЦКЬНЭЕФАПЙКЛУЭБЮОЭ
ЙЛЧФУКСШУЯЙШГЩВДСВЛББКАОЭЙТШУАКЙЮКМЮСДУЦАФХЛБУОХФВООСХДЯЭШИЯНИШК
ЯИОЮЧЯНФДШЯЙОЫРББХБЧГДФДСДСЫВЦЯ

2. Разложить на множители числа:

(a) 528093860830550394579056441501

(b) 983059209638732861695659454601582421858204149513901615772747

(c) 172919135806917245237198566236177859504338794479564873938648009230472065717326058796528128 9

(d) 114966985077690152844315537919297730485295817429708236721818794158918441618889502193829182784375808291243267916576749335 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 353710342294869681296315855762080088191622942963316199535782537034077592279 87$
- $e = 257$

Сообщение:

- $M = 328166208964418217151510422313316714569822248480116392781354591471579217068 99$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 264652380801436742362151924118589117267$
- $q = 200301043844292946162406633658758820833$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 102517405625926245299120560925454504263876550573610776652132751300486936886 16$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 115042391633966469989350986351280906849$
- $e = 3$

Зашифрованное сообщение:

- $c = 467052623005306699854562677418979771 92$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 335349197329150237309650424270400562629$

- $g = 25349608821163163908347302841783212585 5$
- $y = 24813717347869208999661956803592700 4805$

Секретный ключ:

- $x = 25956308983771602008785751679438231 3053$

Сообщение:

- $M = 12647701187209179658560695709349756 7683$

Использовать следующий случайный параметр для создания подписи:

- $k = 48450669918186251502727949366037519503$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 22312698858705652684605597780109182791 3$
- $g = 11991862060533669599202985270375913163 0$
- $y = 42707231651958854675349082154733819578$

Сообщение:

- $M = 89277455345217992747072488851244810543$

Подпись:

- $a = 13150426221713177349798994747287422718 4$
- $b = 10767572555612106066963224331127375107 5$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 953$
- $g = 608$
- $y = 601$

Сообщение:

- $M = 370$

Использовать следующий случайный параметр для создания подписи:

- $k = 405$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 3$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 50

1. (a) Расшифровать текст:

МПЬСЕАЬПЛАЬЭЦЯКЪЬШШЫЦПБТКТЬРЯТЬЖЩЬЪШЯЦЪЙЕЬПУЗЩРЪУСЬТЬЯАРЦАКЭЩЖЯЩ
ЙЖЩАШФУЬАЪШЯЦЪЙЕЕАЬРЯЬЫЕЯАЬЦХТЩЦРЦТЦАЫРЙЩХШГЦЕАЬРЙЯЬРЯУЪЯУПЫУПУЮ
УФУАУЦЫУТБЪУАУЬАУГШЬАЬЮЙУХРЯЯЬЯЩУХЪЦПЬСЪЬЩАТЬЩСЬПЙЩПЬЩКЫШЬСТРЙХТ
ЬЮЬРУЩЩУШЯУЧЦРЫЬРЦЕШЬАЬЮЙЧШЬЪЫТБУАБЫЯЫЪУЯАУЭЬШЬЧЫЬСЬПАМЖШЦЭЮЦЫБТ
ЦЩЬАДСУЮЯЦЪРЙТАКЪУЫУЪБХЯАЮЗРЭБСЕУРЙЪФЦРБРЫЖУЪТЬЪУЭЬТШЮБЩЬЪЩУШЯУЧ
ЦРЫЬРЦЕЭЮЦЫБФТУАЪУЫРЙТАЦХЫУСЬХЪБФЬЫСЬРЬЮЦАЕАЬЯЭЯЪЫУФЦХЫКЭЬАЬЪБЕА
ЬЭЮЦШЮЙЩЬПЪЫШБЩЦЫЙЭЪВЦЩЬРЫЙШЬАЬЮЯШХЩХЩЬТУЪПБТАЬПЙУУЭЩУЪЫЫЦДЪЫУЩУ
СЕУПЙЩЬПЙБЪУЮУАКЫУФУЩЦЯТУЩАКЯФУЫЬМАШЬСЬЕУЩЬРУШШШЬРЩУШЯУЧЦРЫЬРЦЕЬ
ЫЬПГЬТЦАЯЯЬЪЫЬМЬЕУЫКФУЯАЬШЬЦСЮЬХЦАЯШЬЩЦЫУЬТБЪМЯКЦЫУЯЬСЩЖБЯКАЬЭЮЦ
РУХУАЪУЫРЩСУЮКШХЩЬТУМЦЯРЪЦТУАЬФУПБТУАЕАЬЯЩЦХРУАЬЧГЮЩЬРЬЧЭЮЬЯЦЩЩУ
ШЯУЦРЫЬРЦЕТАКЪЫУЭЬТБЪАКЬЫЯЬСЩЯЦЩЯФТАКУЗУАЮЦТЫШЬЩЦЕУЮУХАЮЦТЫХЫУСЬ
ЫУРЙТБАШБФЫЦШШЬЧЭЬЗТЙЫУПБТУАПАМЖШЭУАЮЫТЮУЦЕРЙЬТЦЫБЪУЫЭЬШЮЬРЦАУЩК
ХЯАБЭЦАУЯКХЪУЫПУТЫБМБЭЮЬЯЦАУСУЫУЮЩЦРЯУГШЬЪЫТЦЮЬРЭЮЦЯЩАКШЫЪЭЬЯШЬЮ
УУЯЦШБЮЯБТЭЮЦУХФЧАУЯЪЦУЯЩЦЪЬФУАУЬЯАМЯКРЪЭЬШЬЮЫПУТЫЯЦЮЬАЬЮКЪЦЮЬЫЬ
РЭЮЬЕЦАРЛАЬЭЦЯКЪЬЕБАКЯБЪЫУЯЬЖУЩЭБЯАЦЩЯРСЬЮЬТПУХЪЦЩЬЯУЮТЦЭЮЦЖЭЬЮЦ

РПУТЫЬСЬЪЬУСЬШЬЫТЬЮЬСЬМЭЮЦТБЪЙРЩЦАЬЦТЮБСЬУТЩЦХПРЩУЫЦПУТЫЬЧТУРБЖШ
ЦЦЫЦЕУСЬЫУЪЬСРЙТБЪАКЭЮЦЯШШРРСЬЮЬТЬАЭЮРЦЩЯЭЮЪЬШСУЫУЮЩБЦЬЭЮЬЪУАКМШ
ЫУЪБРПУФЩСУЫУЮЩГЬТЦЩРХТЦРЭУЮУТЭЬШЬЪЫАУШБЮЯРЬМЭУЫШЬРБМАЮБПШББРЦТЪ
УЫЬЫЬЯАЫЬРЦЩЯРУЮЬАЫЬРЦТЪЬЧЭЬЮХЦЩУСЬЬЫХПЬАЩЦРЬЬЯРУТЬЪЦЩЯЬЭЮЦЕЦЫУЪ
ЬУСЬЭЬЯЭУЖЫЬСЬЭЮЦГЬТРЖУЭЮУРЬЯГЬТЦАУЩКЯАРЬЯШХЩУЪБЭЮЦПУСМШРЪШШШЬАД
БЮЬТЫЬЪБЮТЦПЬСЫУЬАШФЦАУЪЫУРЪЬУЧЭЮЬЯКПУТУЩЬЦТУАЬЯЕЯАЦЦРЯУЧЪЬУЧФЦХ
ЫЦЕАЬАШЬУПАМЖШЯЭЮЬЯЦЩЦХБЪЩУЫЫЙЧЯАЮЦШЕАЬЪЬСБТЩАУПЯТУЩАКСЬР

(b) Расшифровать текст:
ЮИМСОЮНРЙЯЫОКФПИШКЛОЭШКХЛЗЙСШМОЫРФГВДИЪЕГИБЙЦЫЧРКМЖДЙПГДИЗМХБШЪУ
ЖЗИХЩМБТПХГЩДЗВПДАУИЙЩДХХВЮЫФЧЖАЭРЙЦЫЧРКМЖДЙПГДИЗМПИЮЗХПИЖУКГЫЧР
КМЖДЙПГЕЖНСЕГДФЧЖШЫЦЩЖАЫИХАСЗУСМЧБИХОДЪНЕАОЫЖТБДЖУЛЖЫЧХХПЮБЦФИЖС
РГФДАХЪЙТГАМЛЫЪШУЙЮВКФСЪЫХНЖШИБПНЖВУЙЯЫЬРЙИДВТЩСЩЪКЮГБДЗМИОЫЦЩЪЩ
ЙЦЧПАЮЪХТЮМКЧМШЮИЧЙЮШЖФИВЮУЧКЫИРСИДШУИЩБДСХГЮЭШУЙЫГНМИДЩЙЙЕЩБТЪА
ГГКККМЙЭТТЖШГНЙЛДШНЮЕЙЖНФЛЫАУКВДЧАКОШОККМВЫТЙПЮВЖПОЗАУУРЖАЧПОЫШУО
КДЬТХЙЮШЦСОЮНРПАГЮЗФЩНИАТЖЧЧЖЦГИЖТЛОЫЮЬСИЮВНШСЪТЖУЖДИПЪВИСМЛМЖДЗ
ХЯЖИТМУДНКЯЪБЮФХПИШНЩЪАЖЧХХАЙЖТБДЪХМЛЕЖНСДЮАРЪХОЫУЩАЫЗЧПКГЫПЙОИЮ
ХЪИАЙГЩГЧЫПЙОИЮХЪМЗИЗРПЙВКФЛЫВУКСГЫУЛЖГГШЦМЪШОШЬЪЮЧХАЖЮЮФГЗИУЙОЮ
ПКУПЪВУЕПЪВУЕБЪЫЛМРСЫКЦМЪМКЦЖБУИМЯЖИФЧЖЗЮЪШЙДШЪОСЖЮТОПШЮЦЩГБИПЙЩ
ЖЭНЩГБТТХХИДЗШГЭЛУЬМИБНШМШЫХЯГГГУШКЙИНТПГЙФЧМЪДРНЙЭЙХПЛИАНИЩИТЖЪ
ВЫИЧМЯЫАЗЧРЮЖЛТЪВСЖВНДЕНЧМШБНЦМЗИХПЛГДСЪБЫЯСТМЯЪЬЩМЬЗГЛЛЫШКЛСИАШ
УСОАШЩМЕЙИЮГШЮРПМГЙФЧКЮИЦШИЭЙБМЗНИУИМГГКИМБЗБИОЮГЙМНЖЫПЧПГСОФЖНЫ
СФГДЧНЛЖИЪЪХОДОКФЪАДКМАОЫГЮРДИАДРДЗПОЙЭЙХПЛЙАПССВЙЭСНЙЩЬМАУИУЛМН
ТФХИДЯТХБДАФПРГВНЧМГДЗЙЩШЫММГЮЭФТГГЮЧМНЫЖБЦОДШУНЬЪДЙМОЫШТПЯИФЭСЖ
ГДОКВЫЮУШРШБГМГААЧСЫИДУЩГЧЫСФГЗЫОЮПЪДПТВСШРПНДВНТСЯНЧХДУИУОЛНЮЧЦ
МЗБКЙПЫЖЦШИЬЙЧМНЫЖБЧВЮЧУКСЗЕУСМЯЧКЛЛЙФЙМАЙОПЪИДИУЧСФЩШШОСИЗХЖЕЫХ
МНЙЩРПЕЙЖНФРДИЬШОЗЕУЧВЮБЦХЛЗВЗВЦЫБТЪЙЮМШПЕШЮТЩЪЗЕКЧГЪВХГГЯЮЗФМШГ
УРАГЫЗХЙТГУУЛЫЪУЧЕЙВКФЖЮЮФЧЖАЭРЙУВЮЦЩОЙДЧЙГЗИНМЗБЙЬЯСФАЗЧРЮЖШЙБД
ЖУЛГДЗЧТПГДЬМАИТШФГЩДСВМИЙЛПЛБЮНСМЩЪУШРБЮЦГАЪШУМКЖЗЦСЕБЫСЪПШДНЦМ
ЛДЛЛГГЮМЪОЮГЦТСОБСМЛЗЧУТЪОЮСЙЛЮВТПГВАУКВАДТЮЖБ

2. Разложить на множители числа:

(a) 8339749733985792490203852491 29

(b) 899535648662713561701726834971953822243475734150052074244129

(c) 1130039631842792853164186915023449147004723401211486458963721821461030243480858104841870341

(d) 157042586147419966414217558036616741862225913653465176125499895456033726080306318649693494625398803038871400451981651663 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 958802253788552921340767494761017336138046050361073407438823877120909800471 61$
   - $e = 5$

   Сообщение:
   - $M = 592001377995492563011285113348639104205885626441851011625974670855057938868 53$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 3017531728066338785072976077244061478 83$
   - $q = 2019056518299325929298547999737251594 37$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 7461223889189042761618603873840055780449640442958923689641729859805303663671$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 22412692075798536409653439193380717752 7$
- $e = 5$

Зашифрованное сообщение:

- $c = 434886487931572418567864081638905135 48$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 17068546312958847068707103930132254852 1$
   - $g = 13304636550443145189882373986322493799 7$
   - $y = 93755182126882107213365082510872395358$

   Секретный ключ:
   - $x = 16274281927283637511363188590031267088 3$

   Сообщение:
   - $M = 23332979122816462607850693894887372992$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 66981015243534510063044080813522117551$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 17849912479829881528428976062284765473 3$
   - $g = 32075942251151201207445189249617952327$
   - $y = 12666367216489048150288090386064445666 8$

   Сообщение:
   - $M = 45126449182304432133092177213463106 74$

   Подпись:
   - $a = 11205398861192396818585163656196286465 1$
   - $b = 11662462172903227576812749868594730257 4$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 1013$
   - $g = 975$
   - $y = 341$

   Сообщение:
   - $M = 486$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 17$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 5x - 9$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 51

1. (a) Расшифровать текст:

АГЖЗСЧЬАЖСЯГВЪМВГГЗЧЪМАКАГДИНЭШЕЪНЪВЭТЗЕИЯЗИЗГВЖЫАЖЧГЮЯГЖЗАЭЧРЮЯ
ИАЯЭЬЖИМЕИЯЧГЗЯЕРАЯГЖБЗИУЕИЯИЭТЗЕИЯДГЧЭВВЧДЕГАЭЗГЮКЕЭЖЗЭВЖЯГЮЯЕГ
ЧЭВГШИЦЭАЖИДЕГЗЭЧВЭЯВЪШГЖЗВЧГАСВГБДЪЕЪДИЗСЭЩЧЗЪБВГБАЪЖИВЪЩГБЖЭЩЬ
ДЪМСУЯЭЖЗЪВЪБЭГЦИКГБВЪЦЦСЭБВШГЧГЕГБЖЗЕЭЯГЗЧГЕГЗЭАЖЭДЕГЧГЕМАЖАГЧЕ
ЧВРЪВГЬЩЕЭМЗГЗРЗБНЪДМЬНСЖЗЕРЮКЕРМЬЯЕЭМАКАГДИНЗЪЦЪЩБЕЧВРЪВГЬЩЕЭДГ
ШГЩЭДЕЭЩЪЗЭЗЧГЪЧЕЪБЦГШЩЖЗЭЗРОЭДЛГЧДГВУКЪНСДГЯБЪЖЗСЖБГЗЕЭМЗГЦЗЪЦЪ

ЦГЕГЩЭНЯЭВЪЧРЕЧАШГЖДГЩЪВЕАРДЕГЧГЬШАЖЭАЧЫВГДИШМЪЧДГАВЧБЖЖГЕЭЗСЖВЪ
ЦЪЩЪЖАЭЦЭЧЖЪГЕЪВЦИЕШЖЯЭЪЖГЦЯЭЩЕРШАЭВГШБЭДГЩГЩВГЮДЪЕЪЯАЩЭВГЮЦЪЩЪЖ
АЭВНЭЯГЦЪАЭБЪЫЖГЦГУДЪЕЪШЕРЬИЗЖВИДГБЭЕЭЗЪЖСКАГДИНЭЦЪАГЦГЕГЩГЧВЪЖЯ
ЬАЭВЭЖАГЧЭБЕМВГЖБГЗЕЪАЭЩЕИШВЩЕИШИЧЭЩЪАВЪГЦКГЩЭБГЖЗСДЪЕЪБЪВЭЗСЕЬШ
ГЧГЕЯГЗГЕРЮБГШЯГВМЭЗСЖЩАБЪВГМЪВСВЪЧРШГЩВРБГЦЕЬГБЭГЦЕЗЖСЯДИШМЪЧИЖ
ЯЬАЪБИЖЧЪЖЪАРБЧЭЩГБКЦРАГЭЬЦРАЦАШГЩЕЭЗСЗЪЦЬАГНЩСЭЬЗИАИДЦЪЬЗЪЦВЪЩГ
ЦЕАЖЦРЩГШГЕГЩЭЬБЪЕЬЦРВЩГЕГШЪИАГЧЯБГИЩАЖСДИШМЪЧЕЬЧЪЖЪАЭАЖЩГАШДАЗЪ
ЫГБЯЕЖЪВЖЯЬАГВБЭШЭДЕЭОИЕЭЧЖСЕЖЖЯЫЭЯБВЪЗЪДЪЕСЯЯГЪЗЪЦЪЩЪАГЩГЗГЮЩЪЧ
ИНЯЭЯГЗГЕИУНЧЦЕЭВГЦЭЫЪЗИЫВЪЬЬВГЦАЭЖЪЕЩЛИБГАГЩЪЛЯГБИГВВЪЧЪЖЗБГГЗЧ
ЪМАДИШМЪЧИЧЭЩЦАШГДЕЭЗВИУДЪЕЪБЪВИДГШГЩРЭВЪВКГЩВИЫЩРЖЯЕРЧЗСЭЖЗЭВИЗ
ЧГВЪЧЪЖЗЬЯЕЭМАДИШМЪЧМЗГЫЗРДЕЪЫЩЪВЪЖЯЬАЩБРЗЪЦЫЪВЭБЭВЖЧЩСЦЪЗЧГЪЮДГ
ДЭЕИЪБДГЗГБГЦЕОЖСЯЦЪАГЦГЕГЩГЧИЖАИНЮЙЪАСЩБЕНАБРЖЪШГЦАШГЕГЩЭЪБЖЗЕР
ЪДЕЭЗЪАЭЖЩЪБЯЩДГИЫЭВЪБИЗЕГЧЪМЪЕБИЩЕЪВЪЪЬЧЗЕДГЖБГЗЕЭБМЗГЖВЭБЖЩЪАЬ
БЕЩЦРАГЗЯЬЗСЖГЗДЕЪЩАШЪБГЮМЬЖЗЭВГЩЪАЗСЦРАГВЪМЪШГЩЧЪБГАГЩРЪЯЬМЯЭЩГ
МЪЕЭКГЬЭВЭЬЦРВЯЕРАЭЖЗГАЦЪАГЮЖЯЗЪЕЗСУДЕЭВЪЖАЭКАЪЦИКЭЭВЪЖЯГАСЯГНЗГ
ЙГЧЖЧЭВГБЭДЭЧГБЭ

(b) Расшифровать текст:
СШБДЪСВБЙЦХЬЖДЛШЧЛМЧЮЧБЙЧЙЦМПМЦАУПЛШДЮКЛТЯБЛЩМААКФПЮКБЧЩФМХОФЪБИ
ЦМБМДБТАЮЯЧТАЮПАЩАБНФПЯГЮЬМЧОКУХЮДНЪПБКОЩМУПБЫМЧЖКЫЙЧОПСУННЗЕЙБП
ОЫГЪИБОУЧВАЬКЯПНЦВЮДДРЙЧОИСОЭКАОМФДБОШЮПЪШЧЪЮБЪЩЪЙКАФЕЪНЦПЮДНЫЙЬ
ПЩЫЪШНЙХВГЗШЫСЮБЙШХВГДФЮДКГХТГДНШЪДЗНЪЪЦШДХХЪЙУСФФФДОСЩЗКЪГФЧНФЪ
КДЮЫГАОЮОЩНИКСШЯБЖЧЩАМКЗИЭЯКЪСЭКЙЦХГОДЗИНЗДЪФАЮЛЩМЦПЭОНЦБЙДЦВКОС
ЙЕИБЦЦВДЮСЛЧИКОКАНИЬАЧЙДМЙВАБТШЬДЕЧЫЪТБЩЦАОМОИАЮЗАЩАЭИОФБКНЫЙЪЗД
ЦХЙЙПЗШДЮЖЬШХЗЮЦВЮАКЦХГДООТЧИЯОФЧМЗЛМЭБЗУТЪЖЙЬЩОЮУОЧКЙБМХЩЗКНМГВ
ДЛХГОДЗХУМОСТГЖАЛМВИКППЦЛКЛТЧЙДЪЙАБЯЧХУЮДЦПДБЗАМВБГЦМГЖКФГЬКИСФЕ
ОГМЧЧИБФПИБЛСЛФБМСХДЮКЩПЭДНЕПФКФОТКЮЭЩПЯДГЬУЪЗНОКАЛБЩМЮБЙОХЯЭЧФЪ
ШНЙЧЬЕАДКТЧАБЦЙАЗКЪМХКЙОЛФЙКАМВЙЧОСЬНИЧТОНКЛМВФБЦФАЛКЪМЦБЗСЛЭДЙЦ
ИАМКНИНЗЮЪСЭКЖЧЮЧЙКЦЦАЮОЧЧЪЗККЙЪЙБЦПГЮКСШЭЭЧХФАНИОТНИЯЧТАНКХЦАБЯ
ЧШЭКЮХХДМВОФУЧЗЧЩБПЯАМФЮКЩМЯЭПЩККЛДЧФАИБПМЦЙБЛФАЮЧООШЗЙШМВБНЫЧЧЗ
ЖСЛУЧЛОЧЧАЮЫГБДНЕУЧЙЙДМЪГЮОШДДКЛШЧИУЫХЦБЗФХГШЮМХВКАОЮДКЙУХЯБТЛФА
ЛБЩМЦЗНЪУАГЮЦЭЕМГГМЩВЗЪФЪИДРСВБЛЧШДДЮУЧЧЛКЪЩОНОЩШОЮНАМГЖДМЪУДОЕШ
ФКДЮЩАЮМСАЧЕДРУЧЙЙССАЮАКВЩЙДХЩОДСХМГОДШХЭШГЧЙДШНЦКВАИСЧЩАЮОУНИДЧ
ЩГИКРЙЯТЮДШЭПФФМХКИЧТЙДЭДТЦКЮЧТЧЙКНФЪИДХУВШДСЙЯКЮЦВЯБЭДТАЛМЧПЩЙБ
ЪМЯКЯЦЪГЙЧХОЭКАОМЮКОЫХХКЗСЮДКНХХЭЪЭСМЧЯКЪЩВАЗЧЦВДИДШЭДКЫХЫЖКЫХВК
ОЛМВЯЗОКАНЛЩМЩМБЦПЧИКЫЩАЯКФПЙОКЛШЧМАЯМЧЯКЫПЭНШСШЬМОЧКАВБАЪФНОЛСА
ОКЩХЧДИОФЩНОЛТЭКИЧТЙОШУСУЧОЧФЪЭЧФХЪИАЧЮЧМДКМЭКЯЧЧГЖКМХЬКИОФЦЙОЦМ
УЧЗЧЦВКДРФЧНБЦХФЛМСШЕОНЫЙЪДЖЧУЪННСПЕОЮОЧЦДЗЪМЛБЭЧТЧБЮХХЧИЙХМВБЙС
ПЪЖКМЛГПАЕПГЛМЧШЪЗДАМЮИКМЪАЛМЧЙЧМЯЦЪДШЛЧСЩЙДБЙУМДЦХДЮБАТЙОКНМВВП
ЪГББМЛХХКНЛХЧЯКЧИМНЙОФЪДЙСЮЧЯКНЧЕЯКМХФКЛЩЙЦЙДОШЧЭБЪСЩОШЦМЮКЯЬКЧЙ
БЩТФБЗОТЯНЮДЙЧНОСУНЮЧБТЪЮИОШДБНШХЬКЕЦХФГЯФФЕЗЙБЙУМДЦФАЙБЪСЩЗБХЪЯ
ДНФХФКЙЬ

2. Разложить на множители числа:

(a) 52654285502960226474467116555 9

(b) 54303537966834221872938010442729236869529361423349498488056 1

(c) 11373244679129615150736050802934285202447338222221780413998304653873837210089202284414413 81

(d) 94674376427959758397279758056747199851640434214613403521909716060068822510434415129369269534935780537267280739867744734 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 93228552189735723505708384259050321662395365901797542191735569026498353585393$
- $e = 5$

Сообщение:

- $M = 19744171849530492709473840187489518665636522323522312574740317020393242867170$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 23149816637208485626853584172785328479 3$
- $q = 17711617666747198416074245462543863871 7$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 39364590719945622356375482144208717599137232473893710194138634250810518931180$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 12782221091356124592807948027415223507 3$
- $e = 5$

Зашифрованное сообщение:

- $c = 92587873698252086372310400315227400913$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 25405480909069043130361805527414603333 9$
- $g = 14125642079958838421560758609916249677 9$
- $y = 17926460834729687271051795499869219939 5$

Секретный ключ:

- $x = 14128977994447670130959552910726483978 6$

Сообщение:

- $M = 10160072521891908525262406914447550594 3$

Использовать следующий случайный параметр для создания подписи:

- $k = 11537930067559954856438319347604834932 9$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 20374041406640801691447105857943415088 3$
- $g = 16878429737674024384757553200828971777 9$
- $y = 19056688072617160328822970392138514835 6$

Сообщение:

- $M = 18682329433967836143295551190818507471 3$

Подпись:

- $a = 17410767242447962411652169383820294923 4$
- $b = 10668475364866532621302574708167341429 3$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 919$
- $g = 144$
- $y = 55$

Сообщение:

- $M = 595$

Использовать следующий случайный параметр для создания подписи:

- $k = 47$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 2$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 52

1. (a) Расшифровать текст:

ЧЕСТИМОЕЙИХРИСТИНСКОЙСОВЕСТИТЫМОЙБЛГОДЕТЕЛЬДОВЕРШИККНЧЛОТПУСТИМЕ
НСБЕДНОЙСИРОТОЮКУДНМБОГПУТЬУКЖЕТМЫГДЕБЫТЫНИБЫЛИЧТОБЫСТОБОЮНИСЛУЧ
ИЛОСЬКЖДЫЙДЕНЬБУДЕМБОГМОЛИТЬОСПСЕНИИГРЕШНОЙТВОЕЙДУШИКЗЛОСЬСУРОВД
УШПУГЧЕВБЫЛТРОНУТИНБЫТЬПОТВОЕМУСКЗЛОНКЗНИТЬТККЗНИТЬЖЛОВТЬТКЖЛОВТ
ЬТКОВМОЙОБЫЧЙВОЗЬМИСЕБЕСВОЮКРСВИЦУВЕЗИЕЕКУДХОЧЕШЬИДЙВМБОГЛЮБОВЬД
СОВЕТТУТОНОБОРОТИЛСКШВБРИНУИВЕЛЕЛВЫДТЬМНЕПРОПУСКВОВСЕЗСТВЫИКРЕПО
СТИПОДВЛСТНЫЕЕМУШВБРИНСОВСЕМУНИЧТОЖЕННЫЙСТОЛККОСТОЛБЕНЕЛЫЙПУГЧЕВ
ОТПРВИЛСОСМТРИВТЬКРЕПОСТЬШВБРИНЕГОСОПРОВОЖДЛОСТЛСПОДПРЕДЛОГОМПРИ
ГОТОВЛЕНИЙКОТЪЕЗДУПОБЕЖЛВСВЕТЛИЦУДВЕРИБЫЛИЗПЕРТЫПОСТУЧЛСКТОТМСПР
ОСИЛПЛШНЗВЛСМИЛЫЙГОЛОСОКМРЬИИВНОВНЫРЗДЛСИЗЗДВЕРЕЙПОГОДИТЕПЕТРНДР
ЕИЧПЕРЕОДЕВЮСЬСТУПЙТЕККУЛИНЕПМФИЛОВНЕСЕЙЧСТУДЖЕБУДУПОВИНОВЛСИПОШ
ЕЛВДОМОТЦГЕРСИМИОНИПОПДЬВЫБЕЖЛИКОМНЕНВСТРЕЧУСВЕЛЬИЧИХУЖЕПРЕДУПРЕ
ДИЛЗДРВСТВУЙТЕПЕТРНДРЕИЧГОВОРИЛПОПДЬПРИВЕЛБОГОПТЬУВИДЕТЬСККПОЖИВ
ЕТЕМЫТОПРОВСКЖДЫЙДЕНЬПОМИНЛИМРЬТОИВНОВНВСЕГОНТЕРПЕЛСЬБЕЗВСМОГОЛУ
БУШКДСКЖИТЕМОЙОТЕЦККЭТОВЫСПУГЧЕВЫМТОПОЛДИЛИККОНЭТОВСНЕУКОКОШИЛДО
БРОСПСИБОЗЛОДЕЮИЗТОПОЛНОСТРУХПРЕРВЛОТЕЦГЕРСИМНЕВСЕТОВРИЧТОЗНЕШЬН
ЕСТЬСПСЕНИВОМНОГОМГЛГОЛНИИБТЮШКПЕТРНДРЕИЧВОЙДИТЕМИЛОСТИПРОСИМДВН
ОДВНОНЕВИДЛИСЬПОПДЬСТЛУГОЩТЬМЕНЧЕМБОГПОСЛЛМЕЖДУТЕМГОВОРИЛБЕЗУМОЛ
КУОНРССКЗЛМНЕККИМОБРЗОМШВБРИНПРИНУДИЛИХВЫДТЬЕМУМРЬЮИВНОВНУККМРЬИ
ВНОВНПЛКЛИНЕХОТЕЛСНИМИРССТТЬСККМРЬИВНОВНИМЕЛСНЕЮВСЕГДШНИЕСНОШЕНИ
ЧЕРЕЗПЛШКУДЕВКУБОЙКУЮКОТОРИУРДНИКЗСТВЛЕТПЛСТЬПОСВОЕЙДУДКЕККОНПРИ
СОВЕТОВЛМРЬИИВНОВНЕНПИСТЬКО

   (b) Расшифровать текст:

СЯПГНЖГЦДНСГКПХРЛЫГРЖИНАХЙКНРЦРМСАЦМРАЙЛТЯДЛЩЦЭТГЪЖМЗКЙМЛРИЦНЮТЯ
НФИЗЖКЦЛЗВЮЦГБГШХНФМЪСРНВРЦМРГУТКПЖХИЖДДБЙАГГЩЦАПЩФУЙЛГБМЕЛАЦИИН
КРЛЬППТМРУЙРЗАКГСУЙЙЕГЖЩСПЦЕМСАНСИНОЫЫИНГЧММЫКЦЙЕСГШМИЪЕЩЦАЙЙЦРГ
БОФОАНЛЦУГРЛЦОЙСФЫУАСОХИЛДГКМТЗПЦИАПДРЦЙООКИИЗГНЗЙРЩХМКНУКПЦТКЫМ
МДОМЪОГМЯЙЛЗИЧМНМКРФЙММКФОЙМЧММЫННЦЛМВШЙАБЖЯЗЛЗЛНЖЯНПЪЖЖДЛЙЯЖМКЦ
ЦЙГЛЦЗЙЗЕНЗЙБЛЫОЙБИЦЦЙПЩСЧВМЙЯЦЙЛЩПСНЪЯГПГСОЫИЙЛМЪСЙРЧРРМЙМКФАЛГ
ХРЙОЖЩСИЪКНЗЙГГМТЗЛЩШЙУЗЙРХЧРОПФАЧГХМЛНВЩЦЭДЛХМЕНАРЛЯСЪНЙЙРМЙТКП
ЖРХЕБИТКЯНЗЛПЭДНШМЖЗХХЯДЬНРЗЛУЖМТВБМУМЭРГЙЙКДОНРАМЖЪАИДИЦЦЙПЩНХЙ
АПЪЖАМЛГЙГЛГХМВГРНПЧНИЪХИНПТЖЛТИЦУГРЖЙЯЖНАМФОВПЪФИМКГХЖЫКНПЧЙЛЫП
ЭВМУТЭДКЦЙДРЛЦХЕГЙНЙЭПСТТКЗПРЕЦКМХЧМБГУАГЦПТЛЖДКЫТНГЗОЙЗМГЪЙКДОД
УЙКМКМИТМЩЦЖЫЛЦЙЭНЕДРГРГЙЙАГСРЛЮНОЦИИМГЩОЙКЪТТЯМГСООГЫЪТМООЦХГКМ
ХХГЖСФПАМЖНРЕТВЙЯИЗЯГПЙМГЪЖЙДВНПЙНРКЙТКПХЙНДОЧЙИЗГФИАКЗЯЦЙСГЙЙЮН
АЦФНЗЛНЧЗМЖЯНЬСЬАОКДРШСЯПГРЫМЙЕУИЙАОГНЯГЪТМНГПХТМЙВУЙАБОЫОЙОЖЩМЬ
ЪЙЦСКПАРПКТРДОЬДОМХЕНЗЩПЙАММЙКПЖЩЦИЗЧЫУОВХНЖКПКМТЛНБПСАРГХЕЦКПХЙ
ЮНКХТКНАЩЙДРРНУГБЖМСЦАЩУМЕНЛЩОГДПУЙЯЪГОЙЯМГКСЙНЯХТЭКГФЯАДУУОЛТНХ
ТДПЩЩАЩРАНПЧЗХНИЭЛМЛХЖДВЦЖНЫЕФСЙЭЖПИЖЗЖТФГЦЙФСАОМФМИТРХТКНРРЬАРС
МФЧПВРЕЙВНЦЦГЧГЧФЙЙЙЪОЖЦМХОЗНЛНЧМОГКЙНЖРКТГЛВЦПЮНЛЦЗГЛЯНХЙЛИЫИМО
ГАМУЫВЦЕЛНЯГСКЗОЪТКНВЦЕОФРЦЗЙЗБУИГБПТТЛДЕЩЖАПИУМЬДОМХЕЗГЦЗИЗНЦЙР
КНШРЙМЛРЩЕТВТЧЯСЩТФГЦЙЩЖАКЪРЫЯНБЦСЗДЛЕЦЙВМШЦЙВЛРЧЛЖЯЦНИЗИЦЖЙАШНИ
АЛЖЭУЙЙЛЩСАТАРИЖЗННЦЛМВШЙГЦЯЪВУЙННЦЛМВШЙГЦЛНУЙВСЙМЮНПЧТЯЗАУИЦЙМЧ
ФЙОВНЦЗНГММНЛЩЧТЯЩГЭПГЙМКФЮЛГЩЦАРРКЙ

2. Разложить на множители числа:

   (a) 339737729273181664714507194293

   (b) 10173535613055793608009002668919720607768964966337492514769 61

(c) 732201865822765054263272158821743528856579736679240327070457669578681349491362197702864919

(d) 175924622565884226625886866282834660811533723446561527166551857093186967909992418911595025140980058071696487162121917041 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 732493825544125632755758808032205664843015646557040676177688078568451578185 59$
   - $e = 5$

   Сообщение:

   - $M = 203125285013490775679670419553449951964614883980163338014011119109765020150 73$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 177875115435467097130913990313893025769$
   - $q = 229558388385751687963518102621419369903$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 272987616421523598574178290319394584019697563872217968535535590306326715565 66$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 171258913208835872448846487641995356681$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 543247309443297419404917619269584120 10$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 186620600726360555993110525304531511133$
   - $g = 145982140543583329318974861914222415401$
   - $y = 146698159670007617061628061248967795128$

   Секретный ключ:

   - $x = 120265221464470710726028838609277064254$

   Сообщение:

   - $M = 171662402430547119701475706060665179 18$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 92121016842833141974739089009912793081$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 32221153658550147964137269943632918 6719$
   - $g = 15114703879435339099894608951254555032$
   - $y = 90801103893822154708119032090080237282$

   Сообщение:

   - $M = 679671015433767092528238528825677 2007$

   Подпись:

   - $a = 17631738282817738048877114696519794 4$
   - $b = 26265320902314382171397760611355125313 5$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:

   - $p = 967$

- $g = 578$
- $y = 796$

Сообщение:

- $M = 584$

Использовать следующий случайный параметр для создания подписи:

- $k = 923$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 10$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 53

1. (a) Расшифровать текст:

ПЕЯЬТВЕЮВДВАГДЩЮДНЩББЬЕЮЗЛБВЭЬАЩЯВЛБВЭЦВЭБПЕДЫХВЭБЬЮАЬЬШЬЮДАЬБВГ
ЗЧЛЩЦБЩХПЯГВЭАБВБЦЬЯЕБЕЬХЬДЕЮЬЙЫЦВШЙЕВХДЯЖАБВЦПЩМЭЮЬЬВГЖРБЛЯЫЯВШ
ЩЭЕЖЦВЦЖРЕЯЗЙВЩЧВЗЕГЩЙЙЕБВЦДЕГДВЕЖДБЬЯЕАПЗЫБЯЬВДЫВДЩБЬЬЕЬХЬДЕЮЬЙ
ЮДЩГВЕЖЩЭЦЕЮВДЩЦЩЕЖРВЦЫЖЬЬЮЫБЬЬВГВЙВШЩЕАВЫЦБКБАВЕЮЦЗЦЕЖДЩЦВЪЬЯБЛ
ЯРБЬЮВЦЦВЭЕЮХЩЕГЩЛБВШДЩАЦМЬЙЦБШЩЪШЩБХЩЕЕЬЯЬЩГДЩЫДЩБББЧВХЗБЖВЦНЬЮ
ЫЗДЬБГВЯЗЛЬЯГВЦЩЯЩБЬЩГЩДЩГДЦЬЖРЕЛЩДЩЫЦВЯЧЗБЩЕЖБЗВГЬЕПЦЖРБМЩЧВГВЙ
ВШЬВЮВБЛБЬЦВЭБПЕЮЪЗЮВДВЖЮВЛЖВХЩШЕЖЦЬЩШВЙВШЬЯВШВЮДЭББВЕЖЬАПГДВЙВШЬ
ЯЬЛЩДЩЫЕЩЯЩБЬДЫВДЩББПЩХЗБЖВЦНЬЮАЬЬГВБЩЦВЯЩВЖХЬДЯЬЗХЩШБПЙЪЬЖЩЯЩЭЖ
ВЛЖВЗЕГЩЯЬВБЬЕГЕЖЬГДЦЯЩБЬЩХПЯВГВЦЕТШЗГДЩЮДНЩБВГВАЩНЬЮЬЗЮДПЦЯЬЕРГ
ВЯЩЕАМЭЮЬДЫХВЭБЬЮВЦЫЯВШЩЭЕЖЦВЦЯЬГВЦЕТШЗБЛЯРБЬЮЬВЖШЩЯРБПЙВЖДШВЦЕА
ВЦЯЕЖБВБЮЫПЦЯЬЬАЬЯВЦЯЬЕВЕЖВБЬЩЦЕЩЧВВХМЬДБВЧВЮДЧШЩЕЦЬДЩГЕЖЦВЦЯГВЪ
ДХПЯВЗЪЕБВБЩГДЬЦЩШЬХВЧЦЬШЩЖРДЗЕЕЮЬЭХЗБЖХЩЕЕАПЕЯЩББПЭЬХЩЕГВНШБПЭГ
ЗЧЛЩЦХЩЪЯГДЩЕЯЩШЗЩАПЭЬЦБВАЬЦБВЦЬЛЩААЬЙЩЯРЕВБВАЦЕЮВДЩЗЫБЯЬАПВЕВЦЩ
ДМЩББВАЩЧВДЫХЬЖЬЬБЮВБЩКЫЗДЬБГВЯЗЛЬЯЬЫЦЩЕЖЬЩВГВЬАЮЩЕАВЫЦБКЦАЩЕЖЩЕ
ЖЩАЬГВЦЩЯЩБЬЩВЕЖБВЦЬЖРЕЦВЭБХПЯЮВБЛЩББЮВБЩКАБЩАВЪБВХПЯВЩЙЖРЮАВЬАД
ВШЬЖЩЯААПЕЯРЬЙВХБЖРЗЦЬШЩЖРАДРТЬЦБВЦБЗВЖЮВЖВДВЭБЩЬАЩЯБЬЮЮВЧВЬЫЦЩЕ
ЖЬВШЗМЩЦЯЯАЩБЦВЕЖВДЧВАГДПЧЯЮЮДЩХЩБВЮЫЗДЬБЕАЩЯЕЬЧВЦВДЬЯГВЪЬАГЯЩЛА
ЬБЩЖЖЩХЩБЩЕШВХДВЦЖРЪЩБЬМРЕББЫЛЖВГДВГШЩМРБВАЩЪШЗЖЩАЕЖДБББВЩЛЗЦЕЖЦВ
ВЖДЦЯЯВАВТДШВЕЖРАПЕЯРВЫЯВШЩЩВХДПЫЧБББВАЮДВЦЬТЕЖВЯРЮЬЙБЩЦЬББПЙЪЩДЖ
ЦЬВЮЫБЬЩЧВВЪЬШТНЩЭЖДЩЦВЪЬЯАЩБГВБЩЦВЯЩЩАЩЯЩАЩЯШЗАЯЕШВЕШВТЫЛЩАБЩБЖ
ЮБЗЯЕЖПБМЖПЮЬЯЬБЩГВШЦЩДБЗЯЕГВШЮДЖЩЛРЯЗЛМЩБЬЛЩЧВБЩАВЧХПЖПГДЬШЗАЖР
ЛЖВГДЬЮЪЩЖЩШЩЯЖРАПЕЯРВБЩАБЩДЫЯЗЛБХПЯЦВАБЩЕАПЕЯЬТВГВНШЩШББВЭАБЩЬА
ЦВШБЗЬЫЗЪЕБПЙАЬБЗЖЩЧВЪЬЫБЬЬВХЬЫХЦЯЩБЬЬАВЩЭБЩЦЩЕЖПЬЫДЗЮЧБЗЕБВЧВМЦ
ХДЬБЫЗДЬБШЯАБЩ

   (b) Расшифровать текст:

ЩЗНХФПНВЙКСДЧОЧГПГММПИПФШПДЦМЦЙГОМЪЭУПКЧУЧЯХАЖФЖШНКНЛЪФОДЧЦЩПОТЙ
СУШЫФШСНЧХШПВХМТТЮШПЮТОЪПУПЮЭЦЩННЬЙЧННПИЦЖНЩШОЩШОХЛТАШИОСПЫГШПЛЪ
ХКФЕТОХЖЙЧПУОБЫЩЦФЙТШХТКМЩЕТЛШЦЬТОШУЬОДЫЙЧЙСХЕНЖЕЬЧЫЙОЖЙОМЪЩХНЗБ
БГЦВМТЩЧДАЩХЪНКЬЧСНУЬХЫЬНЬФОЩШОМФУШОХЦЛДВХЫВБХХМПМЫССКОПЦОСШМЧОН
КЛМНУШЩХУНБЫЩЕТДОПНЕПЦРЦЕКЫЪМЖАШШЛЙАЧПХСШТЙЦПЮЧФОЙГМПЦЯНЖЦОСБОЙХ
ЙЮЦЙОСКЬФЧОБЫСЬШЙШЙШПОПУУЦНМЯСНМЕЭЩЖИВЙКСДЧЪНМДХШСПНЬЙСМЖЪЪФФЙЛЧ
ХЬИШТАМДФННЬЕТОЦТАЭУФРМШШОВЙПШХЖНШХКЪДЬГНСПНХХФНМХСЦИЕШФЖЕМХЧВМР
ТЪЖЭПЙЪЖУЬХЛТКЫЩЧОДТИДМПБПЦЙОЖХРМКЛТООЙЕРБГЭЪПЦПНПИОРКБЩСОБСИЧУД
ХШШСДСФЫЭНХПСФУЫЩЕСКОПЫЖЗПРХПДЯФОТОШТЕЛКЭНЪМИПФУЛНЭЛЕВИЪГСЙЮЧХЛО
ЧСФФШОШУЫФФФИДМКЛХПЖИФЧОТОЖФХЙДОЙЧСКМВХЙЗИЛЕНДЛЩЗЩЖЧМЪНКЬЧЦТЮШЕЪ
УМШКЧТОЖИДМОФНОМЪЛПХЙЭШИДМНЩЧЛЖАХПЛЙГЧТСТОТФЦЬБЧЪПЕЧЩХНГЗЫЩЦЬСПУ
ЬМЪОМТВПЧЩСЦЭЕТРВЗЭННЖЙТМХДЙШЙООЙШМШЭЙЫЩЛПЙППРЫЮХМЦИБТЬЦЖЯШЛЧГЙТ
ЩЬУЛШАНВЧХЙОСКЬФЦПИЪГСГЙШЙЦЛЖЭЕЬШНЬГМПОШЙСМБУЧРГМЬФДКДЛМЪТКММЪУЙ
ЕРАЖЗШЙОЛЙПШХЖЗШШЫОКМПЫЭНЧДЫПЕЭНЪОКУУДТЗТПМПОШЙСМНЩЧЧТОТКЧТЛШЛСТ

ЖШЧОЖПЦМЩУЮТЩЕЖБЧМПЖЗТЙЫПМТЮЦППМПНЖОЖЙЩФЖЯНОТОШСЧДКЧМНСПНЦЩПФХХО
ЪБШСЧМКБШЛЕБЪМЛОБЪОНГЗТШЕРБЫФСРШЧВЮЛМЭТЕОЧПФБЙДЦОЛЙАШЙФЙДОХЪЕПЧФ
ЪСПНТСТШТШЫСХХПЦТДЫЩРОДЦПСТИПЧЫЭЪЦВЧЗДОТСРКЫТОЕНЬЙСФЯЪХРНФМИЩЙЙЧ
СЧОБАШНЖЗХХЪЭЭШТЕЩКПЛЛЙВПФСЖЙОЙЧСБТУДПЛЬГЬТЗЕЯФЙЯШТЧТФМИЩЙЙБЩЧОА
ЭУФЙНЖТСГЧШЩНЖОПШЕМДОХКСКМХФЭЙШЙХПДЪЪУЙЙТСЫПБЦЪЦЖКЬЙОШЗЩХНПВОЙЦЖ
ИЧХМПФМИЩЙЙММФЖЗЩЧСОБЫЩСТКХХХЬУПЧОИЙПШУПЗЖСЧНДЧЪЫГНЩВЮОПХХМПЙЖПЧ
ТЮПЩСМОПУЦЬЕЧИЩЙАЕУЦШЗЩЧЧВДМЩЕТДСЦЧЕХПТОКЛШЧЧДОШКННМЖПЛОКМФШПАШЯ
ФЛКЦФОЙОТЬЧГГМУООГЪЪУФНФОФРКХФЧРБЬЧЦЕМППАОБНЪКЙОПОХЖЙТШО

2. Разложить на множители числа:

   (a) 952155037011311993741967257923

   (b) 98225608235169471266051665764402644651902335074698747122350 3

   (c) 17778792838557691557492314577863857328211635480120639357464781078606810785173024403598166 13

   (d) 12865017227344594583895135939740602229637102347872063279209381666213102102974443865189921964775246535598528649609379993 39

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 447741308044483585454824513196266339294190901653024764489630357969001291483 03$
   - $e = 257$

   Сообщение:

   - $M = 505994844010756169375314067190326127191985559070601528159122915352366568747 8$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 215389959303718898295849218242419980093$
   - $q = 27562263680201669494774247497737689950 1$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 365666789568329464757215927102830732472338780207958166311480670433000743124 58$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 165533422290881554249327623543906712859$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 256646799543473900132752464826023657 40$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 211970218366063629103450053355016356627$
   - $g = 125052507080341736217582532901423627972$
   - $y = 173525585353850709427466130607443625234$

   Секретный ключ:

   - $x = 436091183597311088218766891359841165 01$

   Сообщение:

   - $M = 112786722860164461096702202086234334132$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 146183604761246305633069419186619592393$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 308511587316301898896207155455449201201$

- $g = 18666526332843895049506662626231481925 1$
- $y = 24178006647199406924739167714835275910 3$

Сообщение:

- $M = 56500598410183117451067166688726251035$

Подпись:

- $a = 27561093402621983975822659319224796689$
- $b = 13183477369107075449626278493478463064 0$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 1021$
- $g = 640$
- $y = 439$

Сообщение:

- $M = 797$

Использовать следующий случайный параметр для создания подписи:

- $k = 749$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 15x - 4$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 54

1. (a) Расшифровать текст:

УЧЪЩСХЭЪОУРЪБЪШШЗЮОЪСШЯЭГЭЮФКЫЪШСБФЭРСЧЮИЩСБЪЮФШРХНЪПЮСНСОТСЩФБФ
РЪНЬЪПЪГСЧЪОСЦЩСЪДСЧИШЪОЩЩЪПЪФУШСЩЩФЦЪЩОЭЮЧФОЗДСЧФУЦЪШЩЮЗШЬИФОЩЪ
ОЩЪЭЮОДФЭИЩСРФЩСЭШЮЯДЦЪКЪЮГЭЮФЪНЖЭЩФЧСХЭОЪФЫЬСРЫЪЧЪТСЩФШЮЯДЦЭЪЭЧ
СУШФЪНЩЧССФШЪЧФЧНЪПЪНЧПЪЫЪЧЯГЩЪШЦЪЩВСУШЗДЧСЩЩЪПЪРСЧШЬИКФОЩЪОЩЯЭЩ
ЬРФЧФФГСЬСУЩСЭЦЪЧИЦЪРЩСХЪЩЪЮЫЬОФЧЭИОРЪЬЪПЯЭОСЬЩЪХЫЧДСХФЭОСЬЩЗШЭО
СЧИФГСШЦЪЮЪЬЗХЩЭФЧИЭЮОСЩЩЪЬУЧЯГСЩЩЗХЭЪШЩЪКЯЮСДЧЭЫЪЦЬХЩСХШСЬСШЗЭЧ
ФКГЮЪЭЧЯТФЮЩЬСГСЩЩЪХШЪСХЩСОСЭЮСШЬИФОЩЪОЩНЧПЪЫЪЧЯГЩЪЫЬФНЗЧОЭЪАФКФ
ЯУЩОЩЫЪГЮЪОЪШРОЪЬСГЮЪРОЪЬЩБЪРФЧЭОЮЪОЬСШОВЬЭЦЪШЭСЧСЬСДФЧЭИЮЯЮЪЭЮЩ
ЪОФЮИЭСХЪЮОСЧФЯПЪЧЪЦУЫСЬСПЪЬЪРЦЪХТСЩЭШЪЮЬФЮСЧЮЪЮГЭЭЩСКЬУПЪОЪЬФЧЭ
ИЪНЖОФЧГЮЪЪЩЫЧСШЩЩФВЫЬФРОЪЬЩЪПЪФЭЮЪЫЩФЦФЫЪЭОЮФЧССОЪОЭСЮФЩЭЮОЫЬФР
ОЪЬЩЪХТФУЩФЪЩЬЭЭЦУЧОЦЪЮЪЬЪШГЯЯПЪЭЯРЬЗЩЪНЗЦЩЪОСЩЩЪЫЬЪЭЗЫЧЭИЦЯДЧЦЪ
АСХЫЬЪПЯЧФОЧЭИЦЦФСОСЧИШЪТФЩБЪРФЧФЭИОЮЪОЬСШЫЬФЩСХГЮЪФУОЪЧФЧЪЩОГСЬ
ДЩФХРСЩИПЪОЪЬФЮИЯЭСНУЭЮЪЧЪШЦЪПЪЫЬФЩФШЧОСГСЬЪШЭЧЪОЪШЬУПЪОЪЬЩЩЗОЧЭ
ИСОЩЗЭЮЪФЧЩСЭЦЪЧИЦФБЭЮЬЩФВФЭЮЪЬФГСЭЦФБУЫФЭЪЦФНЗЧНЗРЬПЪВСЩСЩРЧЫЪЮ
ЪШЭЮОШЬИФОЩЪОЩЭЧЯДЧССЭЪОЩФШЩФСШЪЩФЫЪДЧФОЭРЩЩОЧЭИСОЩЬЭЭЦУЧФЭЮЪЬФК
ЦТРЪХЧЧСФФЦТРЪПЪШЪЭЮФЦФЩПЯЧОДФЭИЪЩФОЪУОЬЮФЧФЭИЩЭЮЩВФКЪГСЩИРЪОЪЧИ
ЩЗСРЬЯПРЬЯПЪШЩРЬЯПЪХРСЩИЬЩЪЯЮЬЪШШЬИФОЩЪОЩЫЬЪЭЩЯЧЭИЪРСЧЭИФЮФБЪЩИЦ
ЪЫЪДЧОЭРЯЮЬЪНЗЧЪЫЬСЦЬЭЩЪСЭЪЧЩВСЪЭОСЕЧЪОСЬДФЩЗЧФЫЫЪТСЧЮСОДФБЯТСЫЪ
РЭОСТФШРЗБЩФСШЪЭСЩФДФЬЪЦЪСЪУСЬЪЭФЧЪЩСЫЪРОФТЩЪЫЬЪЭЩЯОДФСЭЧСНСРФОТ
ЩЪОЗЫЧЗОЧФФУЫЪРЦЯЭЮЪОЪЭСЩКЕФБНСЬСПШЬИФОЩЪОЩЫЪДЧЪЦЪЧЫЬСЦЬЭЩЪПЪЧЯ
ППРСЮЪЧИЦЪГЮЪЫЪЭЮОЧСЩНЗЧЫШЮЩФЦОГСЭЮИЩСРОЩФБЫЪНСРПЬАЫСЮЬЧСЦЭЩРЬЪО
ФГЬЯШЩВСООРЬЯПНСЧЭЪНГЦЩПЧФХЭЦЪХЫЪЬЪРЗУЧЧФЫЪНСТЧСХЩОЭЮЬСГЯШЬИФОЩЪ
ОЩФЭЫЯПЧЭИФЪЭЮЩЪОФЧЭИОЙЮЯЭШЯКШФЩЯЮЯЬУРЧЭЫЬФЮЩЗХТСЩЭЦФХПЪЧ

(b) Расшифровать текст:

ЫЖВНКЩШПЭЖЬАЯУЯХШЩЫЭЪЮЦЭЖГЬЩПЭЮТГЫЖФГЯЬЖХШВЫВЮЫВЪАВГБЩББЪВЬКЩЗЦР
ГНЮЛЭЭЭЮЮЩЕИЮЯЩЙНВВРЪЯЗГУКЮЮЩСАЬГЩПЖБДЕЦЭЭЩВШЫЯБЗМЭЪЮЬОИУНЙЫЬДЗШ
НЖБДЦЖДЩВЯЗПЩОЮЧАЭЫЪПЛГЫАЧАЮЙЯЩДЮЫМРЙГГШБКНБЩЭКДИЕЮЬНЧАЩЗЦЖЩЧЭЮЮ

ЯЬФЯЪБСЬМДЕРЕНФАЭЛЙАЦЫАЬШЧЩЙГЮБЩБЭЫШЩЪЯЫЦЫЭЮТЩЩЩЬЮЫЖЪВТЕЧЖГЖЩЦЕЫ
ЮГЮПЩЫГРЕЫЮХЭЦЙАЗЩВЮНЬЭГАЖЬПЪЯЖБЖБЫБЩШЬБТЩСЭФДШШЖЩВГЩГДНЩЧУЪУЖХЕ
ЩЩЬЧЭЬШЕРЫХЗЬЦФЮДЩШЕЦЩВНГЩГЬРЕЩАВОЬЮЫГРИЦНЬЭУУБВШЭЦЧЩТЖВДХРЕЮДЧЩ
ЛИЗЖУАИИЩШАЦУЖЩЗБДЬТЪЯЪЬЦЖУГЩЧЪВЫЧПЛХЮЦУКЦБРШЖЦШВЦЕЦГЬРЮЦБЛУДГЙМ
ХЯЮШМШАШЙЕЭФУЗЩРЫЯЗЦЖПЩЮВМУИЮЦЬЭФЪЕЭИЬЗРТЙДГЗЭФЮЫЕВЙГГЗЙВЮЮЧЮВЫВ
ВСЕЯЕВПГЦЫЬЭВЩВВМИШДАЪИЩЪЦЩИЮСЭХГЦГШЫФЮЫГЩЗХБЕРДДГЧЦЯЩГВОЬАДКРГМ
ВАРЙЗВЫЭЖЫДЧПЖЮЗЯЮПЪГВРЫЯГЙЩЬЩБЖЩЩМШЯЩЗЯМЩЦУЭНЕЧЕЦШПЪЛВАЯЮЮЩЭЕНЖ
ЩЛДЮВЩИЮМКПОЮВАГБГЫАХШВЫЕМЯЮЦЭЮЪДЗАШЖЩПВЯЕВСАЭЕЯРПЭЮЬЪЖУИВЫЪАДЯО
ЖЬДЕОЭЮЫДЦЗЯЖЗВАЫДБЮДЦГЦЫЖГЫХЖГВЫДСЕГДАЩЩЯЮЙЫЖВЗЬФЙЫЮЙЩИХЫБЩЪЫШЯ
РИХШБЩГЩВПШВЯГЩБЩГФМХРУСДШЛЬАЯРЕХЖРШЬЩШБУЗЯЩДЮЯЩБЕНЯХЙАВАУДЕЭФЮЫ
ГЫЭХШЩДЪЙЙТШАИЫЧЩЬЯЧДЩЫЯШШЫЛФДБЩЩБИЬЦЙЫВЖЮРЫЦПЖГТЦЬАЬТЩНЕВАВЦФЫ
ДЯРКАЫЖЫЛЙЫШНЖГЕВГЭЬЗЩЧЕХМЖЖБФДШЩВЯИЦРПЬВЖЮРЫЕЩЭИДОДЩЬЩБЕНКЯИЕЧУ
ЪЩВПВЫДЮЫАУЫЯЭЭГЙМХЕВИЕЗЫБЗЬЧЖУГЬХЖФЪЩДЭХДХЫЖАЖЩЫЪЬЧЖЙРЫЕВЫЭФДЦЬ
ГДЬХЮЗЯБЩЭЭЙХРЫГТГЩЬЦШЬВФЩВШЦЯЩИРШЫЯБЗМКЮЮАЖЙЬТВЬВЯЖВФИШБЗХЭВДА
ШЖПИЮЪЖБЭЬЦДГЙМХЛИИВЩЕДЖВШАЬБВСВДШЮЬКБФЯЗВДЮЕЦЭШСГЩКЦАЯУЗЯЫЩЦАЗЙ
БЪИЯИЬНКЯЩВЭИДЪБЩЖАЮЕЭФЭДЩНЖВЛЬДЭЮЮЩЧУВБРЩЙЬЙЪМЭВБЬНГВТЦЩДЮЫЕЧУВ
БАУЖВШВМЖХЫВМЛХДЦЩГНЗЖНАЖЕЩЭЭБЧЗЫЫВАВФЮЩЭБУЪЯДХЫЮЬЗЩМЖЕЮКРИЯВЧНИ
ХЮЬВКЯЕВЧЕЦГЬЙДЯЫАЮЩМБВНЭБТЙЩДТБЧЩЗЯБЗВАИЫЯЩЪЦНЩЬВЯЩВМКПОЮШЭЬФХУ
ГЮЮГРИЦВЩШКНЗЦЩАЮВЩЫЭЮЮБУЖГАЯПУУИРУНЩЗГЩГЮЫБУЭХЫБЗЖГРЩТЬДВВРДДЧП
ЦЕШГЛРЕЮАБЮЕЦЧ

2. Разложить на множители числа:

   (a) 98757432572884119035225189602 3

   (b) 7135707640248448854065541059436248314376745585478554270023 77

   (c) 9129398211961429476030837961518600815642875803889018265667770019067633263957410344697547 97

   (d) 1092311423379090818755052519200901436296812030843927536243151825112254565744932939922216330747627397736492696870069020871

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 71788367061412336341726968189038870999572757246183729122621547668278643022961$
   - $e = 5$

   Сообщение:

   - $M = 21160557873542685952774243851050199371501360947337042500140149182291661159852$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 185739219356263533026518707015643114147$
   - $q = 253285012068749632130963963484990149473$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 322846895565018839418127325922188656405374592738804616605199892849505131813 29$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 157432593362490992301328818398319116311$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 81505033528719183909140018871714614260$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 19695061766336461082831473337355844639 7$
   - $g = 30131327493955565026669885741374432307$

- $y = 851697071169193815980490717818734176 4$

Секретный ключ:

- $x = 377977696968105494703846999061122406 87$

Сообщение:

- $M = 926853720315358808891607209771176056 98$

Использовать следующий случайный параметр для создания подписи:

- $k = 348234045622158773084496444889992942 19$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 210025716336113023942690407696420024443$
- $g = 515095916969060846367510557913283060 38$
- $y = 889739118940984100814760190399503117 73$

Сообщение:

- $M = 459276283638291943902748738659152319 09$

Подпись:

- $a = 385875527804054977869908508564349884 15$
- $b = 973688596540735429330908261977078435 55$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 907$
- $g = 209$
- $y = 61$

Сообщение:

- $M = 283$

Использовать следующий случайный параметр для создания подписи:

- $k = 653$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 5x - 9$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 55

1. (a) Расшифровать текст:

ЭЯВГЮЯУЩГНВЩХЯЧХГНВЦФЯЬДЮШЙЬШЯТЬЫЯАЬМУДИЩЪАБЩШБЫВХЦЬЬВЦКЦЮЦВЮЦЦЯ
ЮТМЬЯГЭЦЮДЧЦТЬЩШЫЯЩУВЦЦКЦЮЦЭЯФБШЬЩИЩГНИГЯТМОГЯТМЬЯФЯУЯБЩЬЩФБЦТЗМ
АБДВЮЦАБДВЭИГМЮЦЭИГМУХБДФЬДЮУМЙЬЩШШЯТЬЫЩЯШБЩЬШБЦЬЩКЦДЧВЮЯЦЫЮЭЮУВ
ГБЦИДАЬМЬУЩВЩЬЫЩЗДГУЦБЧХЦЮЮЮАЬЯГДГЦЬУЩВЦЬЫЩЮАЦБЦЫЬХЩЮЦТЯЬЦШЮЦЮЮЯЦЬ
ПТЯАМГВГУЯЯУЬХЦЬЯЭЮЯПШЖЯГЦЬУШФЬЮДГНЮЬЩЗУЩВЦЬНЮЩЫЯУАЯЭЯЦЭДАБЩЫШЮЩ
ПФБЦТЗМШЗЦАЩЬЩАЬЯГТФБЯЭЬЯХЫЭЯГЯЬЫЮДЬВНЯАЬМУДИДПУЩВЩЬЫЩЗДУМАБМФЮДЬ
ЩЯИДГЩЬВЭЦЧХДДЧВЮМЭЩВГЯЬТЭЩБЫЬДЮЯШБЬЯТЦШЯТБЧЦЮЮМЦЬЫЩЗЮЦВИВГЮМЖЯХЩ
ЮЩШЮЩЖТМЬВГБМЪИДУЙХБДФЯЪБДВВЫЩЪЫБЦВГНЮЩЮВЩЬНЮМЪЫЩШХЯБЯУМЪЭЬМЪЬЦГГ
ЩЮЯУШФЬЮДУЮГБЦГНЦФЯВЩЬНЮЯТМЬАЯБЧЦЮЩЮЦЭЯФДХЦБЧГНВЯГЧЬЯТЮЯФЯУЯВЫЬЩ
ЗЮЩОГЯТМЬУЮНЫТЦХЮМЪЭЯЪУЮНЫАЯФЬДАЯВГЩВУЯЦЪАБЩВГУЙЩЪЫАДФИЦУДЮХЮЩЭЩ
АБЩТЩГТМЬИЦБЮХЯВЫЮЫЯГЯБЯЪТЦЬМЭЩЫБДАЮМЭЩТДЫУЭЩТМЬЯЮАЩВЮЯУЯБМЩТДЮГ
ЯУКЩЫЩФБЦТЗМВЭЯГБЦЬЩБУЮЯХДЙЮЯЩЯЧЩХЬЩЭЦЮДХЦБЧЩУАЬЯГТФБЯЭВЦЬЯАГНУЬ
ЯХЫДАЬЯГАЯАЬМЬУЮЩШАЯБЦЫЦУЩВЩЬЫЩЗХЯЬФЯИЦБЮЦЬУЯЭБЫЦЮЫЯЮЦЗЯЮЩВИЦШЬЩЬ
ЯХЫЭЯАБЩИЬЩЬЫУМВЯЫЯЭДЩЫБДГЯЭДТЦБЦФДКЦХБЯБВАЬГЩЬВВФБЦТЗЭЩЯХЩЮЩШЮЩ
ЖАЯУЦЬЭЦЮЫУМТЯБЮЯЭДХЦБЦУЮЩЮЖЯХЩУЙЦЪВДАЦБЦУЯШУЯЙЦЬВЮЩЭУЭЦВГЦУЩШТД
УМТЯБЮМЪДВЬМЙИГЯГБЦТДПЬЯЙХЦЪАБЩЮЬТМЬЯЭЦЮХЯУЯЬНЮЯФБДТЯЮЯЭЯЪУЯЧГМЪ

ВЫШЬЦЭДГЩЖЯЮЦВЫЯЬНЫЯВЬЯУЩЦФЯВДБЯУЯВГНГЯГИВЯТБГЩЬВНУГЯБЯАЬЩУДПДВЬ
ДЧЬЩУЯВГНУЯХЮДЭЩЮДГДГБЯЪЫТМЬФЯГЯУВЦЬУГЦЬЦЧЫДЩУЦЬЦЬВЦТУЦШГЩУЮЙДХЦ
БЦУЮПВЫЫЬАЯТЯЬНЙЯЪХЯБЯФЦЭЩЭЯВАКЩЖХЦБЦУЦЮНТЯЬВЯХЮЯФЯТМГНЯВГЮЯУЬЦЮ
ДЮХЯБЯФЦЦВЬЩЮЯИЮУВГБЦИЭЯЮУЯЬФЦХЯЫШМУЬАБЩВДГВГУЩЦТДЮГЯУКЩЫЯУГЯЯЮУ
ЭЦВГЦТМЬХЯЫШГЦЬНВГУЯЭЩВЩЬНЮЯФЯАБЯГЩУДХЦЪВГУЩАБУЩГЦЬНВГУЮУВЫЯЪВЬД
ИЪЩЭЦЬУЫБЭЮЦАБЯАДВЫУМХЮЮМЪЭЮЦАДФИЦУМЭЩАБЩЫШАЯЬЫЯУЮЩЫФБЩЮЦУЮЯЮЩЫГ
ЯЭЮЦЮЦУВГБЦГЩЬВЩЫДГБДШУЩ

(b) Расшифровать текст:
ССЯТРСГЙЭЗЭОФУЬФКРЮУЦРСКЭСПУКШФДРЙВЮНЙЪЭИНЦЗРГКТТЬЧДЛЦЩНКЧЬХЩДЖК
ЬЮЫМЧХЦТИМРБКМЙЩЬНЗНШССМСОЧЙФШОЪЛХЧЦНЪПУРПНЕХШФСАЦНСКАНВУМЙИЩУРЦ
ШЪФКХНЩБНЦЖЖЧНСКЬЧТЬЧЗЭВТЗЩЬЗПУШЭДФЙУЮНЖУЫЪСМРЬНЪСФЩЭСТРЖХГЖУЫЩЙ
ЧЭЦЭАЯЬЙЫНЫННЧАЯЦРНДИУЮЮПЕШЫНТЦНАЧНЦФЫОЗПНЬИАЯЙЦСДМПЮРРУКГФЛИУМЬ
НЕАШЭБИБМЯРЖКЦИЗЫЖЖЧОФЗПСКЦБМЗКТТРГДЗУЬЩДЗЧХФБПНЦЪЙТРЩЦЗЕНЭЦЗУУП
ЗЛПЦЬЯВФУМЧНЬЙУЭСТРУЫНСШЫПНПУНЯЗММЫСГОЗТРПЗННШШМПАЪГМРХЬТЗУЧЪССК
ВСВТЙРЧСАШЦТЗЖШЪЬЕАЦНСКАНВОНФЬЦПКИКЦОНЖЦРЭСТХЩЩЪСЙРЭЫЧЗУРДЦБАЪСА
ФЫФЖСПСФКМРУРНФУОФМТТУГДЗУШСЛТИЫУКМЬУЮЫОХЩШДРШЭЩНЗУХЬТККШФЛЦКЦФБ
ИХЮПТЖНПСКЫЧЩЮНЫКЫЩНЙВФШШМПТЦПМЬЦЭЛТЧЫФЦЦУЭШСОУРГДФТРССХСДФЙХЧЦО
РРЧЫФБЦБЬННЗМШССЕХУЩРОМЦЪМХЙЬИМХЗЩСЛЙЦЭЪБТМШСБТМПСПЙЗЩЩДИКЫСБТПС
ССХЬЭЪЧЙЗРЧЗЦЦПЪККТЩНЪЦБУЧЗЖУЦЦЗПНВСКТЗРЦОФНХУКЙЪЭИМСКТЩЙТСЖХОФК
ПШДЦПЩЮНФАФЮНЦЬЬФРЦРЪЪГЖНОЮЫХТЧЩБХЧЫСЦЧЬРЬДЛЙНСЛМТЮЮЪРАЪЪПЖТЦФРА
ЦВСКТЗРЦНРИРХГТЖЫЗИЫКЦЪБЙПТЦПМЬЦСЛЧСДФЙХПСФМЙМШСЧАРУПГЙЙЩЬНЗЙЩЬН
ЗЧЩУГЙЦЗЭСТГШЮБЙХПЪИУУЦЪРЙУЭОДЫРПЪПТЛШЗИИЬЭЪСТРХЯОТЦЦЯЧНСЮТЗЫУХЭ
ЙЛРРШТЛТРДЫПНЭЗЬЦШЬЮНФУШЯБТМЗШДЬББЬЧЗЦАПЪБЙЦЭФЛЙТПЪМТЬЦСВХЧЩЬНССШ
СЖСПЩШНЦЗРГКИУЫЪЕСАФЭКЖЖЩПТМЦАЪЕЙТУУЩЙМССМЖЙЩЧЫМФЩЫДФКОРБМЭЗЦЙУУ
ОЪГОПЫУРТЖЗСЧАЦЬРНФУОФКЧЬГСЖИКЬИНХЧШЪБМЧЗЭГУКЫСЕИЧЗОНХБМЯПСШЭФФС
КЭРМЙЖЩЫПТЦШФСХЧЩПГСОПСЛИУЫЪВЧФЩУБЙМПШДЗУАЧГСУХЬНЖНРЪАТЙЫФКТСРЩТ
КХРДЗПЦЪЬДИЗЬСАЕУСФДНЗЩЧДСУВСБЦБЪЪРФКПФРЦКЪФЙОЗПЬТЗЙЩЬНКТЖХРЙРЪЬ
НЖУЫЩНСУМЧТЫУХФРОМЦШШМПЮЩТХРННЗШСФКТТРРКЙПЩЭБТХВФБНЗЪЬБТЙЪЪДЛЛФ
ЫНЫКЧЯДЩЧЗШМЙЗЪЬБТЦЪЬНХНЦШШМПЬЩДЧЙЩОНПБЬЮБМКЧПГЙЧЖОЗИНГИГТХЩПТСК
МЪРАР

2. Разложить на множители числа:

(a) 418816215007686922175922677419

(b) 565339663747363478753424676954297996243702391050626647390849

(c) 1143576211228922290397783682296791727577678089952242431530146054440260000323848252405564973

(d) 1349369103742685958503553687619418326799060296199054054962825331168982355275251211600900852931203513158236695401924121899

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 631879097263862212960914359065639160648846562153126949422149605356615182084 17$
   - $e = 3$

   Сообщение:
   - $M = 624661581797953527605773892007365280689212908230481680285124435776500390935 47$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 291120864116998759048442017481504704111$
   - $q = 211796820126837805942260467280740077579$

   Открытая экспонента:
   - $e = 17$

   Зашифрованное сообщение:
   - $c = 395114712904826264308718594180139841884983706063015221414236757158459710653 17$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 266090820843773254648717644052999232431$
- $e = 5$

Зашифрованное сообщение:

- $c = 178066930799168555422997258092035565988$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 257555032329362857510757207461851266521$
   - $g = 652998866111720376848742387426553931 80$
   - $y = 627031014079472055465306158573433 5045$

   Секретный ключ:
   - $x = 68377396337694251717459940818211908509$

   Сообщение:
   - $M = 161069069060454976792892982175133815578$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 171608240315458688030291116324601255 57$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 244018325897657860393785009746386714943$
   - $g = 800765040914522519078231104255087474 01$
   - $y = 208121226575589848616959437078871644335$

   Сообщение:
   - $M = 217751444980361737208091386827448356938$

   Подпись:
   - $a = 117068104812517360937725434270466359126$
   - $b = 129907009966781773696543486745970047396$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 607$
   - $g = 363$
   - $y = 213$

   Сообщение:
   - $M = 380$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 367$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 16$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 56

1. (a) Расшифровать текст:

ИВИОБЕПЩООЗЛЙКБЛЯИЙНХЙНХЯАИЛМЕОИЯЮЛАРМНЕОЗЗИЯЛЯНВЙАНЕКВЯКОПЛИКПЛ
ЙФПЛЮШАЛИЛЯДВЙОЗЛАЛЮШИККВОЗЛИЩЗЛФОЛЯЯШОПЯИВККХВОПВРЗЮЗАРОНШЯЛДЯН
ПЕИЕОЩОМЛАЛКЕДТЯПЯМИВККВОЗЛИЩЗЛФВИЛЯВЗЕТДМВНИЕЯПЛПОЙШЖКЮНЯЗЛПЛНЛ
ЙЯШБВНГИЕЙШБЛОПЛМЙПКРЫЛОБРЙШНДЛХИЕОЩЗГБШЖМЛОЯЛЕЙЗЛЙКПЙОПНЕЗЙКРГВ
КЮШИЛПБШТКВОМЯХЕУВИРЫКЛФЩЮНЛОЕИОКМЛОПВИЩЕЗНВМЗЛДОКРИАНЕКВЯМЛХВИБ

ВИПЩОЯЛЕНОМЛНГВКЕЯВФВНЛЙЙШОЛВБЕКЕИЕОЩЯАЛОПЕКЛЖЛЗЛИЛОЙЛЯНЯВОВИЛНД
АЛЯНЕЯЛЙЕКРЯХВЖЛМОКЛОПЕЙНЩЕЯКЛЯКНДИЕЯИФЖОВИМЛБИВКВВЕДКИОВЫЕОЗИЫФ
ЕПВИЩКЛНЛБЕПВИЕЙЛЕЗДИЛОЩЮИАЛОЗИЛККЛОЙЛПНВИЕККВГКЛОПЩКХЕТЛПКЛХВКЕ
ЖБЛОВИВЪПЛПЯВФВНГЕЯВПЯЙЛВЙЯЛОМЛЙЕККЕЕЮШИОФОПИЕЯОФОПИЕЯОЛЯВНХВККЛ
ЙКЛАЛИЕПЗЛЯШТЙЕКРПЯЮВБКЛЖГЕДКЕФВИЛЯВФВОЗЛЖКБНРАЛЖБВКЩБЛИЛГЕИЕЮПЫ
ХЗВФПЛЗНВОПЩКВЯЕИЕОЩКЮНОЗЛЖБЯЛНОМЛЯЕККЛЫЮПЫХЗЯШХВИЗКЕЙКЗНШИЩУЛМН
ЕВАЛМЛЯИВКЕЕЙРГЕЗЕОПИЕКЗЛИВКЕКРФПЛБРНЗЕОЗДИЛКЕЙДФВЙЯШЯДБРЙИЕЮРКП
ЛЯПЩЯЕКЛЯПШАЛОРБНЩПШКХЛПЯВФИЕЛКЕЯАЛИЛОПЛПЛЯЕКЛЯПШКМНЛЗДПБЕОЙЕКВН
БШМНЛЦЫЯОБИНБЛОПЕФПЛЮЛАМНЕЯВИЙКВОЯЕБВПЩОООШКЛЙМВПНЛЙКБНВЕФВЙКРБЛ
ЮНЛМЛЯЕККРЫАЛИЛЯРЙВФКВОВФВПЯЕКЛЯПШЗЛКВФКЛЯЕКЛЯПШЮЛАБИЯВБНЛМЛНЮШО
ВКЛРЮНПЩЯШБРНФЩВУВИШВПНЕБКФПЛБВИИЕОПНЛОПКНБЕПЩМЛАЛИЛЯКЛКОВКЛЗЛОБ
ОЙЛПНЕНШГЮВОПЕФПЛЮРЙВКЗЕИЩЕКРБКЫЯОВОВКЛЮШИЛЯЗЛМКТРЮЕНЖПВОЩЙРГЕЗЕ
МЛЗИЛКЕИЕОЩЕМЛХИЕКЮНЦЕКРЗЗКЕЯФВЙКВЮШЯИЛНКХЯЮНЕКЛЗДИОЩКВОЙВНПВИЩК
ВАЛОЗЛКЯЛВЙЛПМНЯЕИЕЯЗДКЩЯЕБВИЕДЛЗКЗЗВАЛРИЛГЕИЕЯПВИВАРЯДЛНШКХЕЯОП
НВПЕИЕОЩЛКМЛПРМЕИАЛИЛЯРМЛОМВХКЛЛПЛХВИЛПЛЗКЮЛИОМЛЗДШЯПЩЯЕБФПЛПЛНГ
ВОПЯРЫКБКВОФОПЕВЙЕРКЕГВКЕВЙКВБНРААНЕКВЯБЛИГВКЮШИЛПМНЯЕПЩОБИВВНВХ
ЕИОДКЕЙМЛОИВБЛЯПЩКВОЙЛПНКЙЛВГВИКЕВМНЛЮШПЩВЦВКВОЗЛИЩЗЛБКВЖМЛ

(b) Расшифровать текст:

ЬМЗЩЩЦЬДГДЩГГЬПЬЮНЬЩГЫЫОЦЯЖШЕШДЯШЯПЮЬБЫРЬЫДЩЬЦКИЕЫЯЖСЕСЩЭЙЩУХЮИУ
ОБЗЭДЖЦЪЗЙУЯЖСШГЮБЮЩЦЮЗГЯВЦЬДДРУБЪВХБЗВЬПЦЙЫЩЮЙГЮЕХБМЬЬШЮЗЯШЫЦЫЫ
ДВГФВЮМЯЙДГЬЯЭГЕФВЛДЗЩЮФЗЙЩЬБИЗУЩДЮОРГФЖЬЫЬБЖЫЬЦЖЕЕЦДАГЬЬЦЖГТРВЖ
ЫЪЩЭКЪЗЮФЗЯИХББШЯНЙКВЬЦНЖЮНЬЬМЧЕВЮФВЯХБФБУЧЩДЫДУУЗДЖЮКЮГДЖЭБЩЫРЧ
ЮАЗРАЗЗЙЗВИЖЕЬЩДЗКПЩЫБЬШЩЮВЫНЯЛДДЩГЫЫОЦЭТЮБЮЫАСЩШХЮЖЬНДСАКУВЦИЯЧ
ВДДЩЩЭЕСЩШЦЮШСРЖДЮКНЯЙДЙЮУБЪЬЦВЛЖКЙИМЩКШЮМФЖЮЙГЙКЦЩПСШЖЬБИЬЬЮФЮБ
ЫЩЫСЯТТФГЯТЫБЮШЩЬХОЬЙИКИЯЙАЗАЗЖГФЗЕЦЯЕДХНЦДЫВРЖЛТБХЯЕЫДПЮЛЙЯВЦЙЫ
ЮЧЩЖЙЙЮЫБЧЯЭЫЗЗЙШЯЫЮВЬНИЫЗРХЭЫЗРУЖГТЧХЗВЯХЯЕШТЬГЙДЬШЮФВДНМКДБЩЭЕ
ЫИЭЦЪБЯТХЮЖЬНЮЖДАСЦПЫЗХУБГЯХГЗГЬНВЛЖЬЭЩДВЬШАЗОЬЦУКЫДУЩЗИЩЩББЫНЦ
ЙТЩЪЦЙЫЫШПЧЗЙЫМВЮДНЬБЪИУХЖЗЙЩЬЮГПУУДЗЯШПЧЭЖЦГМГВЩЫЗИУТЦДЫДЩФЗВКШ
ХБЖЩРЬЮББЧДЭДВЩЧБИУЩТЗВДРУЗЯЫУТЛФПХЯЛШЬВЬБГЩЦЩЭГПУХЗВЩЩЙЮБЩВЩКИЬ
ШНГЙХХЯЕГЙХДМЧЗШЮМФЖЩВЛЖЯШЮЗВКНДЬБКЬГЗБПХЕКЕЕЬДЭДАШВЛЫДРУБЗЬЦХБЕ
ВЩЭЗКЯБЦЙЗБУЪАЗЙРЫДДГУУЙВБРЯГДВЩЮЮЩЕХБКДЩЦЩКТВЮТЗНДЖЦГЖЙУЮГЮЖЫЦЭ
ЗЙНЬЧПЯРУАИЯРЫБЗЙЫЩЖЮЕВЫЗШЙХЧЮШТМЯЙГЬНЦКИТУАЗЩЗРТЮГЯРЫЗИКЩЫЖЗЯПЦ
ДЗЙЫДСАЩЭЦДДЪЫЦВАЬУВИБЙХЯЕГЪЩЬЗШЬЩЮЙЭГЭМЫБДУГГЮБЩГЗЖТРХЮЖЭЦБКЕВУ
УЖЖКХЖГЖЯНЯВЗЙЫЩРДБНЯНЮНРБКАЕЧЭМГЫУБЮНЙЩУЕЙЪЩХЖДШЭПСАИЪБЗЗЯЦЯЖЕЗ
ЩХЗБЭЬУЗЫЮШГБЫЕЭУЮНВВГЗЕЗУЦОБДЬЬМЬШЮЩЫЮВЬАЗЪЕЦФМЗЩЩЦЕЙБОЯКЕЕПЩЖЙ
БЪЩЛГКУВЦИЯЧВДДЩЩЭЗЧЗЭЩДЗШЖЬЗАБЫЩЫДГЮВЛЖЯВЫМЕЗУЮБВЬОЯААЕЧЦЖЪДЭЮЗ
ЛЕТЪГЕЬЫЦЪЮВТГЫЫЗСЦЖГКЙЭЖДХЫЦРТЯНЮГЙЮЧЩРЪЕЧЮЮИИХШДДДЩЮИДПРЬЫЩЕЬГ
БАЕЭЗМЩЬЫВБВКПУКЫЗНЮЗЧЙЙЙГЫЪЩЖЗЭАХАЙДПЮЬЧЧЯЭНБЬВЩУЛТИПЩКТШЭПСАЕШ
ЫДЮБШДДЪЬНЫМЮЩРЬЮБЬФАЗЭЩЭНМЖЫШЩГЗЙЫЩРДБЬУЗЮГЩХБГЕХЩЕЩВТЯЕЕЕОЬЭСЩ
ЦЮЕЫДЬЬЧЧЕЪМЛЗЙНЯЕЗГРПКЕЗЩВБИУЬЫАБЕШУФШБХЯЕЕЕЦЫМЮЮНЯДЮВУВДЙЭУГХЙ
ЫЩУДЫЙНЯЙЮ

2. Разложить на множители числа:

(a) 1142240606895934215400087194947

(b) 739618260316697785598109680533737804115498908668884505681863

(c) 883866677007041402869610338828113162807382999185855037621060762512645820498524032826335113

(d) 145957574098753735479171971117929581542384982309878630656113335345423616852498644240747919261831176084211020893890813895 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 500292395133484676451939614236818967100408646571408527235713612697092143137 63$
- $e = 3$

Сообщение:

- $M = 352055076959223628027646953481135033746003023578389112957855752135880304428 0$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 32115604004817903783967766443537714147 7$
- $q = 29631174783899706136558018773665918604 1$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 31777165411094298262102949715406774152340560262268418953554870664443526682100$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 11602418314944159874709176511578164100 9$
- $e = 5$

Зашифрованное сообщение:

- $c = 32852874747753712151352087355981242008$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 21745461578854014927327128716144692668 9$
- $g = 16996505754032362672843784716437118129 7$
- $y = 31532889788106769877871945504984809816$

Секретный ключ:

- $x = 12219330259306655013445958485837123700 0$

Сообщение:

- $M = 17459396196374664146545658732990645927 7$

Использовать следующий случайный параметр для создания подписи:

- $k = 11434235183670724681830120563319950473 7$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 32675078479990219349633174040067636778 3$
- $g = 29052116823397835433315836482381543057 1$
- $y = 71871110086701681246453869294515830 74$

Сообщение:

- $M = 92147691052196533490555804770753557191$

Подпись:

- $a = 23010576425508166211169666910156305003 8$
- $b = 57416093042773717137637749285239016547$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 877$
- $g = 672$
- $y = 784$

Сообщение:

- $M = 822$

Использовать следующий случайный параметр для создания подписи:

- $k = 713$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 14x - 3$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 57

1. (a) Расшифровать текст:

АЭЯЛИАЕЫИЖДВЖЖЩЖЬИГДЭЕЬАЪАГЙДЖАДЩУЙКИУДЛЙЗЭНДАЗЖЙГЭЕЭЙВЖГФВАНЛИЖ
ВЖЪЗИЭЬГЖЮАГДЕЭАЫИКФЪЬЭЕФЫАЗЖЖЬЕЖДЛЫИЖРЛЕЭЬГЪУАЫИУРКВПКЖЩКЖГФВЖЕ
ЭАЫИКФЬИЖДПКЖЗЖЭЫЖЙГЖЪДЙДЙВЪЭИЕЗИАЪУПВЙЖЫГЙАГЙАЕКЖЯЛИАЕЪЭГЭГЗЖЬК
ФЗЛЕРЛАЛЫЖЪЖИАГДЭЕЗЖЗИЖЩЖЪКФЗЖЪКЖИПКЖВЙГЛЮЩЭЕЬЖЩЕЖДЕЭЗИАЪУВКФЩЭЯ
ЗЛЕРЛПКЖАЙГЛЮЩЗЖЙГЛРГЙЭЫЖДЭЮЬЛКЭДАЫИЕРЗИЖЬЖГЮГЙФПЭДПСЭЗИАНГЭЩУЪГ
ЖКДЖЭЫЖЙКВЕКЭДЙКЕЖЪАГЙЖКЪЮЕЭЭРИУЗЖДАЕЛКЕЖГЭКГАЛДЭЕПЭИЭЯЩЖИКЫЖИПА
ГЙЩИЕАГДИВЭИВЖКЖИУБЙПАКГЩЖЫЪЭЬЭКВВПЙЖКПЙЛЛДЕЖЮГАЫИЛЙГЖЪЖДЪЭГЙЭЩВ
ВДГФПАРВЪУИЪЪРАБЙЕЪЖГЦДЭЮЬЛКЭДЪИЭДЗИЖРГЖЕЭЯДЭКЕЖЯЛИАЕЪЯЫГЕЛГЕПЙУ
ЗЖГЖЮАГВАБАЖЩТЪАГДЕЭПКЖЗИЖАЫИГЙКЖИЛЩГЭБХКЖДЭЕЕЭДЕЖЮВЖЙДЛКАГЖЬЭЕФ
ЫАДЖАЩУГАЛЙЪЭГФАПЙКГАЯЪАЕКФЙЯЛИАЕДЭЕЗИЭИЪГЗЖДАГЛБЕЭАЯЪЖГФАЩЭЙЗЖВ
ЖАКФЙДЖЫЛАЗЖЬЖЮЬКФЗЖВДЭЙКФЗЖЭЬЭДВИАЕЛРВЭПКЖЗИАВЮЭКЭЬЭЕФВЖЕПАГКВЮ
ЭЩЭЙЗЛКЕЖВВАЕПГДУЖКЛЮАЕГАЛИАЕЛРВАЯЛИАЕЗЖДАЕЛКЕЖДЕЭЗЖЬГАЪГЗЖЪКЖИП
КЖЕЬЖЩЕЖВЙГЛЮЩЭЗИАЪУВКФЪЙКЪАЯЖЙКЖГПЛКФЬЭИЮГЙЕЕЖЫНЪЗЖГЕЖПФЯЛИАЕЖК
ЪЭЯДЭЕЪКИВКАИЙЪЭГФАПЪЙКИЭКАГЕЙЕВИУГФОЭЖЕНЕЛГЛЪАЬЕЭЙЖДЕЭЕЕУЭЗИАЯЕ
ВАДЖЭЫЖЛЙЭИЬАВЙГЛЮЩЭПКЖХКЖЙЛЬИФЙКЖЩЖЦЙЬЭГГЖЙФЙВЯГЖЕЮГВАДЫЖГЖЙЖДЫ
ЬЭКУХКЖЕЫИЛЯАГЙНКАЫЖЙЗЖЬАЖКИЖЬЛКВЖЫЖЫИЭНЕЭЩУЪГЖДЖГПАНИУПЖКЪЭПГЭД
ЛЯЗАЕЙФКУЪЭИЕЖЗФЕЗЖРЭГЙЗКФАЛГЖЮАДЭЕЕЬИЛЫЖБЬЭЕФЗИЖЙЕЛГЙЙЫЖГЖЪЕЖЦЩ
ЖГФЦЙДЛКЕЖЗИАЗЖДАЕЙЭЩЭЪПЭИРЕАЭЗИЖАЙРЭЬЙКЪАИЯДУРГЭЕАДЖАЗИЭИЪЕУЩУГ
АЙЪЭГФАПЭДЪЖРЭЬРАДВЖДЕЭЙПРВЖЦПИЕЖЗЭКИЕЬИЭАПЙВЯГЖЕДЕЭВПЫЖГЖЪЖЦИЕЖ
ЕПАЕЭРФЫЛГКФАЪВЖЫЖКУЗЖРЭГВЮЭКЙЕАЩКЦРВЕАЬЭЬЛРВЗФЕАОДАЕЭЩУЪГАЖДКЛР
ВЭАЫЖЪЖИАКФЕЭПЭЫЖЖКИЖЬЛВИЖДЭВЪЙЛЪИЖКЕАПЭЫЖЕЭАЯЪЖГАГЩИКФВКЖЪЙЭДЛЪ
АЕЖЪКЗИЖВГКУБДЛЙФЭКЖАЬЭГЖЩУЪГЖВЕКАЗФЭЪЕЭЯЩЭЮАК

   (b) Расшифровать текст:

ЕБЖЖИЕЛЙИИНЫЩДЬЭЖЙОВЧЛКЮИТВОДЛМНЖИЗЭЖГЪЫРЯЕДДСНЖАИНГГФЬГНАЙСУЛКУ
ЛХЮЖЗЯЗНЯАКИЙЭЙЗРМЖНЕХХБАКХГЭНДРАЖНИДВКЖИНЕКЧПРФЭФЦХОЗБМЮПЖНИДВК
ПШЖВБНМДЛЪОЦПВЗБЛЗКВИВЩПЖЩМРОЛАКЮДЕУВФЕЯЮИНЩЖЭФУКАОЦУОЖСИФЛЦЩМРД
ЕУВФФККЯИВГДПРФЭФЦЩПЖЭЖЬЙАМИПЛЪСИЖЕГЖМЗЮЭЮЛХЙЭМДКПЖЮЖЗОКК3ЗГЕЧПУ
ПАФДРЯЗКЮТЕЭЕЙТРЙБКЗАВМИДЩДКБМЕЗБЕСЛПБЖХПУКЫПВБОДРАЖИЗ3КАНЙТЛЙДЕ
УПИПЮРЙЛАЯТГАЮЛДЛЭЙЯЕЛЬКЬПЕЭЛИФЛДПИФЯЭУЕРКЙАЛМЛБПЛОВРЖИАФККБПЫЗК
ИСШКПЯЗКИЮВРЮУУГФШГВЯЪЩДБКЙЯЭТЬУЗИДСНЯЩБТЗКЙОЬЗПУЗАЗХФНЖЭЙЩБЛУПУ
АЗЭЙЖЭКЙЛДФЬГНАЙЙЗНЭИЯПЕГНЬНЕОБЧФЛКБЫЗПВЙЯСНЖЕЮЗПЙЖБНЛЕНМКОЕПЬОК
ЭМНМРЪЧЖПВЬАВФВЙОВУСВТВАЕЯЮИНЩВКЭЖТЖУЯЪЩЖОЬЗФГКЫТБЖЮЬЪЕЙШЬЯПЛИВП
РКПЭРПЖЮЫЭИИНМЗНЯОЦЗАЖОИФФЙКМСНЪДЕУЗАЮЗХЕЫЙМЮЕППВЙОКЗЯЕЛЙДЭРИВКШ
ДНЛЖПСЛЗМЯСЛИПСЗКАЪДРЙЭЙЮППРДИПКЕДБЭЯГЯККЮУАЕУРРБЗЮКЯДЖХМЭОКПБИБ
ВЩОВГЕРКЛЮВЖЙЭЙЮРЮИКЙРГГКЬФЩВЖЧФЛЪНЫРАЗМВПВЙЛИМЗЖИНЖВГПЛОВЦНЙТЛЙ
ДМЮЯВККРПВДПУИЖЮПРЮТНЗКИЭИНЩПЖЛИУОЖМВНОЙЗЯМОЭБЖКЯЕЧСЗЙЭЯИКЯЕДЭПП
ФДССНЖФНГШКШЖРЕДНЯМРЕАЗФЛДДЬПЕЫЙМЮЕПЮХУИЛФЕОВЕНИДКАИЗКВДЮХФНСЙЖЗ
КЙЮИЛВЬДЗУПЪБЗПШБЯЕЙЯУДБДЛГДМЗАЖЮИТЕКШЛМДГКЗОКЭУМРТЖОВФВГБДУВАЮЗ
ЭФЯЖИНЛКШВИВГБМЗФККЫСНАОИОЮУЗЛДЕЬБМЗИЭИММИАНЖЗЫЙЛКРОАОЦФЛПЙИФЗ3К
ЖКИЛЕМЗМЭОКПБИБВЩФККЧФЛЪЧБФВГДЬЭОГБДУВЭИВДКУУЯОМЖЭКПЕГДЛЮЯЭЗВМЮЭ
АЫТКФЙЬРНЖОНПВЪДЛПВККЗДОЗКЫТКАЗЬЭВЫКЬЭНЛЯГФВЖЙЬУЯИЧЕРЯУБЭРЯЛСИДБ
ИПЭРВЪОКЗПФБВТДЖЕЮКПЭНЦОШЪННИМЖИВТЕДОИЖЛЩМИЗИАААЯНЛЯЖИНЛКШЛДЛЭЯИГ
ИАВ3ЗАЖНЖЗЫЙЛКРОАОЦКБЖЭКРЮЛВБМЛГКЕКЯУБЭРЮЖЯЛПЕДНЕ3ЗЙБЯОЕЪЙХЩВДДЛ
ОБЖЙЯЕЛЕБИЧЛКЙВМКЛБЛНЕЖЙЬУМИКЛДВИЗВФКПОИЯПЖЭНЖВКЛИЧЛЮБДФЛЩПЮЗПЪА
НТЗННЖЗЫЙЛКРОА

2. Разложить на множители числа:

   (a) 991475809602404273900693445347

(b) 65618887584025504697716829207191402634965793650784384928794 3

(c) 971462530321103730708682878868414248240893858439864587917121252749279575561111729120364589

(d) 113638317808744092720698244172474812119237296651819888167230612541084145552910919038633992971183801521424003701159640963 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 37070161213534939973666437616266161503352381989571110472443055484918377248953$
   - $e = 5$

   Сообщение:
   - $M = 13750416690051384713046244247509153863265164082946657429225714739626305028 90$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 32523855397738549766514583555595859734 9$
   - $q = 22523641604931690251795514750219996052 9$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 61588257907670484512445012274014903652494702914706874686428404669622604801 91$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 16285992384989322008168418832832169576 7$
   - $e = 3$

   Зашифрованное сообщение:
   - $c = 61181117756874862428712398533280279 44$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 23951728783124008925620386518286517270 1$
   - $g = 13289289048458427386147494244422376200 2$
   - $y = 15803217376731262787154675503043982104 1$

   Секретный ключ:
   - $x = 90565677121031119878930275110222393980$

   Сообщение:
   - $M = 53634034173549799328706032170214071420$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 30793005154354474613365411555156382911$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 21222959231182708226052885033206572489 9$
   - $g = 65786292629836647054285794400800110791$
   - $y = 11364352947231913286324729589407080162 9$

   Сообщение:
   - $M = 32680687368424150606058617483184619255$

   Подпись:
   - $a = 19949762821334645907422835136202346607 8$
   - $b = 20357663301130843872686447524688303055 3$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 541$
- $g = 178$
- $y = 529$

Сообщение:

- $M = 387$

Использовать следующий случайный параметр для создания подписи:

- $k = 497$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 17$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 58

1. (a) Расшифровать текст:

УЙИРЛИЗСЕСОЯРСТУЛХРСИРСТОЦХСЕФНСИЕСОСФДЮОЛСДФХУЛЙИРЮЕНУЦЙСНРРИПД
ЮОСДСУЕРРЮМУПНЛХХУФНЛИЫУСЕУЮТСЗРИФИПЦЪЫНЦЪБСРСХЕИЗОЛТСПСУЬЛОФЕЫИ
ДОЖСУСЗЛИФЗИОМХИПРИХНЦБПЛОСФХЯТУЛНЙЛХИТСЗРИФХЛФХНРЕЛРЪМРИРЫИНКЩН
СИТЛХЯИФСШСХСМЛФТСОРЛОИЖСЙИОРЛИШСКЛРЕЮРЦОЛКФХЕЩЫХСЧЛФХНРТСЗСЫИОН
РИПЦЛЕКЖОРЦЕИПЦЕОЛЩСАШИФНКОСРСТХЯХЮЕРЫИПНУБСХНСОИДСЖТУЛРИФЕСЙХЮМ
ПСМПЛЖРЦОКРЪЛХИОЯРСЛСХЕИЪОТСЖСЕСУНСБЕСЖСУСЗОИХОНСРСТОЛНОИЕОЫЕЮУР
ЦОДДЦЫННПЦЫНСПЗПЛПСРЦЪХСЕЫЛЗЪХСРЫЛСХЕИЪОШСКЛРТУСЗСОЙЛРСФНКХИОЯРЮ
МУКЖСЕСУФХОЛДЮОСНЕИЪИУРЛКЕСРЛХЯЗТСТЗЯРИЕИОЛХТСТЕЖСФХШЪИУХЛРТСЖСФ
ХИПСОЪЛЗЗЕСКУКЛОПСМДУСЗЖДЦЗИХЗСЙЗЛНДЦЗЦХЛЖУЛДНЛДЦЗЦХЖУЛДНЛДЦЗИХЛ
НЦКСЕХИТИУЯХЦХСРПЛЖРЦОСТХЯКХНРЛХСТСУКФТЛРЦОИФРЛЪЛМШСЗЛХЕЫИДОЖСУС
ЗЛИКЕЫИКЗСУСЕЯИТУЛФЛШФОСЕШСРЕКОФХНРТИУИНУИФХЛОФЛЕЮТЛОСЗРЛПЗЦШСПТ
СХСПТСНОСРЛОФПРИЛЕСУСХЛОФРТСОХЛРЛЪИЖСРИПСЖХСЖЗТСРХЯЛКАХСЖСЕСУСЕФ
НСЖСУКЖСЕСУРСТСФОИЦЙЗСЖЗОФЪХСЗИОСЫОССЗИОШЛЩНСЖСЕСМФНЕХСЕУИПХСОЯН
СЪХСЦФПЛУИРРСЖСТСФОИДЦРХЖСЗФЕИОЯЛЪФОЦЫОФЕЛЗСПДСОЯЫСЖСРИЦЗСЕСОЯФХ
ЕЛСРТСФПХУЛЕОФТСЗСКУИРЛИПХСРШСКЛРХСРЕСЙХСЖСТСФХСОЮМЗЕСУЛОЛТСХПСЫ
РИПЦЦПИХРШСЗЛОФЕФХСУСРИЕФХИТЛЗОИЪИСХЕФНСЖСФИОИРЛЛСЪИРЯТСШСЗЛОРУК
ДСМРЛЪИФНЦБТУЛФХРЯРСЗИОХЯДЮОСРИЪИЖСРИОЯКДЮОСЛТСЗЦПХЯСТУСЗСОЙИРЛЛ
ТЦХЛДИФТСНСМФХЕСФЕИОЯЛЪСЪИРЯПИРКДЕООСПИЙЗЦХИПУФТСОСЙЛОФРСЪИЕХЯЛО
ИЖРОЕНЦФЕИОЯЛЪУИЫЛОФЦДУХЯФРТИЪЯШСКЛРОИЖРТСОЦФНСУСЕФЛКДКШУТИОЛКФР
ЦОННЦДЛХЮМТУСФРЦЕЫЛФЯТСЦХУЦЗСЕСОЯРСТСКЗРСЦЕЛЗИОЪХСДЦУЦХЛШОФСОРЩИ
ФЛОСФРИЖОИЙОСФОИТЛХИОЯРСМТИОИРСБРРИСДСКУЛПСМФХИТЛОСЫЗЛДЮОЛКТУЙИР
ЮУФТОХЛОФФШСКЛРСПНСХСУЮМЕКОФРФХНЦБЦПИУИРРЦБТОХЦЪХСЗЙИФЕИОЯЛЪ

   (b) Расшифровать текст:

ЯЦЙНПЮЙЛЪЧЯИЕУТШЧЙНЗГХМШКАЙНКРЭЧБЦГЮТЙЩНДЫВЧТЩСИЩЙАФВШДЮСЛНРТЮОХ
ЗЮМВРОБАЕКПЯЖККЭВПРАНЭЙКЪЗБУВУКУЙВЦПТЙДЦДВОЛЛРЧЙЙХУГЖМШКШСИЩЮЭСВ
КУЦФБНЩЮТЖЩМЬТКХРВЦЕРУЫЛИЯФЯЙВШРХМПННЩОЛХЗИСЛШЖМЕРМХГЙВЩЩВЦЕЖПЯУ
ЛМХЭНТЦТЯЬВХЮЫТМШКТЖЕУРЮХЛЩФЯФЛХЭГЖЛРЧБТБХЭЖСВЙХХЙПУКАФВЧФВЦЯРЙХ
ЧЙУУУСВОПЯХПРОГЧХТКЮТЖХЗВЧЙХЗУПОХРШСКШДЩТЮШЙЭЯОУЗЪТПЮЩДЖОЪДЯЖИЯФ
ЯПЫЙРУАЙЦПЦХИРЪЫТЙНЕЯЦНЦПЦЦЕЯФЯТКЙХХЙПХПЦЙОФРГФВЪЮЫОКЙНЧАЙЦНЯИЛЛ
РИЙИЦДЦОФРУГТОНТХЙФХРАФЕППЬХЯЪРЭРНДЗЩЖКЦДЮЙЕШЗЙМИЩРХСЗЦСЩХПДМТЦЫ
АМЦОЗФРЧСЛТТВСЛШЗИМЯНЗАФЛЩТЯИЕЪЗЬАОТРФТЮУЕЯХИЦДЦСЕЧРЫЛИЧКВАЙЦОБА
ЕРДЮТЯХЗЫТПЦТЮЬИНЕЯХПЦННЧЮНЖЩЦВУЮЮЯЙРФБТАЪЗЬАКГОИЦЛХЗВТЙХЗУПОДДД
ХМНЧЦЙАЦКАФВМНВАФЫДВЦЯФПЦККЦЕЯХЯЦЗФТОНТХЪОЦДВЙЫМРУЙНЯКУТОЪКПРЛУР
ХТОЪКЩПЫЙДЩХЛАДТФЕХЭЭУЛФКБМИЩДАЙНКЭЦИКРОЯЙАЦДМЛБЦТЯЖИНПЩМЯХМДЛЙР
ЩУЯАЦДБМЯФПЦЛМЦЗХМКЦМВОДУЮЙЪЭСЦЦНХЖБЙЕЯПХПВОНЯЕШФПЦУЛЩЖЩЦЩЪЗТУЛ
МТЦХПМФМЧГРГЦЛПЦЕЯСЗППЬЙЗЩЗЪМЯХЭИЧЙНПГОЕЩКХМПКЧЬЙЮХРЭРАПКЮЙМЦЖЫФ
РУРЭМХЧЕЦЗЛЧРХЛЙТРЭЧЯЩКЬМОГЗФТНЦДЮЯМЫУЫНЛХУЦЕВХЖДРВЪУХФОТЗГХОУКЙ
ОЛФГМПОЯУГПЕКЩГТЮЭТЮМПДДВЙНМШЦЫРКУГЖЛХЗАФЕППЦСКЦЗВЦИЧТЯХЕЪЮШЬЯЙТ

ЩСЕМРТФШСМЯРВХЖЮЦОЩРФПОРУУТВСУДУНЫЕЩФВАКЬХВЛРЯХЯЦГЯИЕЪЮЙЖЮШКЮУНР
ЪЦПЗЦОЮЙЛХКШЮЯРНФПРЙРЫТВЩРЧПВХКЦТПЦОИЦЛЩНДЫЕУРВАЙНИХЧКФКАФЕППЬХФ
ЪРТЯИТТДЗЛФДЩСЛКФЩУНЦУЩПЙНПШЕШЪЮЯУНЦЪЦИХНОТЧБЫЩЩТПЧТЩФЛМЭЮЙДУРАР
ПНПЩХЗШЗЮСЛЧТЯХПРНЦРРРПЙЧОЩРБЧЕШПДРКЦАЯЦКНЕЯУЛУХИЙКХХПЖЗУЗУЙПНЗФ
ТЯРЖЦПБЦУХЧЛЩМЯФЮУЗЮСЛЛРВРЛУАТМЕЦФУЙНЛПДЦЛСНПЕЯРКУЙИРМЯИРАПЯМДКК
ЮПОКРЦЗЛХЗВЫОЪПЯЗЛЩРАЙНХКЫЖОТРБЙЯГЙХТНЦДЦПЕФРФУВШЗТФПДУЮРЛЖМУФПР
ТДХКНФЦФМНПЩЙЙЦИЩИИЦФУЙПХСЯХИХПЯЙМРУНРЛХЗВРВХЖЦЦЩЩКВЦНЩЮШЗИЫЪЩЦЩ
ЧЗИПЩХЭЦУННЖИЧЯЩФУМОКУЩПЕЩРЪЙАЦТЯЖКЦЛЩ

2. Разложить на множители числа:

   (a) 85184530518276691428318185865 7

   (b) 80244525609520796909848752085253795463916051548708888991 3957

   (c) 16624016679301624449722939383703226060840963265650545318277372888700021349126311789209852 31

   (d) 14399554023603960701146968331225484776108691446563460992570583091217041385412056482583825956554999086265761282609448391 17

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 45678190181380092557012817093694564419040744775634464299665886798735653197923$
   - $e = 3$

   Сообщение:

   - $M = 57406460582060937860592151676389161273335471142997967473933641965285503732 56$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 171488639595356867370118470436959888407$
   - $q = 22691862210636440180598536962245856821 1$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 22172436810209566912731521780741843131205125870615030419469193344479261871789$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 176308388881674611028105750061685774209$
   - $e = 3$

   Зашифрованное сообщение:

   - $c = 41564558917312110878425011174161491456$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 27491907012900475799121364273677068886 1$
   - $g = 29188809639468821976935134626405326 37$
   - $y = 15196756904329783067236847144497710979 7$

   Секретный ключ:

   - $x = 11948347146643272860677469977528832367 6$

   Сообщение:

   - $M = 15098367738902603801296965893786641768 3$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 25075785710024591637960483472583641610 9$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 20032464629637162671589989416521478966 7$

- $g = 38317251852932549987345705270051810 73$
- $y = 12983778321078878428370015930854437 9974$

Сообщение:

- $M = 15248179325112848331154926235192139 0983$

Подпись:

- $a = 71111640457274646898724810855837034529$
- $b = 74488004708598456007562255983123120265$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 883$
- $g = 839$
- $y = 683$

Сообщение:

- $M = 424$

Использовать следующий случайный параметр для создания подписи:

- $k = 349$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 3x - 4$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 59

1. (a) Расшифровать текст:

СУЧНХЦФЧШФОЦКЩЮУФОФЗФЮСЧВЧФТУФДРРЗБИЛРЗБСНУРФТОУИСОКОХСЮРУРЦБИСО
ЧШФСЭШФГШФТФПОИУРЩНТОЭЧЛЙФКУШРНЩЭОСЧЧРНСРФТЛУКУШЮХСЮРХФНФИОЗЦОУФ
ЗЛКШВКЙКЛМЛТЮШЩШИФЮСКЛИЩЮРСЛШФЧВТУКЬШОРЦЩЙСФСОЬЦЩТУЧЧИЛШСФЦЩЧБТО
ИФСФЧТОЙСКРФНЭЛЧУУБТОНЩЮОРФШФЦБЛЩУЛПШРОЙФЦЛСОЧХЛЦИФЙФИНЙСКФУУЛФЭ
ЛУВТУЛХФУЦИОСЧВЧТФШЦЛСУУЛЛЧХЦЛКЩЗЛМКЛУОЛТЮИЗЦОУФХОЧСТУЛТЮЩРХОШУЧ
РЩДКФЭВЧФИЛЦЮЛУУФДКЩЦФЭРФДТЦВОИУФИУЧЛСИЩЙФСОЧШСЮОШВТЛМКЩШЛТХФКСО
ЯОИЧОСОЧЛЙФЦФИУУЛИОКТЩМИШФЦОЭУФХФЧССНУОТХСЮРЩЧРМОЗЦОУЩЙФЧШОКЛМКЩ
ШЯОХЦФЧШБУЩШЧСИЗФЙЩЩЭЛУВЛУЛЩПКЛШЩЧХЛЛШУРЦОЭШВЧРХОШУИЧРФЦЛИОСЧЧФХ
ЦФИФМКЛТБПРЦОИБТЧШЦОЭРФТЭШФГШФТФПЗШДЮРЧРНСЛТЩМЛУРЩЮУВЛКИУБТКИУФХ
ФКУФШЛЗУЛКФНФИЛЮВЧЧСБЮВШБИЧОСОЧЛЙФЦФИУФШИЛЭСОИУРЩНТОЭЗБСНУШЧСЩМЗ
ФПЧФСКШЩЮЛРЩЭОСОХФСУФИФНЦНОСРХОШУЮШФСВРФЧСИЭШФЧФСКШЩЭОЮВУООТЧСЩМ
ЗУЛКЛШЧУОШБИУЛПШФСРЩУЛИЛКЛЮВЧОКЛСЗБКФТКЗФЙЩТФСОСЧШРЗБСФЗБСЩЭЮЛКФ
ЦФЙОЛЙФЧШОТОСФЧШОХЦФЧОТНЧШФСТБЧЛСОФЗЛКШВИЧОСОЧЛЙФЦФИУУЛЩТФСРСУОУ
ТОУЩШЩОФЧБХСТЛУИФХЦФЧТОРШФТФОЦФКОШЛСОМОИБСОФУОЙКЛМОИЩШОРРФИФОЫЧФ
ЧШФУОЛЩЧСБЮЭШФЩЗШДЮРОШЦОЧШКЩЮРЦЛЧШВУСЛЙРФСОЧРНСФУИЛКВЛЧШВМЛУЧИЛШ
ЛЗФЙШБЛСДКОЩУЧТФПЗШДЮРИЧЛЙФШФКЩЮФКУКЛИРХСЮРКЧСИЗФЙЩМОИЛТХФТСЛУВР
ЩФКУЗЛКТЮКЛИРУИБКУВОРРФЛЩУЛПХЦОКУФЛЭЧШБПЙЦЛЗЛУВКИЛУОРКСШБУКЛУЛЙХ
ЦФЧШОЗФЙЧЭЛТИЗУДЧЫФКОШВЫФЦФЮФРФСОУПКЛШЧКФЗЦБПЭЛСФИЛРШФЧОКОЧЛЗЛИК
ЛИРЫИЛРФИЛЭУФПУЛИЛЧШФДИНЙСУЩСУТЦВДОИУФИУЩФУИЧХФРЦЧУЛСОКМЛЧСЛНБРХ
УЩСОУЛЛШЦЛСРЩТУЛЧШСФМСВЛЛОЧХЛЮОСХЛЦЛТЛУОШВЦНЙФИФЦЧСБЮСЧРНСКФИФСВ
УФУЛРЧШШОЭШФУИЮЩРЦЛХФЧШВЧФЗОЦДШЧУХЧШВЗЮРОЦЬБФШ

(b) Расшифровать текст:

ЧФБЛДЩЦКЧДОСКШИРЖБШИДТЛХШУЙЙПЮЧЧЯЮЫКФГФЫЩПНГЕЦОММЕЦХОПЮКСЖЪЭФМУЬ
ДЪАДХННСШЪШОПНЙДЖХПЦЖЫЗПФДХМГЮИЦСНЙЫЪЙЙМДЪОМВБЙЯБРИССЧЙШНФБФГЦНБ
УЙЧТНТЙОЕБЦДУЧУПШЧМНГВЦТОКЫХЙМТДХИКЙДУАЙХЮЩОПШГГРКИЖПТИЙСЧФКЙДММ
ЗЙЗРПДШЙНЗКЧДКСПШАПЖБРЧЫИОХЧГТОММЛЙМШЮФУКТЙЯМЗПЭЦФБФЧЫФЯСАРЙОХНЫ
ИЙВЫРЛЮМЗЪМЖХИЦФЧМЗЦИБЧЬРЦЮЙЫУМЖХЯЪНЙМШЩМЗПЗНЗКЧДКСОХИЯХГЬДЪЙЗХИ
ЧФЮПИДХЮКДЩЦДСЕЦУАГЫРУКШДКЙОЪЮКСЖЪЭФМУЙЭУХНХЧЦВДУОЫЫОХЧННЙМЧГПКШ

АЫЫЙХДМСКРЮКСЖЪЭФМУХЗЪЖФПЗДУКТГГРСХЭРСКУИЦЦУШЕЦХЗТЭХРДЦБАОПОЕНФЮ
ЮЙУСУЩДЙТЙФЫФТЯТГЩУКЛЗУЧФЩТКХДТЮЩЙЯХЖЦЖЙЙДПЖМЩЮУХШЛДФТЕФЫЫХЛМШХМ
УМЩЦЖЧЙЫМЦШХИЧТЛЛТРМПОГУЫОХШЦЖММВНЙКЩЗЫЦНЩШРЕЧТДЫМЮФАЫЛИПНЩТЮМПХ
МБПНЪТЛТОТЕЧТЕЦИГУАЦРКФЪЦЗАТЗДЫОХЧГПКИВХЧОУЙОЙИПЕШМНЩЙЧМЗСГНРПШЪ
ЦУМХЗЦРЙХЮКСЖЪЭФМУЦЖРЗКЩДКМЗШАХУАМГРВКФГРРЗХГНХИЪИРПНПЧЦИМХДЪЖБЮ
БЩЖКМЯУВЭХЕГЦЙХЯЩТВПИНПШФЮЮЙНТСААОВВЪЧФСЧЙЯЙЯЮКЛАЪВУМЛМНРЦКЦЮЪАН
ХБЦРКЕАТТОЩДЛТИХЬНЦЛЧДРЛКРИРСБШНЩЦДМИЦМКЩЪУХОЧДЛМЕЦЖРОГЙЕШЙАГЗЦП
КУДЖЕЭУЕНЫБРГНЦКЦЮЪАОХЕРЦШЬШЦФКШИЦРДЙБНКЙПАЦРАТННЗКНЧГПКЩЫЙЙГЦЮШ
ЦШЦБАОПШЕШТНПБТТИМГМСОЯЭЯЦКИЫМСАМШТУМХЗРИБТШЯЧЗФЫЧТЖУСХЙЮХЖЦЦДТЮ
ЩАДЙГТЧГУЮЯСБИСУУМПЩЦЦКЙБНСЖЩАЦЖКУЙКТЛЧДЩЧКФЭЧЧОТЗРУМХЧЦФИХИУЫОХ
ИЦТУМГДСБШАУИЙХЫКХДТЮЩЙЯХЖЦЖЙЪШРИБТАЦЖМШИКТНЙДНЗКУЙОСКОГЯЦКФЮЯЙЯ
ХДЪСБКДХМАХЧДЙОШЕШЙЖЧИРПНЙДРЖКЦЖЦХЧПЭКЙЗЧЫЯАКШДУЙЙВЛЦЗПЧМЭОКЩДШЯ
БСЙУМЙЦВЬМЗХШХУМПЩЦЦКЙБУХКЙЫШЬБФГЦТНХЧНСЙВВЦЕМОДФЖКЙЗЖСКЮТКХДТЮЩ
ЙЯХЖЦЖЙФЫФТЯТЭЩСПЩТРСДСАХЙИХЩУИККЪЪАНЮИЦЕЧЩАЦЙЭВБЦЖЯХБЦЖБМЫФЧВХН
НРЭВЫССБТТПЕЧТДПСОГГМФПКДСИБФТКТГЙЖБХШХИЦЕБЛГРТЙЪШРИБТЮКСДКГЪАДЮ
АЦЦКЧССЖЧЩЗТМЮТЮПУПЯАРЦМЦЮЯОДСВЫЬЖППНУЖПЧЙОДПЗЦФЮШАЦЗКЧДМЛЛПЛХСЧ
РШХЙБЧЫЙЦДЯАФМУЩДЙЯГФНРПДДИ

2. Разложить на множители числа:

   (a) 949065978509881484787977642191

   (b) 737366396512465635998274311730228208251478680547368510843017

   (c) 166114420743496849615429198066746504275193157584841485129049400515715855072338264371593222 9

   (d) 134088488575407360325487773381154249638623087241304410663645832616365556583250939513618088366924079807830961068816134191 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 59740157383275391798426364154236755376532316631592202380938050021694890689581$
   - $e = 5$

   Сообщение:

   - $M = 48339372961748298425824745208042160743048690592902076889283648765728261362496$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 190746151808658777532295123957906925671$
   - $q = 184928118136282424531658935699606054993$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 97223255739170932224285735267819340478134889237648849012247920014772408732 82$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 143289379513442754902449512364152452969$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 84582593585637715923681644780277311434$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 22775009432514704198488438883970281 4941$
   - $g = 59859605060653528182897076308684426227$
   - $y = 10263202274531145681208950845963675116$

   Секретный ключ:

- $x = 81145287638518551034653610177543455362$

Сообщение:

- $M = 17432879218498457259262951561009335137 2$

Использовать следующий случайный параметр для создания подписи:

- $k = 67655104005724833328205550831071499901$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 26283811450451895862961583274513871 1109$
- $g = 72445725719186425660937211003996621572$
- $y = 25647256347988401844257173859258200 7871$

Сообщение:

- $M = 44751138674116698722813412225350554393$

Подпись:

- $a = 15590415130740960205543808380552892 6840$
- $b = 18499091360953061926812416563994156911 1$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 997$
- $g = 645$
- $y = 530$

Сообщение:

- $M = 227$

Использовать следующий случайный параметр для создания подписи:

- $k = 371$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 14x - 15$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 60

1. (a) Расшифровать текст:

СОЧЛРМЫХЙНЫХМЩУТИФЙХЦУЙЦФСИФЙМЫПЙОХЙНМЖСЯЫУТИЖНЦЙХВИЖЬМЬУЗМУТИЖН
ЦЙУТИЖНЦЙУПЬОТЦСЙХМБЦМЬУЗМЖЫЧПСУЙЦФСИФЙМЫБЦТЗТТЦЦЙЕСЙТКМИПООЦЙЕЙ
СЙХТЖЙХЦСТИТЕФТПЙОХЙНМЖСЯЫТСЛИЧЬЙЗЧЕХЦЖТММЛЗЖФИММЖЯУМХСТСМЖЗТХУТ
ИЕТЗСЙЖЙФЧЙЦЦЯЦТЫЦТЦЧИКЙПЙЛЙЬАМЖСОЧЛРМЫЖУТПСЙХТЗПЬПХХХЖТЙВХЧУФЧЗ
ТВМУФМЗТЖФМЖПХПЯЬАЦЯЖХМПМХЙЗТФТЖСУФЖИЧЗТЖТФМЦУТЙИМСОМШТФРПАСТЛУФ
ЙЭЙСЯЖЖТМСХОТРФЦМОЧПЙРЙКИЧЦЙРУПЬОЖЛПЧСХСЬМЬУЗММТЦСЙХПЖЫЧПССЙРТЗС
ЙЛХРЙЦАХЬЖЕФМСХТЩФСМПХЖТВЖКСТХЦАУФМЖХЙРРТЙРЧЖКЙСММОЖРХОЛПТСЙНЩПИ
СТОФТЖСТСЙРТЗЧСЙЛРЙЦМЦАЫЦТСУФХСТЖЯМЛЖТПМЦЙЕЙХУТОТМЦАХУТИЖЙФЗСХЖЬ
ЙРЧХЧИЧУФЙИТХЦЖАЦЙБЦТМЖСЧОЧЛРМЫЧБЦТЙЗТИЙПТЩРТНЕЦВЬОЖТЛФЛМПОТРЙСИ
СЦЬИФЛЖЙРЧКМКЙССЙЙИМСИЧЩМЙИМСУПТЦАМЖСОЧЛРМЫЫЦТЦЯЛЙЖЙЬАХЙНЫХФХХИМ
МЩУТФЛСЯРЧЗПРСЩПЙЕИСЖТИЧЫЦТЕЧСМЩИЧФАЦТУФТЬПИУЧХЦАТЦЙЪЗЙФХМРСПТКМ
ЦССМЩБУМЦМРМВЫЦТЕРТПМПМЧЕТЗУФТЭЙСМИОПМХАУЙФЙИПВИАРММЖСОЧЛРМЫСЙЛС
ПСЫЦТФЙЬМЦАХРФАМЖСТЖСЕЯПЫФЙЛЖЯЫНСТЕПЙИСРПТУТРПЧЕЧФЧЦМЩПОТРЙСИСЦЬ
ЧХУТОТМПХАМЛХЦЖМПСХИФЧЗИФЧЗУТЪПТЖЦАУПЬОУФМСЙХПСРСЬМЬУЗМРЯЖЯЬПМТЦ
ОТРЙСИСЦУТЖМИМРТРЧУФМРМФЙССЯЙМЖСМЗСЦАМЫСХХТУФТЖТКИПООЖРСЙХЦЯИСТЕ
ЯПТХОЛПЙРЧХЙФИМЦТИТСТХМЦАССХОТРЙСИСЦЧУТХПЙЦТЗТООИПМРСЙХПТЖТЦТЗТС
ЙИЙПЦАООЕТЗХЖЦМЖСЧОЧЛРМЫЧЦТЗТСЙЗТЖТФМПТЦЖЙЫПТСЖХМПМХЙЗТФТЖСЖЯЖЙИ

ПЖХЙТЦРЙСТСЖХЙРМФХУТФИМПХАЕЙЛЖЙИТРОТРЙСИСЦЖУФТЫЙРХПЖЕТЗЧЫЦТЖХЙЦО
ОТСЫМПТХАХБЦМРХПТЖТРТСУТЖЙФСЧПИТРТНЬЖЕФМСМТХЦПМХАСЙИМСЙСЬЙИЙПТБЦ
МРОТСЫМЦАХСЙРТКЙЦХОЛПЙРЧОТСЙЫСТТЦЖЙЫПЬЖЕФМСЖЯХЖТЙВОФТЖАВЕЧИЙЦЙТЦ
ЖЙЫЦАРСЙЛЖЬЧИЙФЛТХЦАСТЛСРМЖЙФТЦСТХЦСЧЦУФМХРЦФМЖЦАСЙХОТПАОТИСЙНСР
ИТПКСТЕЧИЙЦУФМЦЖТФЦАХИТХЖ

(b) Расшифровать текст:
ШУНШДФЗЭНЕЩЛКЗЭФРРЮНЮПЖЮЬБЦРЖВЛЦФКЕЗНМЛЯЦКМЗЮОТМПДСКПКЬЩГЗХЯХКФБ
ЕВПХФЯСПРЮНДТТКЮУФЗНЗИВФПЗФЬЮЙЯЧФНДЗЛХЙАЯИРУЙЖЛХЗЙЫБРРОЙЦЗКОЦЧТЙ
МЯРПТБЙФЦФЙХТЗРМИШСРОДЩЙОМЦОЗПКЬУЙРЗАУЖЭЗЬБКЧОЦОЧОЛКФЦФДМВЦУЙЯДЗ
СКЛСКЖЙВПХЙУНИЦФЮИИРДНЯЗКДБЕОПХЪЙЛХЗИЯУШДКЕУКПДЯКШЪДЖФКЛЭХСУОЙЯЙ
УТГЮФСЗЙЯЛЧЕКЛШТРЙЯМКНДМФШПЧЗОКДЖИШУТКЖЛЮЗЙЯКЗПКЫБРСКЭЦШИБЗЧИТПЛ
ШНАМБСШМДЛСНДЗВЧБДКЖУККЙЯЧТЭБЗФЦНАИЧЧПЧЯУЙЗВЮБНПБМЛХСБЕОЗРБИМНЖЙ
ВЛУСНЗФЦФБГОЬХЮЛШЗГЗЭФХРАЗФИРУЯЧЧРЗШЗНПКСВФТКТСТЗГЖЛЧПКПФЧЗЗНМКД
ЧЮШНКГЮФСХЖДКЗЗМЦТУРОЬФХКЗЛВНМКЖУКДДЕЧПСМЕЧЙРЙЯЧКПДЯТЬФКЗЮНМГДОТ
РУЦДЗЭНМЩФКЗВОМММЯХУУОВИМДЙЛОРЮЙИЧЦРЭИДГНДСШУРЖИСУММЯХУУОВЦМЬББМ
ГФЙЯИКЖКЖБКНЪЮОСЭНЕВЬФКЖЦБКЮЗФЗПЙЯЩЦСБЯШЗЭБПШБХВЛУШНИЯУФРНЙЛЭПКЮ
СПСМЕЩТЗНДФРЮЖИУЦФЮЕЛТКЕВШУФУЛЗХРНВСЦМЖИТКПАЗШШХВКЧЦДБМСУНБМЛРСК
НСНШБДРШУЗХЮРЩОИНУДПМТКПКЛШТРЮВСЦМПЮИАУЖБСНДЙВЙТФШВЭЙРЯИУСЗЙВИТМ
ПБТНЩЙЬСШКЛИЧРНИЯУМДИВХШЕУЙЦНЪБЕЩКЧЗЕОСТШВИТРЮЗЧФТКЛОРУНЯЦЙЗУЗБС
ФМЯХКФКЖУКХНЙЛРРОЬЛЬНДЬУНЕЙМВНЩАИЦУЕЮИЦКПЭНЦИРОКЛМПЖКЛФРНМВУММНМ
КПЛЕФЪРЛЯШХПАКЛНЩИХХУЪЗВУЗНЮИНЗЭФЯУНЗКЫЦМРЮЗУУЗЛКОХРАИПНХЖКЛФНБЗ
УУЗУЛШУМКЕФСФИНМКФКЕХННДЛВЗУБАОЧЗЗВРХЗЛИЧЧКЯКУНЙКЗЧЧРЗЬЦШИШЯХШЪЖ
НШШЖЛЯЦКФХВСНПЖЗЩТЗЖИТКПАЗШХУСАОЗНЛЯЦКЖНЬФНОИЕФЬКНЕЛТПЧЖЧЧТКЯТЖН
ДБФЦФШИХЦПКЛШНРАНЮКДЗЕЧЧТКЭФЗРДЗЗУЖМИЧЧКЪЗЛУГЧДУУДБЗУУЛЛИЧЧЗЛВУК
ДАЕВТЗИКЧЦФКЗОНРОДЦКСКЛШНТГФЛМИЗВЭКНКЬЛПЖЮЮЬЧЮЮЯЦЪОДИУНМГЕФЦМГДО
ТРИЯМЙХДЖОТЧКЮОРКНЦОЖЪЖВЦЫЭЖИШУТЧПСКЕЖИТУИЙИЗАНККЧФРГЗШБСКВЫХЭНЦ
ОСЪЛДТНСКДФРЩЙЖРУОБЗКТФКЫФЭЗЗЛИУЗЮИПЦМКЭФ

2. Разложить на множители числа:

(a) 969795026024400328764103538461

(b) 113545028288643857241105121713035437675695916825716204120638 9

(c) 125125464824331884237906968529743707154777189086693947533644575880598602906638225563846191

(d) 156991542727739191024511129487678055487744203381070667903249147139626387673060128565457588956299470946020857536923628481 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 32771482804884559509234444260813315320355991972999477587678927593850836214179$
   - $e = 5$

   Сообщение:
   - $M = 29393179982636032523772790094754505431543895070243456730148805949640284488 5$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 300159702670867556957807649380911248493$
   - $q = 196645031235482860375396843082742207191$

   Открытая экспонента:
   - $e = 17$

   Зашифрованное сообщение:
   - $c = 257759675134411013681608885642779199692681763127738997729403817469210721659 97$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 19497800401439481833468549942673369499 1$
   - $e = 17$

Зашифрованное сообщение:

- $c = 29597398131190523239141121350263409075$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 269153093898291166987643484914398075111$
   - $g = 218098197374990915626988042963399407315$
   - $y = 909701679627475707645753074383543953 56$

   Секретный ключ:
   - $x = 237255304561544602055540674737016508038$

   Сообщение:
   - $M = 437340174656316592507795753195155781 91$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 930742910841724966608146847611193352 87$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 268964197996947159732635144475991241327$
   - $g = 160342137021901562965093382192713813769$
   - $y = 201183333608894282723255573144911051645$

   Сообщение:
   - $M = 332707902873483698969043163668199254 41$

   Подпись:
   - $a = 174471143029384887637590594113916000267$
   - $b = 268882625108691101377747743879007219618$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 653$
   - $g = 595$
   - $y = 82$

   Сообщение:
   - $M = 219$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 41$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 8x - 13$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 61

1. (a) Расшифровать текст:

ЩГНЬЩЙЮЩЦХЦЮНФЩЮЯЫГЯЧЦТБЬЮВЦТГБДХДУЦХЯЭЩГНЯГЗЭЯЦФЯЯЭЯЦЭАЯУЦХЦЮЩЩ
ФЦЮЦБЬЮЯЯЮЫШЬЯВНЯТЯЭЮЦЮЦВЬЩЙЫЯЭШТЯГЩЬВЩУЮЫДШЭЩИЮЦАЯИЦЬШЮДЧЮЯЦБАЯ
БГЯУГНЯЭЯЦЭАЯЦХЩЮЫЦГЦБЬВУХЯФХЫЖАЯХЯШБЦЮЩЭЯЩЯВГЮЯУЩЬЩВНЮЙУТБЩЮЦЯЮ
ЯХЩЮЩЭЦЬУМФЯХДУХЯЮЯВЦЫЯЦФЯВЬЦХВГУЩЦЭЭЯФЬЯТМГНДХЬЦЮЩЦЭЯЦЩШЫБЦАЯВГ
ЩЩБШБМУВЫЯЭЦЮХЮГВЫЩЭВЦЭЦЪВГУЯЭАЯЙЦЬЯТЛУЩГНЯТЯУВЦЭЭБНЦЩУЮЯУЮЦЯЮУВ
ГБЦГЩЬЭЦЮЮЫБМЬНЗЦИГЯОГЯВУЭЩВХЦЬЬЯВНВЫШЬЯЮДУЩХЦУЭЦЮЫЫУМТЬЦХЮМУВЦЫ
ЯЮИЦЮЯЯГУЦИЬЩЯГХЬЦЪТГПЙЫЩЮЯАЩВНЭЯЯЮАЯТЬЦХЮЦЬУВУЯПЯИЦБЦХНАБЯИЩГУЯ

ЮУЯШУБГЩЬЭЮЦАЩВНЭЯХБЯЧКЦПБДЫЯПЩВЫШЬХБЯЧКЩЭФЯЬЯВЯЭУЩХЮЯЭЮЦЮЦВДХНТ
БЯХЮМЦУЙЩЮЦЖЯГГЭЦЮУВУЯПВЦЭНПТДХЩУЯУВЦЭУЯЬФЯВАЯХЮТЯФЬДИЙЦЮЙЦФЯШЮЦ
ГИГЯЮЭЮХЯТЮЯХЦЬГНЮЦИЦФЯАЦГБЮХБЦЩИТДХНГЦЖЯГНУМВИВГЬЩУМОГЯЭДЮЦТМУГ
НУВЫБЩИЬВЖУГЩУЦЦШБДЫДГМЭЦЮЬПТЩЙНФЯГЯУЮУВЦАЯЪХЦЭЫЩЮЦЭВУЮЯФЩЫГУЯЩЭ
БЯХЩГЦЬЭЯЮЩЬПХЩАБЯВГМЦЮЦЧЦВГЯЫЯВЦБХМЦФЯБХЦЗМЯЮЩЮВТЬФЯВЬЯУГЭМЯТУЦ
ЮИЦЭВГЭВЯУБЦЭЦЮЦЭДУЦБЦЮЭМДЭЯЬЩЭЯГЗЭЯЦФЯЭГДЙЫТДХЦГШЮВЯЮЭЦЮАБЯВГЩГ
ЮЦГАЦГБЮХБЦЩИЯГУЦИЬЭЙЮЦУМЪХДШГЦТТЦШТЬФЯВЬЯУЦЮЩГУЯЩЖБЯХЩГЦЬЦЪТЦШЩ
ЖТЬФЯВЬЯУЦЮЩЮЦТДХЦГГЦТЦВИВГЩАЯЫЯБЩЭВУЯЬЦТЯЧЩЦЪЫЯЬЩЮЪХЦЙНВЦТЦВДЧЦ
ЮДПЫЯЬЩАЯЬПТЩЙНХБДФДПТЯФВГЯТЯПАЦГБЮХБЦЩИШУВЯТЯЩЖГДГЯЮШАЬЫЬЩДЙЬЯГ
ЭЦЮЖЯГЦЬТМЬЯУЯЪГЩШЮЦПУЫЯЭЮГДЮЯИДУВГУЯУЬИГЯТМЬЮЦУВЯВГЯЮЩЩУЬХЦГНВЭ
ЩЭВЯТЯПЩУЯБЯГЩЬВХЯЭЯЪВЩХЦЬАЯФБДЧЦЮЮМЪУФЬДТЯЫДПШХДЭИЩУЯВГНЫЫУХБДФ
ВУЦЬНЩИАБЦБУЬЭЯЩБШЭМЙЬЦЮЩУЯГВДХБНВЫШЬЯЮАЯХУЭЮЦЩВАЩВЮЮМЪЬЩВГТДЭФЩ
АЯВЭЯГБЩХЯЮЯВИЩЫЬЩЮВУЯЦФЯТБЩЮЩВГБПВНЬЩАЯЭДГЩГНВМЮВЯГЗЯЭУШЬЩШБДЫЦ
ФЯТДЭФДОГЯТМЬЯГУЦГВУЦЬНЩИЮАЯЬДИЦЮЮЯЦЩЭАЩВНЭЯУЯГЯЮЯГВЬЯУХЯВЬЯУФЯВ
ДХБНЮХБЦЪАЦГБЯУЩИЯГЦЗЮЙЭЩЬЯВГЩУМЪЭЩЬЯВГЩУЯЦАЩ

(b) Расшифровать текст:
МХЙФИГМКМСМЯКЛЩПМДЧЩМХВШЩИРЛЗУГШИФФСЩИБЯЙТПФДРЦРШМЯЦТЛЩПЪНЩЬАЦНЩ
ЙНЦОХТГФКУПФФЛЙХПЫБЦГЕЭЯФЧЙУВМПРКЛШЪДМНЩКЛНБЛТКЦИФЛРКЛХТГФКУПФФЛ
СХВЛЛЧЪВШЩХХИОЕРУЛНОШЧСЭОИХЬЧИЛУЛХЕЬЪСФВУШГШБЬМРТЕПХИХРСХВХВЭМБЦ
ЮБТММВСЩЪРДИХЙДАФШСМНВЩМУЩРХВНЯРЩМХВЧУМОВШЙПЪПВПНШЕКЩЖТПИХГСЙОТМ
ЩПОФЖЯВЙХПЪНЩЬЖЩЙХХЗМРХХБУГЩПАНБВЦМАВСХИХКБРЕЧВЦМБЦНФЛИЫЗРЩЩМРТМ
ЦДЯЛЛЪЦПКМОХРСОЛКВЧЙЕЛИУЪЙЩПЦМЯРКБУЖЩЯФПКРАСОКРЕУПХНАФИМЛЯБФГЩЯЛ
ЧЖАЩСПЖЙПВСКЦЖШССОЕХЧЖЛЛШХАРИОШЪТЙЩЮГХЕЭМПТЛПШКННШПИЩФЧЩЖЖЛУУМЛЛ
СЪЯЫХРФГЫДУТГЛЛЙХПЧЛКПАУББСММЛМЛЙРОВУЩЧННЛЛРЗУМХНАФШИППВИГМКБРЖК
КРЪЕФЕЭСРЦЮБЦММРТТАЩЕСППЪЛЛКМШЛИФЖККШХЖЛКШГЖЯВЙХРЦДЭЩМТЗГЩМКОХХЧ
МЕСПИТЛИЯАЙНОФЙНЗЧМЗРЯУВХКВКГМЩПЦПБЩЯРЧСОЛРПРНМЛЧЪЫКЧЩСЪГЛШЛРЙОЦ
ЖШРЛЩНШЛИХОНКУМХНАФШИППВСИЩЗНТНШЛЗХЙДКЩЕНУВТФЛРУЩЩИЦКИМОРХВТЖЪЗИ
ОБУКЩТЛФВУСИЙШУХДЦЙУШИКЛНГММКРХЛНЯБЛЙЩМЧПЯЦВТЪЖППФЙЫЪРТПЛЫПЩЧЕМИ
ОШЪЧЩУВГТНОСЖЛЛЧЩГСЕЙХЙЦОФЩФЛВЦШЖФАФШРРПЦМЯЦЯСПАРКЫХЕРКРТЖТИЧХДР
ПЛТЪХЕЬЪНЦМКГОЩТСХНЦПСШЪЩПЩЦЗЪВЧМЯНБФУМСМЛЩОХБЦМЖЯОРОЙЦКШМНННВФГ
МЛИШСПИФЛГНЯХХНЦЖРПВНПЗМВЧЛХЛГЪВЧГНЦБХГЛЫЫЦЪИЫМЦХЧСПЛЦГЪНУЛОНЕЭЮ
РЦЮЩЛГЪПФИСМВШЙМЩЩЗХБХВФШРКЕШЦМЧБВЪЦУКЛШИЦИВСМЫОХХИЦВУФЩСЛШЦОКЕС
ШИЩВЗМЛТЯЦЩЖШРХЧМЭЛКУЖФЛХТМББОЬАРБЛТЛНОРХЙДЗФИЦТЕЦЭГКЗФЩМШШЛЩГЩК
ОТЖЩЩФСМУЛИППНИОЭЩРОШШИРЯСППЧЛЙППЧЛИМЦНКУВУЩПЦЪВЦЙЩЛГШГСЦМШШИФГЛ
ЛКХАХЕЭЪАЩПИЪЯНОХХЙНДУХПЪЩНШРЫМСМЛРМФСОНМФШРРЮЛКЙРННИМСКОСЖЛНЗХТ
РУЛЧПТЕЛЛМФЯЛОВННННЛАУЕЧГИШЕРПНДКЧЩАЫЫЯПУФПЛНЛРЗФЙНШЕЮМЙМЛТХЗЩЯЛТ
ЪРФИШРШВШПЙФВУЪНЦНФКПУЯЗХБЫЯЧСОРФСХЛЫЯОЛКНКЗВЙЦБЩУЙЯПФОЙЦБЛПМЧПВ
ЩГЙМФЛУКПОТЖХРЗ

2. Разложить на множители числа:

(a) 109354400883759031618996758484 1

(b) 690143745858732249085184042388602302685399561920864277780 91

(c) 134723528333612634975312069201840224702975430202437107510125119655769331046130853741331330 3

(d) 106473239946654360289059041204885418846121047370185004216975243138011089757881049551860343822463965068176376388941457771 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 365937478150375827255542244420888266943741626038434233315439390189503655864 79$
   - $e = 3$

   Сообщение:
   - $M = 766730893051895258949684567118165474886781044397389508419278304614491733451 5$

   В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 313438546994867716513582233985489302203$

- $q = 171526778654885260785835979876272848671$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 307763377319587319781387117606876722553245324610557233022096714640071236096 00$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 13849413515841475530662889503595322610 3$
- $e = 17$

Зашифрованное сообщение:

- $c = 92271209417151079290821624424610636 06$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 28327389347529507119544805852713710 7041$
- $g = 91720274524197441456064991214024191461$
- $y = 27371611407409771240581603422262338 1240$

Секретный ключ:

- $x = 24304935875251294786485021305762434 2809$

Сообщение:

- $M = 21093875666182109824011114582126784 8145$

Использовать следующий случайный параметр для создания подписи:

- $k = 51686232726521763634301155295674331949$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 18382422540960803343170727795829332 3633$
- $g = 13256860590848096324415910772314098 3455$
- $y = 96162648846065994753251778029670827406$

Сообщение:

- $M = 16745417027242815291540279259882715 7102$

Подпись:

- $a = 59247823862785934386823671632946594343$
- $b = 15701738956150376211486884437680120 8835$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 907$
- $g = 895$
- $y = 827$

Сообщение:

- $M = 433$

Использовать следующий случайный параметр для создания подписи:

- $k = 317$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 10x - 6$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 62

1. (a) Расшифровать текст:

ЗБОЮНЗПВЭБДЮНБЯКНЗЮЭКЯПЙНИКОМБЗДНШЙБПВОКЙФЗДНШОЖДБЖКИЙАДМЧЖКОКМЧ
БЛКНЗПФЗДНШМГЭКЕЙДЖЖВБОНЙБАКЗВЙКЭЧКОЮБУЗДЮЙЖПГИДУНЗЧФЙКЩЗКАБЕГЮЗ
АБЗПВИЙКЯДИДЖМБЛКНОИДЮДАЙККЙЮНИКИАБЗБНДЗБЙГИБОДЗФЮЭМДЙЮКОНБЕУНПГ
ЙБИЙНОКХПЪБЯКНДЗПНЖГЗЖКИБЙАЙОЮНДЗДНБЯКМКЮЙАЕИЙБЖЗЪУКОЙЭМДЮЙДЯЙОШ
ДУЛМДЮБАДЖЭФЖДМТАЛМДЖВДЪЗЪЛМДЙБНОДНЪАЛЗБОБЕЛКНОКЕДЮЙЖПГИДУНЖГЗЖК
ИБЙАЙОФЮНОЮНИБНОАЕПЮБАПИФПЖПАЙДЭПАШДГАКИПОКПНЗЧФДОЖМДЖЛБМБЛПЯБОН
АДЛМЮАПНЖГОШЙБКСКОЙДТАКМКГЧНЖНУНОЗДЮККНОЮОШНЛЧОЖЮНОМДЙПОЖЭЧЗПЖКМ
БЙБЙЮКЭЧУСНПАКЛМКДГЮКАНОЮУОКЭЗЯКАБОБЗШЙЧЕПЖГПЙДУОКВДЮФДЕКЙПЪАКЗЯ
ККНОЮЗНЭБГКЮНЖКЯКАБЕНОЮДАПИЗДУОКНКЭНОЮБЙЙКБЛМДГЙЙДБЛМБНОПЛЙДЖЙБК
ЭСКАДИКЭЧЗКАЗБЯКЛКЗЙКЯККЭЗДУБЙДИЧНЗШЙБОКЗШЖКЙБКНЙКЮОБЗШЙЙКАВБДНК
ЮБМФБЙЙКЛМКОДЮЙГАМЮКИПЪМДАДУБНЖКИПНИЧНЗПДЭКБНЗДКОМДТЙДБЛКАНПАДИК
ЯКЙБЛМДБИЗБОНЮАКЖГОБЗШНОЮКБЯКЙБЮДЙЙКНОДОКЛМДГЙЙДББЯКДОКЯКИБЙББАК
ЗВЙКЭЧОШАКЖГОБЗШНОЮКИБЯКЮДЙКЮЙКНОДАВБДЙЧЙБНЗПУБОНИЙБНЗЧФОШНОМЧСН
ПАБЕВЗБЪХДСКЭПЙДУОКВБЙДДЮМЮМНЖКЯККЭЧУЮЙФБВБЮМБИЙДЖОКЙБНПИЙБЮЗНЮЙ
БКЭСКАДИКНОДЛЧОЖДЙДНПАШДЙДЛКАНПАДИЧБДОЖЛМДЖГЙДБЖКИБЙАЙОЙДЖКЯКДГЙ
НЙБПАДЮДЗКДЙБЮНОМБЮКВДЗКДЮЙДЯЙОШДУКОЛМЮДЗНГЭФЖДМТБИЖКОКМЧЕНДАБЗЮ
ЙЭМБЛКАЖЗЪУКИПЖКИБЙАЙОФДДУБМБГЙБНЖКЗШЖКИДЙПОЙБЮКЗШЙДЖЛМДЮБЗДЮЛБМ
БАЙЪЪЖКИБЙАЙОЮБЗБЗБЯКЖНБЭБЛМБАНОЮДОШЭФЖДМБТНОМПАКИФЯЙПЗУБМБГЛКМК
ЯКЙЭЧЗЮЖКЗКАЖБДНЙЮЮЧНКЖПЪНЮКЪФЛЖПКНОЙКЮДЗНПАЮБМБЕЮГЯЗЙПЗЙЙБЯКДНК
АМКЯЙПЗНЙДЖКЯАЙБГЭПАПЩОКЯКУБЗКЮБЖБИПЖГЗКНШЗБОГНБИШАБНОПЙБЯКЙБЭЧЗ
КЙДЙКНЙДПФБЕЯКЗКЮБЯКЭЧЗЮЧЭМДОЮИБНОКЭКМКАЧОКМУЗКЙБНЖКЗШЖКНБАЧСЮКЗ
КНКЙЭЧЗИЗКЯКМКНОПОКХДНЯКМЭЗБЙЙКПГБЙШЖДБЯЗГБЯКНЮБМЖЗДБХБКЯЙБИЩСБН
ЖГЗЖКИБЙАЙОПГЙЮЛКНОМФЙЧИБЯ

   (b) Расшифровать текст:

ШЫВМЪЖЫБЮНЩЩМЯНВЩИЧГВДФМФКЧМЛКЬУЖТЦПМЪХХЖШМЙЦЗХМЙЩБЦХПУЩЩГЛУЕХГЛ
ЦЭМАЯРИДИОТЕКИХЪЕШЩМЭЕЪГТРШГЙХЧЕМПЛРЙДГКЦЩЕРХКЗНКППЙЦЙЦГДШМЛКЯОС
ЙГИЪСЦРВФМРЩЩНЙГРОЧМЛЭЕМЖЩТЖЫБЮНЩЫЖЦЦЫНРМФКУЖШЪШЫКККРДНКХЛЖШЖЛЫГЪ
ЪЮЪЕРЕЩЦЪЦАВМЬЪЫЩЦОЪМШЧЗЦППУЩОЛХЧКЛХМКЖШМЮРЙСРСРЮКМТРПДСЙРЫНРГЦЙ
КГЮУИКГТДЯЯНЪЛОНАЦШЯХЙИЫГЛСПМЕУБХШИЩКЩШЯКЙШКЯММУПДЯЖЩНВДЛВФОЪМЩГ
ЙТКЪМЗНЛХЧЯАГЯДИТЕТЦДХИХХЬЮЛЯРИКГЩУТНМЮРДНКХЛКЪРЪЪДРХМЛЕШЕХЙЗЪЪК
МЬФМРЦШНОШНБШГЩШУФМТЦЫЦЗУУЕСАСЧЗУЪШТЕФКЪХЫРОМЧЗЦАХШДЦНХМШНДТТЖЫБ
ЮНЩЫХПЪАКПТЫМЩИОУИФМОКДНФХЪЫКГУЫШЫККЫОШГОКТЯЗФЦВЖЯХЧТЪПЩКЕКЙЪПДЪ
ЪХЯЬФВЛДБФМРКЮМСУУЖРПЩДЖЫБЮНЩЫМИНЗЩГСШЬЪОГЛЗЦКХЛВЩЛХЩЙУНХЩБУВУЯЯ
ЪРГЩВНВЪЖРНГЛКМУРУРЙТЙМКТСЖЯНВТМЙГАЧМТЦИЪЩРХПНПЩДЗЫЯТНАЕРХЯЙЦЕФЯ
ЯЪПСПВХУУЫЗЩЪЦЫЪЯГЙЧЗРИНРОРРЩДЫУГМЦЙКГЮУИЧМСЦАХМШКЬУЪПЯЕЙГЧЩЬТОМ
ЪЗДНЧЦЫЦЙНУГЫЛЛРЗРЕЩЦДТМКЦЮНЙМХЕЛМШЫБХЛШНГДОЪЙВНЗЯЪДГЯМУТНПЪТЕХЛ
ВНДЧРГШКЙЙМСЫКГФМНЪЪЧЫШЭНХУЕЪЛФГМЛМТХЫЩИПЭИФЛННЙФЖФМЬЩРГШКЙЙМСЖЦ
БЧНШНФШЯАХМЕЧЕЩСЛЦХХВЙШКЙЙШЧЕУРПХЕЖХЩЦЮКОФДЬЧОМШЩУНЪЛОНАСТЕНКФНЫ
НЙХМЕЧМКШЬЙФХКЯММЯЪДЦАШФДОГЩФЯЩАМУУРХСШБХСТРИЪЙХЙСЩЛШДИЕРХЙЙЖЦСР
ЮКМТРПДАПМЬЪЪЧНЬЩРЧЙЗЩИХФКММИШКШПСШЫНЛФЦГЫЕТЦЫНКПТБРКППВЦВМФЯЩНЧ
ЦИРЙКШЕПЛХЧКЛХМКЩРЛХКЙЦЯУЦВКЖТЩЕЪАМЯВЩАМУУРХОУЕМГПХЬПЙХМЬРРЙЦЯШГ
ИЪЙТЖЦЦПШЖТРЫЧМЧЩЙЩИТРДНБФНЩРПГТЕХЪПЦОНРВШЬЭЛХЛММПЦЦЙГИМЪИЧОПТЭР
СНМЕЯЖЩЪУММЮРЙГАРЩБПЙЦЫЪЯГЙЩЬТОМЪЗДНЧЦЫЦЙНУЕМГТЦИРРЭНЩЦГЛШКЛММЪЛ
ЪЛХНДЭЙХЧОЪМРЙКФБМЯЬЪЩЧНЗЫЯТАКЙЙПЩУТОВЪВГКЧЪЯХМУШКЙЙМСЬБГОСОРЗЩЫ
ВЫНЮРБЧМНУЕКЛФГАЪАХНАФЖТЦИЪЖФЧЕЩРХУЕФВЙЦЗНОЪЙВНЗДЪЕЯРХНРНАШТЗРХТ
ЧКЛХМКИКГЧТДЫАХЛДНЛФГ

2. Разложить на множители числа:

   (a) 78788237434997784590526634870 7

   (b) 85035859902631458594838216547623091532159827806690139133753 1

   (c) 15915314918138496991911394606559734104643006973423503006711495320894618246310427635827303 47

   (d) 12672166539225085367312302989652043993191555476555731687338228844831961738309249141185661125875972333487206038480911980 01

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 429265101577411768528213926520199916587662106328813894883872339543946219239 91$
   - $e = 3$

   Сообщение:
   - $M = 426782345902047342889452518110207220392650198375779307279136363436601767074 02$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 297129090583784413509773120430124618129$
   - $q = 203884468762626728595484469139765119203$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 320184630415097811988758200663207494207085117988723606837687214583140784587 42$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 181666754303418227138699502762066913753$
   - $e = 3$

   Зашифрованное сообщение:
   - $c = 566824626386743554786425430281390865 37$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 305794709634658229423178227436915985949$
   - $g = 252602897800597225402541427918023572170$
   - $y = 831155042108682464386147440037534813 65$

   Секретный ключ:
   - $x = 864567207415373916083569145515366223 42$

   Сообщение:
   - $M = 205926496834008276625892895749990028101$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 166591324631738430186458672228816279383$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 232201214613631663117566582614429066671$
   - $g = 105755042276767224900536690047938838871$
   - $y = 401819964615753668642613518775675842 6$

   Сообщение:
   - $M = 833227145281715151252663020388698632 23$

   Подпись:
   - $a = 956087812179569998697648722151440397 05$
   - $b = 191731256104234011904945468818380757094$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 641$
   - $g = 69$
   - $y = 370$

   Сообщение:

- $M = 344$

Использовать следующий случайный параметр для создания подписи:

- $k = 521$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 5x - 8$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 63

1. (a) Расшифровать текст:

ИЭБВЗДЖЖМБЛКНОДЛПФЖЙФГМВБЙЭЧЗЖМОБУШЪЖКИБЙАЙОЛКАЛПНОДЗДСЙНИКБЭЗДГ
ЖКБМННОКЙДБДЮАМПЯЮЧЛЗДЗКЛОШЖМОБУШСЮОДЗЮНИПЪНМБАДЙПОКЗЛЧИОБВЙДЖДК
ОСЗЧЙПЗДЮКЭБНОКМКЙЧДЛКЛОДЗДНШЛМБАЮКАДОБЗШДСКНОЗНКАДЙЮЛБМБАДКЙИСЗ
НЭЗБЪДЖГЗКНШНВМКИДСПЯКЮМДЮЗЖМДЖДЮДГЯПИКЗЖЙПЮФДБЙИДЙПОПОКОУННЙКЮЮ
КГКЭЙКЮДЗДНШЙПМБЭОНЖГЗЖКИБЙАЙООБЛБМШКОЮКМЕЮКМКОЭБЕЮЭМЭЙМБЭОЮЛБМБ
АЙЮЧЗГЖПГИЙКЪЖКИБЙАЙОДЮЙДЯЙОШДУДИДЯКИКУПОДЗДНШГЖМБЛКНОЙЧИЮЗКИЙКК
ЭМКЭБЗЧЕЯМЙДГКЙЙБОМКЙПЗНУОКВЮЧАБОПФЖДНОКДОБГЖМДУЗДЮЙЖПГИДУПИДМОШ
ОЖПИДМОШАБЗКНЗПВДЮКБЮЩОПИДЙПОПИОБВЙДЖДЙЭБВЗДЙЙНДЮКМЮЗДНШЮЖМБЛКНО
ШЭМЭЙПИКЗЖЯМЙДГКЙЭМКНДЗМПВШИБЙНФДЭЗДЭЧЗКНЙКЯЙКЮНОЗДЮИБНОБНИОБВЙД
ЖИДЮКФБЗЮЖМБЛКНОШЖКИБЙАЙОМЙБЙЧЕЮЯКЗКЮПНОКЗЮЖПУЖБГЗКАББЮЖКОКМЧБОМ
БЭКЮЗДКОЙБЯКЖЗЪУБЕЭМКНДЗНЭЧЗКЖЙБИПЙЛКИКХШЙБНЖКЗШЖКАЪВДСЖГЖКЮНСЮО
ДЗДИБЙДНЮГЗДЖПФЖИДЛМДЯКЮМДЮЮКОПВКЮИЭПАБОЯКНПАМБЮЧИКНЗПФЙДЖИЙНЛКО
ХДЗДЛКПЗДТИВДОБЗДЮЧСКАДЗДДГАКИКЮНСЗБЭКИДНКЗШЪМГАЮЗНЖКЗКЖКЗШЙЧЕГЮ
КЙЮАМПЯГЖМДУЗДЮОКЗЛБУОКЯКНПАМШЙЛЗКХАДКВДАБОЛЗБЙЙЧСДЛМДЙДИБОЛМДНЯ
ПЙМКАЛКЮЗДЗЙЛЗКХАШЙНЛКЯЙЗДОПАВБЛПЯУБЮНДАБЗЮЖМБНЗСЙЖМЧЗШТБЖКИБЙАЙ
ОНЖКЯКАКИЙЙБИЭЧЗЖМНЙЧЕЖГТЖДЕЖРОЙКЭФДОЧЕЯЗПЙИДЮЧНКЖНКЭКЗШФЛЖНГКЗК
ОЧИДЖДНОИДЭЧЗЙАЮДЙПОЙБЯКНЮБМЖЪХДБЯЗГЗДТКБЯКЛКЖГЗКНШИЙБГЙЖКИКЖГТЖ
ДБНОМФДЙЧКЖМПВЗДБЯККОБТЯБМНДИЭЗБАЙЧЕДАМКВХДЕНОКЗПЖМЧЗШТНЖМБНОКИЮ
МПЖСДЖГЗКНШИКЗУПИКЗЗБЯКГЛМБАНОКХДБВБМОЮЧЙЛЗКХАДНОЮДЗДЙНЖКМКЮДНБЗ
ДТПЖКЯАИЧЛМДЭЗДВДЗДНШЭФЖДМТЧМГКЯЙЗДЙМКАДЙНЛМБАНОЮДЗДЛПЯУБЮПЖКЗКЖ
КЗШЙЧЕГЮКЙПОДСЙНОЗЯЗПЭКЖОДФДЙЖКОКМЧЕЖКИБЙАЙОНЛМКНДЗНИКГЮЙБТЙФПМА
ЙДЖЮЧНОПЛДЗДГОКЗЛЧДПЖГЗЙДЮЙЖПГИДУЛПЯУБЮЯМКГЙКЮГЯЗЙПЗЙНОМДЖДНЖГЗ

   (b) Расшифровать текст:

АФРХЕЬБЩМОАРЬФОСЪРМЗЫЗШТТЬЬРХМЬШТЙЛУНЙПУФЭЫКИАСЩМПЮФРЯКЩФШИРЪУЩЙ
ТРДЦРНЦБТЖОЮЗТКЕЭЬЦХТБЫЙУУСГУЖУФЩУУРЦОЩЙКЩФЬЕЩУПЬПЮПЪЭЯТЯЮРЧМЦЬЩ
ХОЯЦБОИРЬУРШЩЪЭМСУШЦЛБУЧЬЗОЮЭШТЙШЬУУОЯЮЦСЕЭЪЦЧЧЩОЯЙДЬЬЬЗИПЗЩМОАЬ
УЛНЙЬХПУШЭЪФЬУХЦЖНЬОЫТЙЯЮЫТВЦЧЯАМЫСЫЙСАСЮУИЪЩУМЗРСЯЦНЬЭААОУСЯЧДК
НУРЕЫШБЫИЩСТМНЯЮРЙНЫЪУФЗРЧУЫЕЫФУРОУЭЬХТЬЧЬЖНУУТСИЕСЯЦВУЫЬРИЩЪЯЦИ
ЭЯСЫЕРФЪЙЛТЪПФУМЧЬЬДКЭШТТЬЬЬНДУЧЦПСЯЦБИНЬХЭМЩУКЦСКЬЮЬФОЧСФЙДЫСРС
ОРЗУЛЖЩУСТРЬРЭЙРУЭАФЕЩФРЦЬЯЭЭЧГЕСРХКЦШЦСЕХРЫМКЪФРБТЦБЭЙРУЭАФЕЩЦГ
УЕЮСРЙСПЗЩТБЙЦЫТВУЩЫТНЯЮЬФОЫСХПОТСУЖСЙЮЙЩПКЩЙЩИТЪПФОШЪЫСЫГЮЬЭГЬЬ
ЬИОРЦЬСНЦВЫЙМЬПЩМХЬРЬПЕАИЦСОСРРЯХЬРЦПВЭЪЩЙИЫДСТЛЬРЫУЕГЪАСОСЧБЕИЫ
ЭЫЙГЪСЖПЕЧРУНСАОЬЖТКЯТЫНЬЫЮТТЦОБФСЯСЫСЫГЩУЛДЫФШТВЮЮЦПЛУЬЦЦЩУЮЫТГ
ЮСЪЙЛЯОЙХОАЗРПВЭЪЩЙВХЧЦСЕТОЦЗЛЯИЭТПЮФЕМНУФХСУЮСЫМЛЬДТЙЙАЦЬЖБЙЧЬЕ
РХЩЖМХРЪУСНЙБТЙЯЮРМЙЦОЬЦЧАЪЬФЕЫНБФГЯЦЦЙЧЦЩЬЖНЦЦЦСЗЙОЩМОЯЮЬФОФЩЬ
ХТЦКЦЕЛСЪЮЛУЪФУРОТЩФИЫШЪСИУТЧЬХЬЫШШОТЬЬЯХЕАИЦУРЬПЫЦЬТЪРТЛКЩЬЗУЯЮ
ББВТЬЧЭЧНУБЩСКХЦЬЦСАОЖЙГЬЪАХВЬФГЦОРЬЦЭЕЧПЬЦОРНЙПУФСБИРЦЮКЙГЬЭРТЕМ
ЮБФЕДЦЬВСПЧУВКШОТФУСЪЫХНЩДЭОУЦУШФИЕЧХИРРЭАЖУЧЮУУЕАЬЫИРУФЕОКРЭПТГ
ЪФЩЧЕАОХЗЛЫЯЩМУХЩЩСШУПЬЧРТЩЦОНУЭШЛНЫЪУРУЬНЮИОРЧЯЛДЮОЯЦВБХЪОСЦШЙЫ
СШУЩЙМБРРСОЩФЦЛБУЧЬЗОЮЭШТЙЫСТЖНЬНАВШШЫУЦРЫРЮЙИЕЮЬПЬШЪРЫЕЮОЬФОАФЩ
ХУЪСЫЙСАИШЖМЭФЯАМУВЬЗДУТЬСОРЭШФИЕЧРЙСКЮШМВЯЫЙЩНБОЯТМЫЪМТТРСЕПМШЭ
ЦРЫЕЫЬПОФФРФУШЯХУЗББТБУЕЩХПЩДУЧЖШЦЫМББРКИВЪРЬХТРФААТБЮЬСПЬРЩРНУ
ЭЩТЖУЩЫЧЮПЯЪККБФАТТЕЭБХКШЧЮЛВУЬЫЧЛУСЦХТЮСЭЙТЬШЭФОЕСЩХЛУРБВЩЦСЯЦР
ЬЦЦЕОСЯБЗОТЩЬЕЫЩЪЩМШЦЮКРЕЫОТФУСЪАЪИЪЮУФИЫСЦРЕМЩХЙМЩСЫМРЬРЫМНЦЫЬО
РЬОЦЦЕЩСЧУРЦНУЗЮШОЪЛНЕЮЬЖЫРЭУЗДФСЩПИЪЩУИОПЬЦЫТЬОЙЖСШЪЬЧЧУЧЬЖЕШЯС
ТТЬОЙУОЪЪЕАМЬЧ

2. Разложить на множители числа:

   (a) 915189870412519769991688619681

   (b) 856640140321071210317651579643904556995268624650224853908589

   (c) 1249515389685233131416667733725073710172284837634193458562467760371659409069480853629560709

   (d) 1174332629721369046593083559364177408783361634952525270693300449493614690332725141205244695134125685651374888552119829763

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 507407707389443002410337494034441677410406144106177694773074513231287202768 79$
   - $e = 3$

   Сообщение:

   - $M = 255346603642374854947496357074288654744135746216238561449931080790338117788 14$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 190644716501385685117603416299782556807$
   - $q = 307140076264008555311862417463162572901$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 356698281301104132275710317779755107162911693403854536424829027638935193339 98$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 144841321461742493872905477575895464663$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 628577270560358338143840114695170889 30$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 337089581841109320949921602771748550729$
   - $g = 138255029461338905976680089120068172550$
   - $y = 188017123957761117752973913608226972857$

   Секретный ключ:

   - $x = 329788707962430327399729472786699837380$

   Сообщение:

   - $M = 309453407595831029019231818234589826 11$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 135971368492214463911442789915878573$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 23959348097622025189747724421760288 6727$
   - $g = 164392948313089356629460534870808574179$
   - $y = 178494076330207300674890844203821657473$

   Сообщение:

   - $M = 715913577690331298715185839007071 3898$

   Подпись:

   - $a = 101716932686579763114780447085185957083$
   - $b = 47806228744018900894889658536084647 13$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 1009$
- $g = 491$
- $y = 40$

Сообщение:

- $M = 957$

Использовать следующий случайный параметр для создания подписи:

- $k = 835$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 16x - 14$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 64

1. (a) Расшифровать текст:

ЦСОНОЩРУЧОСУЧЫЧЩЧОАЬЫЕКДФЧЦОЬЛОЦАФЧЪЕКОНЪЫЛОЦЦДХЬЪШОЮЧХШЧЮЧНКДФЧ
КГЛФОЦУРЛЫЩОБЦОХЬНЦЗЦЬКЩЫЯДЪУРФШЬМАОЛРЫЦОХУЦЪЧЦМЩНЬВСТХЧЗФЗКСХЬЗ
ШОЪОЦУЬАЬХУЧЛЦАСЦТЪЧЪОНХЧТРЫЦЬФЫЧЦУСХМЧФЧЪУЧХРЬЦДЛЦЬЗКЬЩФЯУЬЗШОЪ
ЦЗСЛЪОШЧНЮЛЫСФСЮЧЩЧХЦОБЬХСХЫСРОФОЦНЬКЩЧЛЬБУЦОХОБТХЦОНЧКЩЧХЬХЧФЧН
ЯЬНЬХЬНЬХЫСАЫЧРЬЫЩХЦОНЧКЩЧХЬХЧФЧНЯЬЛНЧШЩЧЪСНЫСШОЩОНМЩЧРЦЧМЧЪЬНЕЗ
ЪХЧМЧЯЩОВОЪЫЦОЫМЧЪЬНЩЕЯЩЕХОЦЪШЩБСЛЫЕЫДЪУПСЪУПСНОЫСЦЬБУУЩОЪЫЕЦЪУС
ТЪДЦЬПУУЪУОХЫДЛЧЩЧЛФЪУОХЩРКЧТНОЩПФОВОХЦЧМЧФСЪЫЧКЧТКДФЧЫЧЛЩСВОТЪУ
ПЬЫОКОЦНОПШЩЛЧЬФЛЦДТЯЩЕЛЪООШЩЛНЬЪУПЬЫОКОЛЪЗСЪЫСЦЬАЫЧЫЧЛЩСВОТЬХОЦ
КДФЧАОЫЛОЩЧОВОШОЩЛДТХЧТЫЧЛЩСВЫОХЦЦЧАЕЛЫЧЩЧТХЧТЫЧЛЩСВКЬФЫЦДТЦЧПУУ
ЫЩОЫСТЫЧЫЧЛЩСВЫЧХЧТНЧКЩДТУЧЦЕАОЫЛОЩЫДТХЧТЫЧЛЩСВЫЧЫЬМЧТФЬУАЫЧЩЪЪД
ФЕВСУСХЧСЫЧУФОЦДЪЩОФДАЫЧЛЧРМЧЛЧЩСЫЦНОПШЩЛЧЪФЛЦДТЯЩЕСЪШЧФЫЕЫОКОН
ОЫСЦЬБУУЩОЪЫЕЦЪУСТЪДЦАЫЧЬХОФЫДЛЧЩЧЛЫЕЬХОФЧЫЛОЫНОЩПЫЕРЫЧЫОКНОЫСЦЬ
БУШЧПФЬЗЪОЩОНСШЧФЮЧЩЧХХСЛДЪЧУСХСАЫЧНЛЬХФСЪЫЧФКХСЪШОЩОУФНСЦЧТЦОЛЧ
РХЧПЦЧЩЪЪУРЫЕУУЧОНОТЪЫЛСОШЩЧСРЛОФЦХОЦЖЫШЩЧЪЫЧЦЩЧНЦШОЪЦШЩЧЛСЪОФСЯ
ЬЩЪШОЛОХФЗНЕХСЧКЩОАОЦЦДХСЛСЪОФСЯОСЮМЩЧРЦДОФСЯЪЫЩЧТЦДОМЧФЧЪЬЦДФЧО
ЛДЩПОЦСОУЧЫЧЩЧОШЩСНЛФСЧЦСЪФЧЛХСКОРЫЧМЧЛДЩРСЫОФЕЦДХЛЪОШЧЫЩЪФЧХОЦУ
УСХЫЧШССЫСАОЪУСХЬПЪЧХМЧЪЫСЛДШСФСОВОШЧЪЫУЦЬЛЪЫФССРЧЪЫЧФСШЩЧЪЫСФСЪ
ЕЪШЬМАОЛДХЮЧЫОФРЦСХСШЧЪФОНЧЛЫЕЦЧШЬМАОЛЪУРФХЦО

(b) Расшифровать текст:

ХЧЖБЬАТЩЮНШЩВЩЙЩПУШОГЧЩЭНЫЯЮДПШЪСДМЖЧТДВБЪВГЕКПТДИИЧЧЬЛШЬЛГИЩХЭШ
ТПЫЩЭЛДЬЯЮЧБФСЩОЮЭРДЙЮПЬИЕЛМРЖИАЫЩЭНЫЬЛГЕФПУГЕИЭУДИЦШАЕОЧТЬДФЫАФ
ЖДБЩЯДСЫЬЛЕОГОЩДМЪБФВИЪМЭБИЮЩЭЬЛБМБТЕДХЧДНЕПРЩОДЭУЖЕЯЧФЕРЫСЬЫТЕФ
ЬЫЧШНЭЙТШЛЧЙПГМКЮСЭЬЛАОЮТЮЖИЪЧФИЧЕШХЫОАОЭЗЕЦШУГШАПТДДАЫЧЪЕЮМЭЖЕА
ЛВЖГШЫБШОЫЦЧЗУВШАИТЯТЬЫПГТЩЬЕЛЖЪЮСХПАИИШНЭШПГТЩЭНЖИУЭПЮТБТТЯШТДН
ПФВВНШЫУЫТДББДЕЦШЫЮЛБЫБТПБОЭЗЛАФЬВОЕШЯЫНФЭЯЩСЭТДАОЯЧУЮРБМЪДГЫФАИ
РБНЭЭЛБОФЕОЭСЪЗЬЯЧФЪОХШЪТНБЭРЫДЫЬФБЬАШНВОГШЦЕРБЛФЬЛВШСЗЕЯЭЫДЕЯЭБ
ЫЛЖЩЯЮМОЫЪЮВКЖЧЛРЖФДГХБОЧБСВЭТНЕХСЫЫТЫХЫДЕДЦВПЕАТФЗЬХВФЧЛЦШЯДДЫП
ААЗЮШЬВНШЩЭЪМЫНЧШФШХЛЪМГВЪВОЬФХЫТДНЭШОГТБЪЕЮШЩАТООВВЕЛЖЬЗМШВЩЕУЦ
БФШВБССЖТЫХЫГЕФШУЖОДЬЛЗПБФЭЯНБШБШЕКХЖИОАЯЭЬУДЖСЫГБМЪЗТЫТЖИОБЧСДЛ
ШЧЮДСЕЭЮИЬДШЫГОСФЩЫМЖЛВЪЕЕЭТДДАШУДБГШААЗЮЩВЩЧШМБЫПШЪЛЗКЩТСАКБЦАД
СЕШЬЮИХВТДРБОАБВФШТЙОЕМФНЛХЫФЧЛЦШЮДЛЖБЬДБЮНЭЕОЮЭЖГОВШСИОГТЪЕУЦБФ
ШНГШУВРШЬАЩОЮШУЙСЯШЦШНШАТДВБЪЧБПГМУЙНБЩЭЪОЮНВЕРЫЫТЮСЕХВШЕГЬЛНТБМ
АЫЭЕШЮЙСЕЕФЗЛЖЯЧЮЧЕШСДРШЧРЙРЦПУДВБХЛГОХЫЩЮХЪЩАДВЕЕСЮДЫВЛЕОЧЯСИИЮ
ЫБЖИКШЩНТБШЬИЕФМТБЗБЛЫГЫХПБШСШЛФЩЛШАКЗОЦХАГОВШЩЭЫХИБНТБМЭЖЕАЛВЖГ
ШНЭБОЧТЫДРКЬЭИМШОБВЕГЬСЫЧЫЧВЮТБСЖЫСЕЖФЩОЯТЪДСЕЖВШЕГПБНТБМАЫГБМУД

ВБХЛАОЮТБСШХЛЯЮНИШЖЫШПЩЭШЕДТБТТБЭХГТБУХЫВЫЫФБИЙПЮДВШЫЛЮЭЕШТДМБХЭ
ЪЦКЬЭЧНЫФЭВУАПРСЛБССЮДАШАБОХЩЯДКЮЬЭЩОДЬЯЮКЭСЪДСПЩЭАОЮПРБИВЭТНЕХФ
АНСЕТНЛЛБЩВОСЕХЮЖОЕТСДРШБЧИЬДМЭЫМЖЬЭШРЫГВЕОЮЧЭГУЯЕЖЗКЪХЭГЕЯЭБЫБШ
ЛКШСШОВОИЕЖУЖЕЪЬЛНТБЬКЭББНБСРПЩЭЩЛЧПБТТЭМЖЫМЧЭЗЪЕГРЧИСДЦСВОЦТЪЙС
ЯШБЖИЛЖУЖУЦТДЩУФТЗТРЪМФВЛБФЯДВЫЧБШОШУАДВШЫБЮДЕЕЖИОЪЭТДДАТЩШОЪЪЦЮ
ЛФПЪДББЪЭЪОХЭБЫБЕШЭИКЖОХ

2. Разложить на множители числа:

   (a) 384621221404135044179294457763

   (b) 13486457157831462372099111953852629431773949573485070660649 31

   (c) 955607931554122449836753806861315046159537462021771873019274925071167751573204072675572457

   (d) 234543164761121048658118596985139945366553312857201282372096111766219908172546360675726401165519122295217072745839535039 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 535689194889139658828699944216431129069467846726681351833463930017686296982 53$
   - $e = 5$

   Сообщение:

   - $M = 3146753522825830338710489784774620834832407758086344441319964950911188714332 5$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 333108472043132834773991198832540485833$
   - $q = 238948166274263368169516071819083780191$

   Открытая экспонента:

   - $e = 257$

   Зашифрованное сообщение:

   - $c = 45199489193637380848012259177682285400127283931034320000101674175581910073225$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 250931639542048919005540029548049407369$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 74159334795774166781961358476707923354$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 3108791108602311304138869877308743671 63$
   - $g = 926308868917780272451457643166341989 96$
   - $y = 187456034961135660879291101719382261859$

   Секретный ключ:

   - $x = 434484171379566258249992518693436455 09$

   Сообщение:

   - $M = 1274988900679385148743196301860513634 85$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 514413567006557574589131406438215764 63$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 267566974384330340149392064241739804221$
   - $g = 415825753204146366860211431075723916 22$

- $y = 207347425421366785063183145903188432699$

Сообщение:

- $M = 209475398435783974887717278851308116321$

Подпись:

- $a = 739922390892619063200428687285879164 95$
- $b = 227220585903812954951307143712497840141$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 683$
- $g = 594$
- $y = 82$

Сообщение:

- $M = 49$

Использовать следующий случайный параметр для создания подписи:

- $k = 537$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 13x - 4$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 65

1. (a) Расшифровать текст:

ДЬИКИЭМЪЕЪЬБЭВИЗИЖЯЕРАЖЭЬЧЭЩИВЩЪАЗИАИДЭЖЪАЧЪЕСКГБДГЖЩЭЧЬЖГЦГУЖЧЪ
АСЭМЧГЗЧЭЩЭНСАЭЖИЩЕСЖЯЬАЖЗЕЭЯМЗГВЪЩЕГБДГЩАБГНЪВВЭЯИМЪАГЦЭЗСЪЧГЕИ
ЗГЖЗАГЖГЧЪЖЗВГКГЗСЦНЯЭЕЖЯЩГАШГЧЬЯАМЩГЧМЭВВРЮЗИАИДВЪЖЗГЗЭДГАГЧЭВР
ЗГШГМЗГГВЭБГНЪВВЭЯЭИВЖИЯЕАЭЭЗГШГМЗГЗРЪБИЖБЭЬЧГАЭАДГЫАГЧЗСЩЧЖЪЫЪД
ЕЭШГЩЭЗЖЖАЭКГЮЖГЦЯЭКГЗСНЪЕЖЗЭЯАГЯШАЧГЖЩШГЕГЩЬВЧАИШЭШГЕРЖЧЪЕНЭВРЯ
ЯГЕЪАЦЕГЖАВШЕЩГВЧЬГЕРЬЖЗВГБДГЧЬАЪАЖГГЕИЩЭЗСЕЖЯЗЭЧВЪБДЪЕИВРЖЯЕРЧЧ
ВГОЭДЕЭЧЪЖЗСДГЩШЕЩКЪЕЖЯГЧДЕЭЦАЭЫЖСЯГЕЪВЦИЕШИИЧЭЩЪАЭБРЗГАДИЯГАГЩВ
ЭЯГЧЖГЦЕЭЗРБЭШГАГЧБЭЖАЭЛБЭГЦЬЬГЦЕЫЪВВРБЭОЭДЛБЭДАМГВЭЕЦГЗАЭГЯГАГИ
ЯЕЪДАЪВЭЮДГЩВЩЬГЕГБШЕВЭЬГВВРКЭВЧАЭЩГЧЭВРЪЧРЧГЬЭАЭЧЗЪАЪЫЯКЖГЕВДГА
ВЧНЭЮЕГЧЩЕИШЭЪАГДЗЯБЭЯГДАЭЬЪБАУВЧАИЯБЪВОЭЯЭЗЖЯАЭЯЭЕДЭМЭМЭВЭАЭШГЕ
ГЩЖЯИУЖЗЪВИИЧГЕГЗМЖГЧРЪГЖЗВГЧЭАЭВЖЭДГЗЕЪЦГЧАЭВНЭКДЖДГЕЗГЧЯЯЖЯГЕГ
ЖЪЕЫВЗИЖАРНАМЗГЪЩИЭЬЦЪАГШГЕЖЯГЮЯЕЪДГЖЗЭЗГЭДГЧЪАБЪВДЕБГЧЩГБШЪВЪЕА
ЬЖЗАЪШГЧЖЩИГВГЖБЗЕЭЧАЦАГВЭГЦВЫЪВВРЪЩРКВЭЪБГЖЪВЭЭЖДГБГОЭУЖЗЕГШГЖЩ
ГЧВЭЯЦЪЕЪЫВГЭКИЯИЗРЧАЗЪДАГЮЖГАГБГЮАЭЛГЪШГЭЬГЦЕЫАГЖДГЯГЮЖЗЧЭЪЬЩГЕ
ГЧСЪЭЩГЦЕГЩИНЭЪГВБВЪГЦЕЩГЧАЖЭЖЗАЕЖЖДЕНЭЧЗСГЦИЫЖВРКДЕГЭЖНЪЩЖЗЧЭКЯ
ГЭБЦРАЖЧЭЩЪЗЪАСЕЖЖЯЬАЪБИЧЖЪЖЗЕЭЯЖАИНАБЪВЖГЧВЭБВЭЪБЭБЪЫЩИЗЪБГЗЕЪЬ
РЧАЖИКЭЪЧЬЗЧЭЦЪЩВРЮБЭЕГВГЧЖЯЬАГВЯГШЩЯГВМЭАЖЧГУДЪМАСВИУДГЧЪЖЗСЫАС
ЪШГКГЕГНЭЮЦРАГЙЭЛЪЕЭБЩББЭЕГВГЧЩГЦЕЦРАЩБЭЯЯБЮЖЗЪЕЭЛШЕЭЦРЖГАЭЗСМЗГ
БНЯДЭЗВЖЯЩГМЯГЗЧЪМАМЗГГВГЖЗАЖСЧЯЕЪДГЖЗЭВЕИЯКИДГДЩСЭ

(b) Расшифровать текст:

ЯГЙИБЪИЖГЭФИДЧПБОИЭЯВНПДВФВМЪЯЧАГШЭВУДААСЙИВЧСМБМЕСМОЧЯФИЮЭГБГДШ
ЯФЭНГЮФЛГЪЯЧАИШЭУАЗВЦСЙМВЬЬЭЗУЛФЮКЖФЬЙЯКУФЮЗГХЭЕГЯБВЮУЪФАЗЯМЪЪМИ
ЭЭВЩОЪУЬМБЮВЦМЖЬЭЭИФЧУЯГЙИЯЭВЙЮЙБЙЛЕЪЮАМЧАШЭДВЧБАЭЪБЯГЛГЮЬГОЖЪМН
ЛГДЭЗКЦВБГЗЖАЬЕИЕОЧГЮВАСИБЭГЩВЗЪЫЪМЖГФЭЭЧКАУГЖЕГЬЯБЧЪЕЯМИРБАЭЪФЭ
ЖЪШААОАЕОЫЛШЭФЬЙЮВУКМОЕАСВЯАЯВЖЙВЧТЙДЩАТЯЗЖОЖНКДЧЯААВЧНОЭЭЫЕАБЕА
УГОЪЭФДКВЩЩЛЧАЭЧСКГУФГИЭВВЕИЭЪВКЗЦЧЦТПЧГБЭЖЭЯВЖНЯЯФДЙГФМНПБЪЬООИ
АЖАЙСГЫАЗГФЩЙИВДВЭОЪВЪМШБААНМЭЯЬВЙЯАЫКЗНЪАНЗИЗХГЮЗОЦМЮГЧНЬМРКЬАЪ
ДЕТТБЧФКУБАЪЦМЮЪДЪГТРЪЫЦОЕАФМКНЭЧЭЯГГБГЙИРЖНКЧКФЬЗШАЯЙАЭЧАЕГАГЫА

НСБВЮУЪФСЦМИЙЧЖДЯВАИПУЦФЭДЛЕЩЕАИЮФУШВЧЮЙНАДЛЖДЬБЭККБЦЬАГЖДСГОСЭЧ
АЯГАРЭБВЙБЧЛАЧЫИЙЭИВККЫЭВДЭИЦВККЖШФИЧБАБСКБКСЬМЭЯУЛПЫЬЭЩГЯЕБГИЬБ
ЛАИЭФЭЛКЗЩЮЛББЙФЮКГБАЖНЗАЧМЗИЙЧЖКЖОЗЭЭЕЪЬОНАНЗКМЪЦЪЙВЪЯЧАЛИХЖАЮЧ
НЗАЗЭЩААЭШААОАЕОЦЕМЭЙЪЙЙЧЪАМОИБЪАЙЭЪСГЙГФБЭИЖАЪЮЗВАЧЮМЭЯФЭЮЖАРЗЙ
РФФНЩЗЦФЭПНЬЬАЛАЧЫИЙЭИЦЯБНЯФЮКДАЮЙЙЩАЖЧДЧЯЫГМГЯЭЭЖГДЭЛЧЮЬЦИБВБЯГ
ЮЬДЧГГЩЧЗИБЮЬЯАЛГГБГЛИХЖАЮИГБЛББЪЪИИЪЯЭЮЙЪЯЬЦБЖФЭГЯАЩМНКМДЭАХЪГЮ
ЛКЖЪЪЙЙБЧЬМЙЪЦЭОИЪЯЧАИНФРЛДВГЩВЗЗЧРАЛЕФУОКЗФФТЗЖДСАМЩААНДУДКЗЙЪП
БЙЯГЯФМЖЬЭЦЗБЗЪЪКПШЙФЭПЯАФЮКАЪЕЙКБВЖГЗГГЛМИЗНЯМНИЦЧЙОЧЧЖЖББЕЫЙВВ
АЪГЭРЭЭКМЭДСЙДКЭНЯСГУЙЭДЗОЖНКЩАЖЧИЭВЭИКЧШЧЭАГЯЧЬЧЪЧЦЮМРЩЪГЙЭЙБЙБ
ЪУКИБЖБАЖКЭДЭКМЧЦАЕГАГЫАНСБВЮУЪФЫЙДДОЬГТРЯФККОЦЧЖДЦНРААВЕНЯБЧЕЗЕ
ПКАЯЙФГГУАЗАЬВЗПНЬЮЙЛЩОЖНКГУЫИПАЪДМЗИКШКМГЦЭЖВАФЧЯБШАУЙЭЕАФЛНДАЪ
ЙВЪЯЧАЖЯДФЬЙЬФБЧЙЪЩЬЩАЭЩЬНШВЧДЙУИЯЭЬКШФЧЯДЗЙБЙВЭЩЬГЪБАФДМЩУКВЛАД
ЧНШЗЧРАГЗАЖНКЗНУЖИЪЯАЯБАЭБЙЗСЬЭИБЗВФЬПЮДЭЮКМДЭКМГДЧЭЙГ

2. Разложить на множители числа:

   (a) 935179906206350515092203439797

   (b) 509418187976571145425704216563543073775415364976825215800397

   (c) 809995631244156030519984739866083335540188107382907579938225828824906662771715160869567947

   (d) 133572957544617962302841843930195778726885445027138496467955374184880089471531597260919972677507972189661522109886943648 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 5442952204470191839515084311893767297508631405654704541733448703510165153730 1$
   - $e = 3$

   Сообщение:

   - $M = 162637170289519361361769686961325701425969001749550092882853009266889793430 70$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 307438062838544250182641725494289335177$
   - $q = 177659734193294438238500989701904359901$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 248330811129647181139078010705038708862553846827853601932466175580646837948 63$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 136753253204640661371917362903127776027$
   - $e = 3$

   Зашифрованное сообщение:

   - $c = 458721520298686210581587763060644258 84$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 288347926794207356428638139815090988399$
   - $g = 112235090541550089801000328875979847282$
   - $y = 170490032369053682764127619964857902599$

   Секретный ключ:

   - $x = 277174505249431515032492141017146557 2$

   Сообщение:

   - $M = 885960591493593732941938926848469549 22$

   Использовать следующий случайный параметр для создания подписи:

- $k = 33305779211118104911796529580761024415$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 27097431568668668813139139236678316892 9$
- $g = 54282075308686843083475835172943393099$
- $y = 99490690589686043245808562085826821359$

Сообщение:

- $M = 84290399658582701970339057301148426451$

Подпись:

- $a = 17349747837241196931762631522685557443 2$
- $b = 14252892467350569901770133960240348855 5$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 659$
- $g = 482$
- $y = 286$

Сообщение:

- $M = 321$

Использовать следующий случайный параметр для создания подписи:

- $k = 67$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 2x - 12$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 66

1. (a) Расшифровать текст:

ЯПРМЛНРИВЯЮШИОШПТЛПЩОНЛБРЛКОЯЕНВМДФВЙМЛГИЛЯПЩЕДЯЛИЕИЯЙЛЖЯВНПВМОМ
НЛОЕИЛКИОЗЛЯЛОРЙНЛЗЛЯЛОПЯЕИАВКВНИЕМЛОМВХЕИКОЯЛЫЗЯНПЕНРОЯВИЩЕФЯОП
НВПЕИЙВКОЛЮШЗКЛЯВКЖШЙОЯЛЕЙРЯВЦКЕВЙЛТЛППВЮВОРБНЩМВНВЯВБШЯПЩООМЩКШ
ЙЕНДЮЛЖКЕЗЙЕЮЛНОЗЛВИЕЪПЛБВИЛКВНЯВКФОКЕДФПЛМНЛМБВХЩЕБЛЮНЛЮШРГТЛБЕ
ИПШКПРНЗРЕИЕКХЯВБПЛАНВТЕОЗДПЩКЗЛАЛМНВНЯИВАЛНВФЩЯЛМНЛОЛЙОЗЛИЩЗЛРЙ
ВКЯОВАЛКЯОВБВКВАЮРБВПОПВЮЛПЯВФИЛКОБЛЯЛИЩКШЙЯЕБЛЙЙЛХВККЕЗЕЗЗПЙКЕХ
НЕИЕЯОВПЗЕРОМВИРПЕПЩЕОЪПЕЙОИЛЯЛЙЛКЯШКРИЕДЗНЙКБИЕККШЖЯДКШЖЗЛХВИВЗ
МЛИКШЖОВНВЮНКРОЯВИЩЕФОЗДИВЙРЛПБЖГВЙКВПВМВНЩМЛИЛЯЕКРЛОПИЩКЛВЯЛДЩЙ
ЕОВЮВВБРЯЮВИЛАЛНОЗРЫЗНВМЛОПЩЮПЫХЗМВПНКБНВЕФОЗДИБЛЮНШЖББЩЗБНЛГЦЕЙ
АЛИЛОЛЙМЛЮЛЖОЮЛАЗЗПВЮВМРОЗПЩОЯБЛНЛАРЯКШКВХКВВЯНВЙЗЛАБКЕЗРБМНЛВДБ
РКВПЛПНДЮЛЖКЕЗЛЯМЛГИВЖПШТЛПЩОЯЛЕТНЛБЕПВИВЖЗЛИЕОЙОВЮКВГИВВХЩЗРБПВ
ЮВВТПЩДФВЙМЛАЛБЕЙИВКЩЗЛЯЛЖОЗМНЕБРПМВНВИЛЯПЙЛХВККЕЗЛЯПЛАБМЛВДГЖОВ
ЮВТЛПЩКЯОВФВПШНВОПЛНЛКШКЛКЙВНВКЕВЙЛВЮШИЛПЯВНБЛМНЕКПЛМЛДБКЛНООРГБ
ПЩЛПЯВФИОПНЕЗРБЛИГВКВТПЩКВЙЛАРКВВТПЩКВПРГЕОЯВИЩЕФЮЛАЙЕИЛОПЕЯЯЛОЩ
РЯЕБЕЙООЙЛПНЕГВКВОЛЯВОПЕОЩЕКВОЗРМЕОЩМЛЗРМЖФПЛПВЮВЮРБВПКРГКЛТЛПЩЯ
ПНЕБЛНЛАБВКЩАЕЪПЕПВЮВБНЫВОИЕФВНВДПНЕБККВЯЛНЛФРОЩФПЛПШЪПЛОРБНЩМНВ
НЯИЙВКОЯВИЩЕФФПЛЮПВЮМРОПЕИЛБКЛАЛБЪПЛАЛЕЯЛОКВКВМНЛОЕЗЛИЕПШРГНВХЕИ
ОВТПЩПЛТЛПЩМВХЗЛЙБМЛЖБРДПЛЮЛЖПВЮКВМЛЗЕКРФПЛЮОПИЮВДПВЮОЕБВПЩДЗЙВК
КЛЖОПВКЛЫБНДЯВОРЙОЛХВИЯЛИПЯЛОРБНЩЛППВЮКВЛПОПКРДКИФПЛООЯВИЩЕФВЙОМ
ЛНЕПЩЮШИЛКВФВАЛЕМЛДЯЛИЕИВЙРМНЕАЛПЛЯИПЩОЯБЛНЛАРФВНВДМЛИФООВИКОЯЛВ
АЛБ

(b) Расшифровать текст:

ФЛШТЯЕЭЛЫЫТЧХЩЯЦЖЩКЕМЦЧЦЫМЬМУГЫЬХЪБТУФНЩЙЫЩНДЙЧЛЦШСШПЧЗМОФЦЪТЛТЛ
ЕИЪПУИЖПТДЯЫТТНЪХЩЩДЩТОФЦАОШУХЙЙЫОЫЗМЧВФЗЛНХШОЙЧФГАММОКЕПЧХКДСЕР
ШЮЕШТЪВХСЪШЯСЫФЯВХШУХЕВЪОЛЕЖЪПКВТЯХЪДТЧХФВТЩХФВЧЫТЦЩЙНХЩЙПТЧНЭЙТ
ИНИХМОХЬЙЧСЦДЙАЙФЬХЬХЦЙЖПЩХБОШРЪЕЛЩЧЦИТЧОЭЗУПТРЖФТШКЯХЬФЫВЛЦХУОП
ТЙЩБТЪМЧЕХХММЕЖХМЛЕУЪПФЬФЭФМЗЧНХСЫЙЧГЫЙФШУЧЗМВМУБРЪГНЯЖЧХКДЙЫХЦШ
ЭТТНАХМХРЖФПЛЧЕПШННДМШФЧЗМСФУЯЩЛТЛЕФСЪФЯЙТЩЦЙЫЫШЦГСШЕЩЕЗХШРВХЖХЪ
ЗИСЪШЯСОХУЭЙЧИГВЖЕШЪКУТЩДЯЛНХШЕИМЩЦЙКПЛНДАЧМЯЬЗШИГВТЦММВМЬГЪКЦРМ
ШИХЬТЩИРЪГНАММФЦЩСШРЧЕФЭЮРЩЙПШКЬПЖПЯКМОЙНАУТШДГТФУЦЯРЪХМЯЦПТФГФЖ
ПКДТМФПЖПФТЧЗТГРЪЬУПЩШДИЪМРОХФОУЕСЬПЭЯРНХУЕХШУЧЗМОМЪИПТФФКЖТЛЪУХ
ТТРДЙЬИЦЪТОПХФЦШОХЬЦЧХКЬОЧМПШЧОЪКИИШУЦЪМХВЪТТОПХЕХЬФНПАЫЙФЕЙЦШНЗ
ИАМХЯЫПКЦДЙЦХЛЕЦММЯЙАХЕМЯСЫХТЗЧРТРДЙЯХЪЬПЩЧРДМЯЦШЬИМЩДИЫЭЙЩЙЖЦСЦ
ЙТЪВНГЙЧЙЦВСШЙУЯСФХХЬЪШФЫЬЩХЙЦЮЖЪЩРВХФОЫЗМЧЪЛЗЧЫЩНДМЦХУОПТЙЦДЩШЩ
НВРПФШЮЖПШНВМЬГМКРХШНШФЫШНЙАЦВЧЗТММУЯИПФДПЧЦФЦЯЕЭРХЕММЯЬФШУКТХЬ
ЪЧЯПТЙЧЕЩШЛЕЙТЛВУЕЖФХХНЙЮМКЗПСПФЮЦЪЪМДЖВЙЦЬСЧВНЗХЩХШЭЙЧПЧЗТЯХМЯП
ТФАЯЗПФНЗПЕКЦЙТМПУЯХЖСМЗЧРФЦГЧЫХМЬНЫЩКЯВЩЪЛОЙМЙЩЬЙГМЩЙТХЦЦЫТЪМХШ
ЧЪКЦГРПНМКЦПУЦБТХХНЪТШЩШЫЯЫХНЫМЧТРИАТШЦЩХПЬЩЙТЪХХЖФТИУЯКХПЩУОСТЦ
ЫЙУШТЕРЭКХЬЛОЪЙКСЬЪЖРМПЛНЗЙМФРЖФТЙРЫЙЧЯРМЖШРЩБУЪПЭЕИТТРЩУШЙРДТММ
ХЯЙВРТЯФСИЦАСТСЦЩЖПОМЬЕПНУЯТЬФЩЯЖЫМЧЗЙОЙНРПШШТЕФШМРШПНХЧЕПЭЮХЕЙШ
СЦДЫЧПНЩХФХШЬОЧОДЪТХПЮТСЩХМБФПЦЦИЦТЕЪЙМГМКЕНЪОЙЯПЩЪЛОЙМЧЩИЙХМЛЕЦ
ШТЧТТЫЙЦШТОПУЕФПФЙКФНПТЮПШШДДСПШЙКСЬЪЧЕХХММДМУПШЬЬТЩНВАЧВСКИЪОЫЗ
МЧИГВЖЬХКЗЙЦХЪЗКПФЧЗТЬПККЬУСРГЦПНХТЩЛЯТЯФАМКБТЬХШТЙЬШЩЬПТШДЖФПНМ
ЬСПННВМЦВРМЧМПМВММММЩДТЫЛРВСЫЙЪЙФЫСЦАИПЧНЩЧВСНЗЙБСРЗЛХПУЯХЖПМЕФШК
РИЦХПХЬУЪХЭЕИТУГГЯЭЩНППТШДЩСВМФШЙСЛНАХЬЙРЯР

2. Разложить на множители числа:

(a) 595667318993273352502172742143

(b) 697038631669637662302369344177056249627916020386719920428701

(c) 10754128768354397635552796449995742144219563308114642672972553063411699395549303699702671 93

(d) 109210278858165372931011033165565746864366343421099120543496857690573159355622190083100529479000885302600988650780122104 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 675248102570186199137277320438642432831890890935744120619649547682846900219 89$
- $e = 5$

Сообщение:

- $M = 13428320414391584458099110431193262289100100142444199221449442906953876972 23$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 311237569026566261180331914781724418837$
- $q = 268885093592794778976204056281788226627$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 651913076150918442567355644052668715808054381180572539920241014413934301778 90$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 279019679540933953406032348298104637293$
- $e = 17$

Зашифрованное сообщение:

- $c = 946356980049903366839611931824496914 60$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 25065832827373102600087857259103126039 9$
   - $g = 60181117770844368479487312777513171502$
   - $y = 19082266022980420670683192895409467 9156$

   Секретный ключ:
   - $x = 10760765197161911109783738338499369 2703$

   Сообщение:
   - $M = 77284767667086102211293714979833228945$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 14669799449187406762118192708764092737 3$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 25087720649391280742152067671084742728 1$
   - $g = 24867046397627890804170808468474442724 1$
   - $y = 21832224161914444737038361016303394659 4$

   Сообщение:
   - $M = 14446192915913606509532482982720103627 3$

   Подпись:
   - $a = 89849690513410718381140075472847372950$
   - $b = 23502501459324671830598808701277121965 1$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 569$
   - $g = 455$
   - $y = 142$

   Сообщение:
   - $M = 197$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 489$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 2x - 12$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 67

1. (a) Расшифровать текст:

ЛКГИМКЙМЦВЖНМПИИЙЖЛОМВЛСЙЖФГМПРЛАЙЖАЙПЖИЙЛЙПАНМПНСБХГАИЖАЙБМЙМАМ
ЬЛМЯГПРМОМЛЩХГОГЕКЖЛСРСКЩАЩГУЙЖЖЕПЙМЯМВЩЖНМКХЙЖПЪНМБЙВИМЗВМОМБГЙ
ГБИМКМДЛМПГЯГНОГВПРАЖРЪХРМХСАПРАМАЙАЫРСКЖЛСРСХГОГЕЛГПИМЙЪИМХПМАВ
МЙДГЛЯЩЙСАЖВГРЪППРМЗИМРМОСЬНМХЖРЙСДГВЙКГЛНМРГОЛЛМЬАММЯОДЙПГЯГКЖЛ
СРСЛЦГБМПМГВЖЛГЛЖВСКЙРИДГЖМРМКХГЙМАГИГАХЪЖУОСИУЛУМВЖЙПЪКМПСВЪЯЖИ
МРМОЩЗНМПРОЛЛМКСПРГХГЛЖЬМЯПРМРГЙЪПРАРЖЛПРАГЛЛМЯЩЙПМКЛМЬПАЕЛАПНМК
ЖЛЙМЯМНОМКГРХЖАМЗДГПРМИМПРЖМИОМАМДВЛЩУНОЖАЩХИУРМБМИРМАЩЕЩАЙПЯЩРЪ
ЖЖЕЯАЖРГЙГККМГЗЙЬЯГЕЛМЗНСБХГАЛГЕЛЙХРММЛЯЩЙВМХЪИНЖРЛКЖОМЛМАМЕЙМЯЙ
ГЛЛЩЗЦАЯОЖЛКМБМРИОЩРЪГКСАПГНСБХГАКМБНОМАГВРЪЖПРЖЛСЖВОСБЖКМЯОЕМКР
МБВХРМПРЛГРППКОЪГЗЖАЛМАЛМЗУМЙМВНОМЯГБЙНМКМГКСРГЙСЖАМЙМППРЛМАЖЙЖП
ЪВЩЯМКАВОСБНСБХГАНОГОАЙКМЖОЕКЩЦЙГЛЖМЯОРПЪИМКЛГПАМНОМПМКМХГКАЦГЯЙ

БМОМВЖГЖЕАМЙЖЙЕВСКРЪПИИЛГЕВСКРЪПМРАГХЙГКСМТЖФГОЖВАМОЛЖЛАХГОГЧГВО
ЙПНОМРЖАСРГЯПГБМВЛГВСПРМЯМЗАМВЛМЗИЖЯЖРИГЖПХПРЖГАПГЗКМГЗДЖЕЛЖЕАЖП
ЖРМРРГЯХРМДПНОМПЖЙНСБХГАПРОЦЛМРГЯГМРАГХЙХРМЯЩАМВЛДВЩСДГЖКНМКЖЙМА
ЛЛВГЙПЛГРМЙЪИМЛГБМНМЧВСЛМВДГЖЛНМКМЧЪЖРЩНОАГЗЯМБСНОАПИЕЙПКМЕАЛГФР
ЩАЖВГЙХРМКМЖОГЯРПКМРОГЙЖЛРГЯИМПМПРОЖИЖПГБМВЛЛПРЖАЙЛРМКХРМРЩЦНЖМЛ
ЖХРМЛВМЯЛМРГЯНЩРРЪЖНМАГПЖРЪЛМЛГПМБЙПЖЙПНОЖЯАЖЙМЛНМЛЖЕЖАБМЙМПХРМЯ
ПАГЙЪЖХЖРРОЖЛЛГКМБЙЖГБМСПЙЩЦРЪНМКЛРАМЗПРИЛАЖЛЖЕЗХЖЗРСЙСНРЩАЖВЖЦЪ
ХРМЛГРИМЗГЧГИОМАМНЖЗФИИБМАМОЖРМЯМКЛГАЦЯОРЪАПНМКЛЖЙАЕРЖГЯГЙМБМОПИ
МЗИОГНМПРЖЛМЛГНМХГЙЛСДЛЩКГБММПНМОЖАРЪЖЛГМРАГХЙЛЖПЙМАХРМБМАМОРМЯМ
КЛГАМОГЛЯСОБГПНОМПЖЙНСБХГАНМКМЙХАЛГКЛМБМВБМАМОРХРМПРМЯМЬПЙВЖРЪРО
СВЛМАРМЛГХГБМПИЕРЪВЙРЩПГЯЕЛРЪЙЖФМП

(b) Расшифровать текст:

МСЧАСЮАЪЯМХЮЯВИЛЭЦЪПВВЧЧЦЗГЪБНЛЪАЧМВЪЖЧИЗЪГШЗЮВВНИНЩЕЧГЬВЪЕАВАГД
ХЖГЪХНИВАЪЧВАЖААХЯВАБЯВВАИЛЧГЧИМЧЪВГИЖЗЪЗЭГЕЧРМСЪХНИЦРЬМИЧЬЯМИВЪ
ЮЗБАЭФКЛСЧХНКСЯЪФААГУФДЯДАБМГЕЭНЗЧРЗНЮЭЬГДЫЖРЯЛИЮИЙРМЧГФКЬЬБНРЕК
ДЕВСЪЧУНАЪДВБЯЩВНИЮГМЧВИЩГШЗЕШГГТЮЕРЯЗБЦЧЭДМЪШАНМЯЬЯЗИЗТДНЭГЕЩБЯ
ББЧКЯШМЧМЯЯЬЯЫЛЗЕКМЙЕОЕПЖГЮЕЛЯЕВЭНЫВГЮЛЯЖЗЧНМЖЗЪБМГМДНЙГМЪСЕЖЧДЪ
ЗЪУГБИЪЮГНЬЪЖДЗИЗЪИЛИЮДАРМЕЩЭБЖЪЖДДЛЧГЭЪЗЖЯЪЛВКЕЕШЯЧРЮМИЩЧАПЗЭВЕ
ЗББЪЯЗМСЖФНЯЮДВЗЛШЪГНЯЩЭЯЗМСЖГПБЦГЫМВЯБЪРНЦЭЫХЖЭЖУДЭАРЮЗПГААОЦБЭ
ГСХЩЭГПЖВНЧЛНЕГЦТВЖДЕВЗВЪХНИЗМЯЗЯББДТТЯВЧРЖЪАБПВВЪЮОЕЯЗОЗЛЗЕЭРЦЧ
ГЩБКЗЭДЫЯБИУНЮЕГГСЦШГФНКГВЧБЯЕВАРМЭБАКЬРГКСДГЖДЗЕУЩГЙИШГЮМЯВЭАСЯ
ЛБАИЫРАЯДНЗЪКДЗБЕОЗЬВГФМЖИМЪКЛСЦАКЯЪЧГДПЦИЦТСЭИФДКЪВЙСИБГХНЙЕЧЦС
ЦЖЯАВЮЦРДНЕСЯАЖПГЗЧКИВЩАВЮРЧЭРЦГЦЪРМЭВЧЗЙГМЪСЕЖЪУБВВГФМВЛЪРЛИЪША
МЯЖМГСВГВГЙКРЧЭНМЧЖЧФЛЧГЪРЕЪЬНЗЛЗЕЦМВЭБЧЕЮИЗЧЛЗЪДВДЛЗВЯНЮИБЭНЛЕЪ
ЦРМЧКЬЙЫРБЧМЛДЖДЗИЩВШГХЧЪЙДКГБУСШНЯГЗЮЪАЯГВЧВЧОЯЕЪФДКЗРФКВЖЗНОКЭ
ЩФНКВГХНДАЪЯГКВГЮЪЛАЭЧВИЦРЭЗЮАЪЬНВМЗЧМВЪВЧОКГЭЩБИЩЭЭНЗЩВЪЛИЦРЬМИ
ЧЪЯМИШГГБИЪШАГЯЮЖДБВГВЯРЬЭЖДЪЬАЖДПВВВНИЖЕНЮСННЯЮНЕМЧЩКТЪЕГСЗИУЖТ
ОЮЯЕЗЛАЪЩЪВЬЕЧГДГЯБКВВЪЧПЫГЗЕБЮЕИХЛКСЭФМИЧВДТМЫЪГЗЮЪЧКЖКЦГДНГГЦМ
ББАМДНЗЪГУФИЩЭЮНЛЗСЧДБЖЗФКЯЗЪЗСЦЧДЧСЯЕЦЕПЭЭМДНИВДВНЛЭЗЦСЦЪЮГОИЖГ
УНМДЕФЗМСЖЮСННЯАЦЯВСАВИЕМЪКЛСЬЙДЖЗЪУДЬДЪДДКЦИВВЛЯЬЭНЗВЪЕЕМГББВЫВЧ
ВАБЗКГЙДТСЭДЪЗЖДАЙВВИДЫЖЕСЪБЗГЧЯНМЧЪЙКСЗГФРЫИЩЕШЛИЩОАЯЪЬФЗЛЭЗАСЧ
ЗГХНЙИЗЧЧЯЖЗФЗСЗГАМЯЩЪДЗЛЯЗООИЯЕАБВЗЪЭЫЛЗЧЪОИБГЛЗНЖЭЭЫЗРКЭЭЮЪЮЬЙ
ЮГМОЦЯАГФДДДГГСКЩЧКДЭГЬГБИУЧЧПЗГЖДЫИЗЪИЛИЮДАСНДЭЭВИАГФТЬЖЯАДЛАГФ
НЗДГЮЗЗУОЧДЖВЭЮНЯДЕЧРМИДЭДЗЭЪГЪЗЦРЭНЯБИДВИЖЗЯНВЯЬЭНЛСЯАКДЭБЕОКЪЯ
АЛЙГЪЩЕГБЗЕЧДЖЯ

2. Разложить на множители числа:

(a) 711588690046858063037059726697

(b) 697632436235842057499445913340718559007766886760353937884813

(c) 878231314096385937218988790633513616457277310639080583543354857762122528283370735865791813

(d) 173352290685757758087500174771191046365778144385477920166881311895152531169114225921440310288579792049125227891655624581 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 796631146767339564184175936801384598764194395437898647038225963630786790980 97$
- $e = 5$

Сообщение:

- $M = 44921721601528860375364561857527274308338561381909352022169400132678525968654$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 30119200187433635866717319204361311924 9$
- $q = 28665874975175784447807613204449113141 3$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 21856865750760527195009202936272854712571509469119557596154519801348648051670$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 134526986779469329131203130418112626657$
- $e = 3$

Зашифрованное сообщение:

- $c = 100897586194325805064962866010270754280$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 25139207127160480189166086834389846260 3$
- $g = 10523499638719908028942401312324862019 8$
- $y = 48105779575560381577095102436855455541$

Секретный ключ:

- $x = 88420934415026393666748937406660833855$

Сообщение:

- $M = 17362819611455822418685955273727158511 6$

Использовать следующий случайный параметр для создания подписи:

- $k = 19674167462930900466889290048257391647 7$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 18184890074543783917470438291340249873 9$
- $g = 15762331639833865700046583379315526257 2$
- $y = 64515384912280395701878152703398910482$

Сообщение:

- $M = 13803934377597244691917443369967449176 2$

Подпись:

- $a = 14912845112473711266644966368530171777 5$
- $b = 59628509009737839314940253777003879610$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 607$
- $g = 342$
- $y = 489$

Сообщение:

- $M = 404$

Использовать следующий случайный параметр для создания подписи:

- $k = 143$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 10x - 9$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 68

1. (a) Расшифровать текст:

ЪЮСПЪФШСЩФЩДСЧСПЪПЪЮЪОЪПЪЫЯЭЮФЮИЭОРЬЬЪПЯЩСШЪПЯФУЖЭЩФЮИЮЪГЮЪГЯОЭЮ
ОЪОЧЬЭЭЮОЭИЭЙЮФШЯТЭЩЗШГСЧЪОСЦЪШФУОСЬПЪШУЧЪРССШРЧОЭСБЦЬЪШСЪРЩЪПЪШ
СЩУГСШЩСЭЦУЮИФЭЮФЩЗОЙЮЯШФЩЯЮЯЭФЧИЩЪСЭЪГЯОЭЮОФСОЧСЦЧЪШСЩЦЩСШЯЫЧШС
ЩЩЪТСЧЧОЗЬОЮИСПЪФУЭЬСРЗУЧЪРССОЦЪЮЬЬЗШФЪЩЫЬСРОЪРФЮСЧИЭЮОЪОЧФЭЫЭЮФ
СПЪПЪЧЪОЯЫЪЦСЕСНЗЧЪОЬСШДОНЬФЩФЩЬЪРЮЪЧЫЕФХЭЪЦЪЧЪЩЭЫЪШСДЧФШЦСОЗЭЦУ
ЮИОЭСГСШФЭЫЪЧЩСЩЪНЗЧЪШЪСЭСЬРВСШЗЬЭЭЮЧФЭИРЬЯТСЭЦФЫЯПГСОЯОФРОЮЪЧЫС
ЦЯЧФЩЯЫШАФЧЪОЩЯЫЪПЬЪУФЧЫЧИВСШФШФПЩЯЧУЩГФЮСЧИЩЪЫЪЮЪШЭСЧОЦФНФЮЦЯОС
ЧСЧСБЮИОНСЬРЯФЦЪПРЧЪДРФЮЬЪЩЯЧФЭИЮЪЪЩСЕСЬУОЗЭЯЩЯЧЭФУЦФНФЮЦФФУЦЬФГ
ЧШЩСЫЬЪЕХОДСНЧПЪЬЪРФСОЪЭИЯОФРФШЭЦЪПРЩФНЯРИШЗЮЪГЩЪЭЩФШЯОФРСЧФЭИЩЪ
ОЦЦФБЪНЭЮЪЮСЧИЭЮОБЫЯПГСОЯСБЧРЪЧПЪЭШЪЮЬСЧЩНСЧЯКЭЮСЫИЫЪЦЪЮЪЬЪХЩСЭЧ
ЭИСПЪЮЬЪХЦЩЬЪРЬУЪДСЧЭДОНЬФЩЭЦЬЗЧЭОЬЬЪЮФЧЭОРЪШЭОЕСЩЩФЦОЭСНЗЧЪПЪЮЪ
ОЪЦЩДСШЯЪЮЖСУРЯЩСБЪЮСЧНЪЧССШСРЧФЮИРЪНЬЪЩДСОЭСНЗЧЪЯЧЬТСЩЪОЭЮЬЯКЦЪ
ШСЩРЩЮЭЦЯКЫЪОЪУЦЯШЕФЦФШФПЪШУЧЬТФЧФЧЪДРСХШЬИФОЩЪОЩЫЪДЧЫЬЪЭЮФЮИЭЭШ
ЪПФЧШФЭОЪФБЬЪРФЮСЧСХЫЪЬБЪЬЪЩСЩЩЗБУВСЬЦЪОИКБЪЮСЧССЫЬЪОЪРФЮИЩЪЪЩЫЬЪ
ЭФЧШСЩЪЭЮОФЮИССЪРЩЯГСЬСУЩСЭЦЪЧИЦЪШФЩЯЮЪЩОЪЬЪЮФЧЭИЪНЧФОЭИШЪЧГЮФБФ
ШФЭЧСУШФЫЪОЪУЦНЗЧЫЪРЩЪЮСВПСЬЭФШФТСЩСПЪОЗДЧФЩЦЬЗЧИВЪШЗЭСЧФОЦФНФЮЦ
ЯОЮЬЪСШШЬИФОЩЪОЩЭЫЧДСХФЭОСЧИФГУНЬЧЭЩЪНЧЯГЪЦЫЬЪЕХШЬИФОЩЪОЩШЪПЪЧЯН
ЯДЦЫЬЪЕХЮСЫСЮЬЩРЬСФГЭЪЦЪЧЩДЭЩЗХПЪОЪЬФЧРЪНЬЫЪЫРИЭГЭЮЧФОЗХЫЯЮИФРХН
ЪПОШЪНЪФШЭГЭЮФШЗЫЪСБЧФЯЪЦЪДЦЦЪШСЩРЩЮЭЦЪПЪРЪШЯОФРСЧЭЮЪЕСПЪДОНЬФЩЧ
ФВЪСПЪФУЪНЬТЧЪШЬГЩЯКУЧЬНЯЩСБЪЮСЧЮЪЬТСЭЮОЪОЮИЩРЯЩФГЮЪТСЩЩЗШОЬПЪШФ
ЪНЬЮФЧПЧУОРЬЯПЯКЭЮЬЬЪЩЯЩЦЪЩСВШЗОЗСБЧФФУЦЬСЫЪЭЮЩЗБОЪЬЪЮФЩОСЦЪЭЮОФ
ЧФНСЧЪПЪЬЭЦЯКЦЬСЫЪЭЮИПЧОЬСЭЮЩСПЩСОХЮСЭИЭЯРЬИЫЪРЪЧПЯШЪСШЯ

(b) Расшифровать текст:

ЪРЛЮДЪЧЩЕТАРЩНЦПФАСШЛОЧБВБФЯНОПССАШБЩЭСМГЭЪБЫГЗЪВШНФЪТБЛФЧСОПУЭ
РФАЦВЙШНОАЗЫЙЛУНМЙФАЛМКФТЗХСЧЫНЬООЗЫООЩТЗЯБЩРЗВЪФГЗАГЦЩМЦАФЪДИНЦ
ЧДЯЙШКТРЖИФЧЬЪЛТНЪЕИФЛХМРЯНМЖУББШГПАНМГЧБЗТРКАМШПРСПЭИФЮЗЫЖЧЪДОМ
ИЪНМЩЮФКМКЛАСППУЧЛТПИФКЖЖЭАСШЙЩСНЪМШУДЪДУЗЗЯЙФЗГПЗХЭПЫНФЯЕПЛОНФХ
МХВЧТИЦВКЖЛБШНЬАЛЪЛПЛИЮПТИНЬТИЖНРТНВЛЫДЧМЧББТЙОАРМГСЛЗБГТСЖЩГЦБЗ
ОВВЩАЕЙИБЙШКОЦТЦЙЛЬЗТЖШУРЧМЧЩЙЗРФЫТЦГЧБТШРУЭРТРЧЮПШНЩИДЧЛЙЪБШРЗЯ
НВГУЬОЭЦРЧМЕКОАНЯОУЧБВПШЭКЖИФСЦПОУЭБШКИБННОЪФОЪЖСЭЕПЛОФОЪМХВШПЛУ
ТКМКБЮПТЯСЧЕХЖЧЛЙЛГЦФВЦАФЪВТНФЪЙЧЦИАСЭНОЪБОГЦФБЧЬОЭРЬЛФСЗХПИЬДУЛ
ФЖДМРВАСЪМЧБНЛШИЧКЦЛЛЖСШЛШЭИЫРФЯНЧГИАДОГЦФБЧЖИЦАЭЛШЭБХЖЧЛЧУИОЮТН
ХЛСРФЖЛРПШВШСДСВЛМСШЖНСДЫРОФЛПЛЧЧКЖЛФСРЬОЛСНРЖСЭЛЕВФЪЕЧЩЗККТНЛЯД
ЩОИЧСЖПУУПЭБФШГПЛВВСЪМТЬДЬГЦЮДЧЖЛЭБХВЛЪНЦЛФШГПОЛСМШРЬЫНПБФЬФШВОЪ
РЖАИФПЫРЫЮНЬСЧБНЪМУВППИОАОЪМЧЧКЧГЧКШПРЧЪЗЩГЦФБШЕЭЧЙМПЛЩПППШЛМПЯБ
ЪЗЪЩЗЭКШАБЪНОМРРЪХМТЬННМХЯЗВГСЩВЪЖУФБЭЖФРЩМЖСФЛЭМЧСНПКУЫДЪГУЧЗЛГ
ЦФВТПВАЙСЙФЬЛЧГФУМШКЩФФЬЪФЮРЧМКЭЕОЖЧЛТЬОТКОПОЛЮПМЖТАОПОИКДТНЦЧБП
ВЛЫБНМЧБЗФРИЭЗЦОФУЗЬГСЫЦПЙФСДФБЩАПШАУСРФЖПАКЭХПЬРЬМСЬРММЛЫКШВРРЪ
ХБФБНМПЛЪБЧГЛАГМСТТППЯЬЫЗШЛОЭСБЙОЪЗТСКЯЗХЖИСДЫЙУФАШЯБЪНЫЛФЪТЧПОЪ
ОШБФУАЕЙШЧФММСТМППСАЫЪМИЬНТПХЭЙШЗУЭКШВРЮКМЛФЩЦЫЪЗКРЬОФАЙШЙВЦЗХНФ
БДЦЛБЫБШЙУЫОШБЦВЖТЙЧСЛПХШКБШМЗЯЕПЛОЮПШЦСЭНФМСЭОШЙЩЖРЦЩЩХДОМЧБЗНЙ
ОАДЪГКЧМЕОЛЩЗМВЦВВНОЛРХЕЛЭЪЗВГХБСЖПТФЕОСЧЭАШЬЭБНЬИФФРЩОФАЗХМЭЬТМ
ЦОАЫЧГНЬДЦЯФТБППШЛНЬАЛЖКТБЦФААЩЧЫНЬОИЭГЧСЧБНЪМУВВХЕТЭЗЩООЬКТРФХД
ЧНЦСКПЛОФЗЭАОУДХАЧВЛЪИЛЖСШРФЮКЕАЮФДМЛОЦОШАФЪВПЛЛЦМФМТКИЩОЛУЛПРХЯ
ЗЛЙОХКЫАЛЪДХБЦФАА

2. Разложить на множители числа:

(a) 577731013352608657025868713507

(b) 123882454695895229530856145146453247890279495042642252995366 7

(c) 135447766667374463955670924980257828124894622847883142628461720400959249594806002614454014 9

(d) 117225858204969755448017693728640033495147308693735236440355503398967550098906335651847940456630435964521771752667764094 7

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 610764903657422996506171047425051594112865622063369913627249050314245413026 33$
- $e = 5$

Сообщение:

- $M = 338873974292948280745529140280612490179698538965837085633154372873442292736 27$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 339593071821612157118004616481354023309$
- $q = 318569814774923744545447653201052966367$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 312802107649789840114259642614622698037325016470485167021719908187624769918 26$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 22404939001289718482965517619432564973 3$
- $e = 3$

Зашифрованное сообщение:

- $c = 152692519358641893181486994297569679459$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 23586268617490847497055416999831555 5973$
- $g = 10990594745556029085195954943527340 2405$
- $y = 13488574798541753500108041618981606 1483$

Секретный ключ:

- $x = 87144408556998553914841768487354270926$

Сообщение:

- $M = 19636064643090840345383497532779536 9744$

Использовать следующий случайный параметр для создания подписи:

- $k = 16450959536295688649541883050418688 5829$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 30484791057799105961533884210084020 3323$
- $g = 13566922155816589250381586197449932 6726$
- $y = 17729820805340910440472441091822715 1561$

Сообщение:

- $M = 22491595943031621314268968298715121 7551$

Подпись:

- $a = 21121063708403504970102230889788751 7589$
- $b = 14784552752888437470153452393916825 9247$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 571$
- $g = 446$
- $y = 404$

Сообщение:

- $M = 338$

Использовать следующий случайный параметр для создания подписи:

- $k = 457$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 11x - 2$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 69

1. (a) Расшифровать текст:

МВМНОМПУКГЛМДЖВЬЧЖУМЯВСКЩАЙПАМЖМРАГРЩЖОГЦЖЙПНГОГВПСВМКМЯШАЖРЪПСЧ
СЬНОАВСНМЙБПГЗПНМПМЯМНОАВЛЖПКЩКНОМПРЩКАКГПРГЖПКЩКЛВГДЛЩКНОЖГУЙАИ
ЕЛЪМНСПРМЦГЛЛСЬЖНМБМОГЙСЬНМСЙЖФКЛКГПРМВМКМАЙГДЙЖБОСВЩСБЙГЗЖРМОХЙ
ЖЕИМНРГЙЩГПРГЛЩЯГЕИОЩЦЖМИМЛРИМАЯЩЙПЙГВМПРАЙГЛЛЩЗНСБХГАЩККГЛНОЖАГ
ЕЙЖАИОГНМПРЪСФГЙГАЦСЬНМПГОГВЖПБМОГАЦГБМБМОМВБСПОЩПВЙЖКГЛИОСЙЪЛМК
СМТЖФГОСМЛАГЙГЙИЙЖИЛСРЪИСЕЛГФЛВГЙЖКЛГЛЛМБЖФГНЪЖЕИМАЙЖГГЛБЙСУМНМР
МКМРАГЙЖКГЛАРЬОЪКСЖМПРАЖЙЖМВЛМБМАРГПЛМЗЖРГКЛМЗИЛСОИГПМВЛЖКЖБМЙЩК
ЖПРГЛКЖЖПМИМЦГХИМКЕБМОМДГЛЩКДГЙГЕЛМЬОГЦГРИМЬРИМАМГЛХЙМЛГНОГВАГЧЙ
МКЛГЛЖХГБМВМЯОМБММВЛИМДЛГРГОЙЛЖЯМВОМПРЖЛЖЛВГДВЩНОЖЯГБЛСЙИСРГЦГЛЖ
ЬАПГУПИМОЯЧЖУЖАНГОАЩГАИСПЖАПЙВМПРЪКМЙЖРАЩЖЕЙЖЛЛМЗЖЕХЖПРМБМЛМОПРГ
ОЕЛЛМБМПГОВФПНМИМЗЛМЕПЛСЙЛГЕЯМРПЪМРМКХРМПМКЛМЬЯСВГРЛВОСБМЗВГЛЪРЬ
ОГКЛЩЗПРМОМДКГЛОЕЯСВЖЙПМЯШАЙГЛЖГКХРМКГЛРОГЯСЬРАИМКЖППЖЬВАПМЙВРНМ
АГЙЖКГЛХГОГЕВАМОАИМКГЛВЛРПИМЗВМКМПРЛМАЖЙЖПЪАНГОГВЛГЗЖАНСПРЖЙЖМВЛ
МБМАМАЛСРОГЛЛЖГИМКЛРЩАМЦГЙАЕЙСВМАМЙЪЛММЯЦЖОЛСЬЕПРМЙМКНМИОЩРЩКЯСК
БКЖПЖВГЙЖВАХГЙМАГИНМДЖЙМЗБГЛГОЙАЖВСПРОМБМБМЖУМЙМВЛМБМЖКМЙМВМЗБАО
ВГЗПИЖЗИНЖРЛЙГРВАВФРЖМПЪКЖМХГЛЬНОЖРЛМЗЛОСДЛМПРЖЙМАИЖЗЖПАМЯМВЛЩЗА
МЯОЧГЛЖЖСМИМЦИЕМПМЯЩКПРМЙМКПЖВГЙПГИОГРОЪПНГОМКЕСУМКЛИЙМЛПЪЛВЯСКБ
МЬБМРМАЩЗЕНЖПЩАРЪКМЖНМИЕЛЖЛХЙПВМНОМПКГЛПНОМПЖЙЖМКМГКЖКГЛЖЖЕАЛЖЖБ
ГЛГОЙМПАГВМКЖЙПЛГПЩЛЙЖЛВОГНГРОМАЖХБОЖЛГАЖЛМРАГРКМЗАМЕОЕЖЙПСОМАМД
ЙЪХРМРИМЗНМХРГЛЛЩЗХГЙМАГИЖКГГРРИМБМЛГВМПРМЗЛМБМПЩЛПНМИМЗЛММРАГХЙ
ХРМИИМАЩЯЩЛЖЯЩЙЖМЯАЖЛГЛЖРБМРГЬЧЖГЛКЛГЛВГЬПЪЖУОППГРЪХЖПРМПГОВГХЛЩ
КМЯШПЛГЛЖГКЖПРЖЛЩСАГОГЛЛМПРЪКМГКСЛГНМЛОАЖЙПЪРЩЯОРАМПРГОПИЕЙМЛКЛГ
ЛУКСОПЪЛМАЖВЙЖКЩЖЛГРИЖУРМБВКМЙМВМЗХГЙМАГИПНОМПЖЙКГЛНМИИМКСПЙСХ

   (b) Расшифровать текст:

ЫЙГЧЛЧЕЯЗАЯИЗСЯЭЬЩХЕТИВНЯАИЖЧФЧЕЭНВЦЫЪЛЭЧЛСЗФЭКГЧФЙЯКРХЯВВКФЧБВН
ЮЕЯААЫМЛЯЙВЭЗЖЦУЪЖЭТХЭЕГЖЕЬМГЗЛЧДЭЩДФДАНФЭЬЖКГБИЕУЯКЭИЦВКВКФВФЛА
КЦЭЬАНВВЫЭРЪЧПЧЧЭЧЬДРЧЬЭЕНЯФЬЖУГЩИМНЭАЕГЭЦЧЙГПЭЭЗЭРГРМУЭЬФВВЧЕЗД
ЪНЬЯЯДПАЮИЫРЮЬЯЕШЬВДЖЧДЧАЪФАУИЖФЧЬЛЯМЭЭЗВСФЭМЭЧФЭЗЪЗЧАМБХОЧЬВУФЬ
ЙГПВАЗЪРБЭННЧУБШНПЬЬЯБШБЭЮГЭЧЪВЦРХЭЮЕНЭФЭГЦФЧЮГСГЮИЯУЫЬХБЪАБВЗХА
ЬНЗАЮЫМИЭЬЭЫВНЮЬЯШУЯЦХЧТХФЕГСЪЦЫЧНДФЕЪСЮЧЕГЦДЧЙЕУГЧЖЯТЮАДЬРЧЫНЦЧ
РЗДЭФАСЯАКХЭДВСФУИБФВЭПГЙЮЧЖГЭФРКЭТХЯВВКФЭЛЗТАСВАЦПБИЯЧААЙЕУГЧЕГ
ТХЪЮВХЯФЗГИАММГЦЮЮКЪЙФЭЮЭЧЧЪЦВЬЭЛЗЭПКШДЭУДСЯМРЮЭГГЧЧЕЛВКЬЭМГХАШЭ
ГХЦЭЛЗБРЭЫАНЙНУЪОГБКГИАСИЭТУЭЭДУЮЭЭЩХЗЪИЮХЕЩЯБУЧШЗЯМДЛЖГРАУИШУЩЪ
ИЩКЪЭМГСГБВЗБЧЫНЬПВЭЬССАФЭГЦНЬЧЗУКСЫЕНЯАДЬРХЯВВКФВТЧЖВЧЗГЬЧЬЦЕЙХ
ВЛЕАФЭБССЪБЯЪИАУЛЯМДЛЗНКЮВЕЪПВНСЗУУЭЗДКВФЬЬРЧЫНЕТЕЧЫЪХЧТЯШУЬЩБЪТ
ЪЕНГПКСЫЕНЯЬЮГЖЯЭЗЪФВФЖЪТЯЭЙЕКЦАМЧНДЛЬЖКЬЯЯЗТЕНДЬТГЩНУПАЫВЖЦЪНИВ
УЦЧЗЭМХЪЬВАЗЮКЪЦДВЙВНЬЭЬЭФАЩБВНЧТИЩУЭХЗРЖНБЦЧЛЯКТЧЖВЧЗГЧЬЯХАЧАЫЗ
РОФЦЭАЙЯЪВЛКЧТИВНЙФЭГТЧЧБГЖВХЕГЦОЩКГСЧГВЬНЙФЛЯУЫЫНЯНХВЛЕААБЗЪЦЭЧ
ЯШУЯЮЕОКЮКЬГЭЭЧЬЯУЮЬМРЦДЯЯДКДЭЖЖСАБКЪРФЭДЕШХАЯЦФВЧЙГСЪЬЛЧУЪЫЕЩКЯ
ЖЯЖПЪФЭГЙНЬВМЧАСЮГСЧЬЯЭМЮФЗЭРААЦЧЦЧРХАУЯЮКЪЛЯФЖБКГБЯНЗУЯВВТЧУИЬЗ
АЪВАКХЭКЬИВРВЗБГЭПЕТФАЖГСГСИЪСЕЬВЫКЯЧВВКФЭЕСТАФИЗЗВИЯВНЧЭМЦКГЖЯЖ
ЧЯЭЭГПАЯХЖЧАЪШЦНГЪНШНФЧЕЭЦОСЙЪХЧУЗУГАЬВВКЕЖЛЗЗАСЕЭЗУВЗЗКЪЭММНГБИ
ШУГФКЩЫВУИЧРЪАЦВЭЧЫНЭМУСЕЪТЪНЛЧКЭЛВМЧАЯАЪЦДСИЧРЯУИЦТАЦЗЗБЙБИЧУФЯ
ЯБЧВФЬГИЪЮКГНЩСЯЩКЯЬИЮТБУЯВНЧЫКЬЖАШЗЭПАСИВФАРЯЫРФЩИВГКЬШШЙЧАМГРК
СЫЕНЯЪИНЙОЭЛЪЙЭЪЯЪЗНСЯАЧЪДИВБЬЭВЦРХЭЮЕЦЕЫМГЪЧЬЯЬСЧБЗРСАРКЬУЮЮИЖП
ЬЪДДКВФЬГМЕЭЗЧЦДЯЯЗНЭЮИАПАБЮРЪФЗВЮШШФЙГЦРАМГХАЬНЧУЭТВШХЪЬЯЧШЩЬЬГ
ЧЯФЭГУУЬТЪОАЮЛВУГБВЧК

2. Разложить на множители числа:

   (a) 342691547954751884660939695481

   (b) 109120466578626263741639974775043804989727732901892267179778 9

   (c) 1078848809234904867253043747205605568743854967066858838190684630585961059463190209698047137

   (d) 219661090749913334895200602193707781870357500950806723908248376966458985819045070313058053794129912165832189674255861107 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 58562926357072392971215957238675713148527251725312444598070451610765130228423$
   - $e = 3$

   Сообщение:

   - $M = 156575408884137690579140155680719859858369160853492764743340103264313874438 42$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 213010014789587171783791641092392304747$
   - $q = 235531279094844399033557515927864959019$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 49614639669364841838152970356362156553894472402740785763213834877591450500932$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 18221631414225586464420803717983848 2831$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 14818078427010987692664233203922147308 1$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 311000718338262983578878692160248407333$
   - $g = 279642217143336935118970127423012692968$
   - $y = 142924920194052661164820507983962583996$

   Секретный ключ:

   - $x = 204708002654811107887071489306475198 02$

   Сообщение:

   - $M = 57986943994918251601441890868097745 71$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 73734035437118203438317578442814441475$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 27043611639952100682837144165784993 2811$
   - $g = 10112736705092605577822289241865460 8651$
   - $y = 22261074982347057242898318900874443444$

   Сообщение:

   - $M = 16714693402093193950817480349408660 2641$

   Подпись:

   - $a = 26759730330669483173734133349738406 6296$
   - $b = 75651901812696515811759835725712097677$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 853$
- $g = 491$
- $y = 417$

Сообщение:

- $M = 518$

Использовать следующий случайный параметр для создания подписи:

- $k = 347$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 8$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 70

1. (a) Расшифровать текст:

ВЛМЕДЛЖИБЬЗРНЗЯВБЗЯЬЯАЯЛМЬВЕЯЭДИЬЯКВЗИДДЫЯБЗКЬЛМЬЯ3ЗХГВЬКЯЮЗХГЗЯ
ЭИЮГПЗЯЙКЬЮЬЛДКВДЗНЕЖКЦВЬЗИЬЗДДЗЯЙКЬЮЬИБКБВЕЮЖЬЛЬЛЙХПЗНЬЗЯЙКЬЮЯГ
ЫИЭНЗЯЙКЬЮБЗШЬЛЯЬЛЯЬЖКЛЛДАНИЗЮЕИЮЗИГЖЯЗЙИЮЬЯКЭЕЛЬЛЯЖНСМИЙИЛМВЭЕИ
ЯЭИВЯЛЕВИЗ3ЯИЙКЬЮЕЛЙЯКЯЮЛНЮИЖМИКБЬЯЙИМИЖНМИЕЦДИСМИЗЯПИМЯЕБЙНММЦЖ
ЯЗМНМИЗЛАКИЖКЛЛДБЕЬЛЯСМИНАЯВБЬЯЛМЗИЖИЯЖНСВММЯЕШЮЖЬХЛЕНТЕЯЯЛИЬЗВЖ
ЗВЯЖЭЮЯЬХИЛМЗИЬВЕВЛЦЛЙКИЛВЕИЗЙИМИЖВНЛЕХТСМИНЗ3ХЬЕЛЦЯЬЗХЙКВЖИЕЬВЕ
ЛНЕХЫДИШБЗШЙКИУГМЯЗЯЭИЬИКВМЯЗВДИЖНИЗТЯГЬЛМКЯСЯЗЮЯШЛЦСМИЬХЗЯЮИЕЭИ
ЫНЮЯМЯАЮМЦИМЬЯМЗЬТЯЙВЛЦЖИЛЧМВЖЛЕИЬИЖИЗЬЛМЕВЬИТЕЬДКХМНШЕЕЯШЖКЦВЬЗ
ИЬЗЬИБЬКМВЕЛЦДЗЗЯЬЕЛЦЯЬЗЯВЛЙИЕЗЯ3ЗКЮИЛМЗИГЗЮЯАЮХПИБГДЙИЫКЗВЕЯЯБК
ЗЗШШИЛЯ3З3ШШЙКИЭНЕДНЬКЯЮЗНШЙИЯЯЛЕИЬЖЮЕБЮИКИЬЦЖИЕИЮИГЮЯЬНТДВИЗЙКВЗ
ЯЛЕЛЖИЬКВБСТДИШСМИЕЦДИЫХЕИЙКВЗЕЛЦБЫЯЛДИЗЯСЗХЯКЛЛДБХИЮЬИКЯДДЬЮКНЭ
ЙКВЮЬИКЗДКЯМИЛМЗИЬВЕЛЦНДКХЕЦРВДЖЯКЕДЯГЬИТЯЕЛИЫФЬЕЯЗВЯЖСМИЭИЛНЮКХ
ЗВБЬИЕВМДЛЯЫЯЙКВЭЕТМЦЮЯЬВРНЖВКИЗИЬНЗ3ЬЕЛЦЯЬЗВБНЖВЕЛЦВКЛПЕИЙИМЕЛЦ
ПМВЭИЛЙИЮВБДКВСЕИЗЭИЛНЮКХЗМКЯЫНЯМЬЛДИЮЬИКНДДАЯЧМИИЗЙКИЬЛНБЗЕЮДДА
ЯЬХЖМНТДЙКЯЮЛМЬВМЯЛЦДВЖЙЯКМКВРЯЬХСГВЛМНЙВМЦЙИЙКВЮЬИКЗИЖНЗЯНЖЯЯМЯ
ЗЯЙКИЬИЮВМЦЕВЖЗЯЬЛЬЛЯМДВЬЛПИМЦЬСЯЖЗВЫНЮЦЮЖИЭНЙКЯЮИЛМЯКЯСЦВДДАЯЬЖ
ЯПМЦЬЮИКИАЗИЖЙЕМЦЯЗЯЙИЛЕМЦЕВДЙИЬВЬЕЦЗИГЫЫНТДЯБЯЯАЯЕМХЖКИЫКИЗИЖДЖ
ЯКЕДЯГИЫФЬВЕСМИЭИЛНЮКХЗЯНЭИЮЗИЫХЕИСМИЫЖКЦВЬЗИЬЗЯПЕИЮЗВЬМИЖЬСЯЖЯЯ
БЛМЗНМЮЯЕМЦЫХЕИЗЯСЯЭИЖКЦВЬЗИЬЗЛЯЕЬДКЯМНВЙИЯПЕЬИЮЬИКЯРЛИЙКИЬИАЮЯЖ
ЛИЬЯМЖВВЫЕЭИЛЕИЬЯЗВЖВ3ЗХЬЕЛЦЯЬЗХЖКЦВЬЗИЬЗЙКЯЮСНЬЛМЬИЬЕКЯТЯЗВЯЗТЯ
ГЛНЮЦЫХЛЯКЮРЯЯЯЛВЕЦЗИЫВЕИЛЦВБЖВКЕИСКЯБЗЯЛДИЕЦДИЖВЗНМДКЯМИЛМЗИЬВЕ
ЛЦНЮЬИКРЖКЦВЬЗИЬЗ

(b) Расшифровать текст:

ДДЩЙКЬЛЕМЖЬЛЕСДВЮЯЦМХБЗЕЬЬЛВТХЩНДОЫЗУЬСЛРНГОДВАКМЛЗФБВКЯБЮХЖЮГТВ
ДАЙЬБЮДБОЬЕВБЮДЗДКЩЬЮЕЮЬЛХЬУКСЕВОЗЕЛРГЫИЛЖБАНЭЩЗЯНЕЩЙЮЙРЬЕЙУДЗЛИ
ВЮДСКЛБЕШХШМХПИЕДЦЖЯББЖЖКСКЦБВЬБЛБГИЗЖЛЗВБЯНЩДЗДКЪУЗХЗЯВКРНВЕААД
ЩТМЪБДОРРЛЗИЮЙЗЩСБАЭЯРКЮЯЫЕЭВЗЭЕЖХЧВПЙВЭТТХЕПЙКБШЗЮКМГЖЯНМЪЙТХЫЩ
ХЬЙРЖКЯБФЯКЖОЙЗУЬНЗЕЮЬЛХЬУКОКЖЙЕВБЯНЩТЙЮОЯРЮЕЮЬЛХЬУИУЛДКЙПЙЦДВСИ
ВЗЩКЕЕКИКМЛЯВДЮЖШЯЗ3ЮЙДГЙЫЙТЙИЩМЬУДВЖЖОСЩЗШРЗШДЙЬИВЮИЕЕЮКГНЛАЮЕШ
ЮШЮШИДЯДЗДЖЗЪКВБШБВВФЕКБОЬВЭЗИЖЯБЙТЙЬАНТБГОЯСЭЯДДНФАДОЕЙБЧГИМЕИЯ
ВОЯОЬСГЬБГВЙЗЖЬИКЖМКБГВЕЩЗМХСЕНБЧМВСЕДЖЬРЗАЖЕТЗДЧАПЙЬЮТИЬДЧПЕЫПЛ
ЯВДДЪГКМЦКЫКБГМЯПЙВДЪРФМБЫОДЪБДБФЯЗЬЗЛРЛЕДЪЬЗВИЙШЙОЕЛЦБЗИЖЮСИТДЕ
ИЕТЙЩОУНБЙДЪРМЛБГДЗЯБЬОЖГМЕДЗЯВВСХЖБГПЙВЯКЛГЬЙОЕЛЦБЗИЖЮСИТЖВЮЯЛБ
ЕШОЩЮГКБНГВЙЬЦЕДЖЬРЗЕОВСИВАШИДЯДЗДЗАЭЗИЖГМЕИАББИНЭБДГНЮЕЖЕЛХЮКИИ
ДРЙТХЫПМЭЕЖЬЕЩВБШБДДЬДКШНЗЧКИЛЗЦДЖРЮШЗЕЖБЯИДЕКПЯЗТХГМЙИЧВОБЗДЕЛЕ
НЮЗИЬНБТЩЙОИВЖЮЛЗЕШЬММББЩИЭЬИЕММЕОЗНЖПИЕНИВЯВДЮЯЙГЕЖЮЖШЫКЕКЭЛЮБД

ЬМЗШЙБОЕПМЮГЗЦКЗИДЬНУУАБЗОТЗЩЯЕЗЗЦПЙИЫБКГИЫБКЩИРЩИЮУЙЬЙТМРЖКЕНЙВ
ОГИКЖМЪУКДНБОЬВЛЕЛГЗДДХЗШДЙСЫЕДГББДНБЕИДДЖРБЩИЬРЮЮМКТКЖКЯТЫЖМБТБ
ДБЮУЙЬЙЖРБЧЗИИДАБДОЛВЭЬДЛРНДИЕЦИЬСЛЩУЬМЪВЯЖОКЯЗЖОКВЗЫТКЮДИООВОЕЮ
КВЯВСБЯНГЫКЩЗЯЗКЖКВЗМДДДПБЯИДОЬВДЖОЛЛДЩЛБАБДГЗЦКЗЧЛВЙЫОЪБКЖРБЦЧБ
ТХЮКИЛМЪЭЬОЖДНИКАПЮВМЖЩМГЕВЕЖЯЕЖЩЖЫОЛПКЙКЗЖКЗЫОЕКИМЮЙПОУЛРЙЬВДЯН
ЯМФЦНЙЛБЬГЕСЛВЗИОЫЩМПЕЖБЧГИИДДЙЕДАДЙУЛЦЧЮВДЕКДВФЗУЯТХАБДИЬДОУНЪЬ
ЗВИЙШБФТЗЧКЩОЙЬЗЕНЖЩКШХЗШДГОЭЯЙПЕЬВЭЗТКЯПЭИЫВЯЕВИВСЕДЮБЛЗИЕЩМЖРБ
ШБПЬЫАБИТЮЛЖЕЧЮАЛЗИГЪБПЬАБОУСЫЩАУНЮЦНЬЖЮХДЙЬЯЬАЕВИВЙЬВЗЯБЖОВШБПЬ
ЫЖМБТБДДИТЖЩФУИЬДОУНЪЬЗВИЙШБЫЛЛВЯЕНЭВЭДОМАБЙЬБЧМЙЬКВЮЬРСЩЙДОЪПЗК
БЮЪАЬНБЕЭЕЛХМДГПЙЬЗЬЖЖЬБГПЙЬЙВСАЗУЬН

2. Разложить на множители числа:

   (a) 106954484380694349588078811618 3

   (b) 750983717809581734914266910676030514063117654729445008602623

   (c) 62071632408897394440896210235399257427104238382845226580504365959155497818436101349263994 1

   (d) 1144210619037862898660768331115938360933205984298627435435197347327617915334593786021960720825915894118554239466074422863

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 52164290749852521862141338176221514095447090614739692986966026668151647079907$
   - $e = 5$

   Сообщение:

   - $M = 12299669250505395383617691155833237179010418527015146009483628554863675 4807$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 26693395234863053854917699697454293918 7$
   - $q = 23058444224867782240570758846248954723 3$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 52513662634264966329726213266275929086952344852307682285687859507417576407320$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 12479496172386794597225610021411799154 9$
   - $e = 17$

   Зашифрованное сообщение:

   - $c = 76225123441612189028825916952991241893$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 325507702327831252033656522728180072731$
   - $g = 26797142288889272869573915195523987244 8$
   - $y = 19213890666264537519371353528234590185 8$

   Секретный ключ:

   - $x = 62626611461275020864278704115421269355$

   Сообщение:

   - $M = 38986030397342571764450045706830139 74$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 24831678285728187068606647025627932739 3$

   В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 22243789093201021828102534851796691548 7$
- $g = 19146277602261998963418456957742425330 0$
- $y = 13685103551709070284084363287229157067 6$

Сообщение:

- $M = 21534415436611261580144047872539385841 6$

Подпись:

- $a = 10951040718152681936598524430004775090 6$
- $b = 21340885293209196838468400731479454398 2$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 691$
- $g = 390$
- $y = 365$

Сообщение:

- $M = 360$

Использовать следующий случайный параметр для создания подписи:

- $k = 19$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 12x - 2$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 71

1. (a) Расшифровать текст:

ФХЦМЙРУФТФЧЕПЙССЯРЖУТЦТПОЙЧЖМИЙПРЦАМТЦЪФЧОММЩЕЯПМХЖЛСЯССТЗМСЕМЦЯ
ЕЯПМОТПТИОМЕФТХМПХМЩТЕСМРЦАМСЙРТЗЖЯЗТЖТФМЦАСМХПТЖТЕХРТЦФЙПМСРЙСХ
МЛЧРПЙСМЙРЗТИЖТЙССТНКМЛСМЦОМЛРЙСМПМРЙСЫЦТТСМСЙРТЗПМРЙСЧЛСЦАРЦЧЬО
ЩСЧПМЛПМПХАХПЙЛРМЖИФЧЗЧХПЯЬПРМПЯНЛСОТРЯНЗТПТХУЙЦФСИФЙМЫБЦТЖЯТХЦТ
ПЕЙСЙПТЗПСЧПХМЖМКЧЖИФЧЗТРЧЗПЧРФАВМЖСТЖСЧЦОКЙХЖЛССЧВТЦЙЪЗПИЙПСРЙС
РТПЫСЙХРЙЖЙФМЦАХРТРЧХЙЕЙФИТХЦАЕПМХЦПСПМЪЙЙЗТХУЙЬМПХЕПЙВФЛФЙЛЦАЧЛ
ПЯМЩЖЙФЙЖТОЛИФЖХЦЖЧНЛИФЖХЦЖЧНУЙЦФЧЬЗТЖТФМПТЦЙЪРСЙУФМКМРРЙСОХЙФИЪ
ЧХПЖЕТЗЧИТКИПМХАЦЙЕУЙЦФЧЬИФЧЗРТНЗТЖТФМПРЦЧЬОООЦЙЕЗТХУТИАУФМЖЙПЛИ
ТФТЖПМЦЯХУЙЬМПМЩЖЯЖЙХЦММЛЛОПВЫЙСМСТУТИТЬЙИОИЖЙФМСЬЙПЙЙХСТЖЛУЙФЦТ
ВСИФВЬОЛОФМЫПТЦТУФМООСЙЦОТЦЖЙЫПМЛЛИЖЙФМЛЙРХОМНХМИМОХРЛИЙХАЖТЦЧКТ
СЧЫМРЦЙЕЕЧСМЦАИЛЖТФТЦЦХОЦАЗТХЧИФЙЖЯЩЫМСТЖСМОТЖХЦПТХРЦФМЖЦАСЕФМЭС
ЙЕЯПТПМООТЗТСМЕЧИАХУТХТЕЖЯЕФЦАХСЙЦФЧИМХАХОЛПРСЙЕЦВЬОСЙЦОТЖХОТНЩТ
ЛМСЫЦТЕРТКСТЕЯПТЖСЕФЯРТМЖЩТИМЦАМЖЯЩТИМЦАЖТФТЖХОМРМПЛЙНОРМРЦЧЬОСР
МСЧЦЧТЕФИТЖССРТМРУТЖПЙСМЙРЖУПЖТЦЫСМЙЖМИЫЦТУФМЬПТХАМРСЙФЛИЙПМЦАУТ
ЗМЕЙПАЖХЙНХЙРАМСТЕЯПХУТОТНСЙЙХЦЙЩУТФООСЩТИМПХХСМРММХРФАЙНМЖСТЖСТ
НХТРСТВЕЯПХЕПМИЖУМХЦТПЙЦРТЗЙЭЙЖЯИЙФКЦАТХИЧЗФМСЙЖИТПКЙСЕЯПУТИТХУЙ
ЦАОЖЙЫЙФЧМСХТХЖТЕТИМЦАХТТЕЭМПЖХЙБЦТРТМРФТИМЦЙПРМЧХУЙПЧХУТОТМЦАРЦ
ЧЬОЧТСМУФЙИПМХАЖУТПСЙФИТХЦМХЖМИСМСЧУЙЦФХОЛПРСЙТЦЙЪИТЖТПАСТЦЯУФТО
ЛМПМСЦЙЕУТФИОТРЕЯПХЙФИМЦСТСЙЫЙЗТУТРМСЦАУФТХЦФТЙСИЙВХАЫЦТЦЙУЙФАЦЯ
МХУФЖМПХМУЙФЙЕЙХМПХЛСВЫЦТЦЯХПЧКМПООСИПЙКМЦЫЙХЦСТРЧТШМЪЙФЧХУХМЕТЧ
ЦЙЬМПРЙСХЦФМООТПМЦЙЕЙТЕЛСЕЧИЧМЛЕЖПЙСМЙРЦТКМЛСАРСЙЖИЖТЙЕЧИЙЦУФМЦС
ЙЙХТХПЙЛРМЪПТЖПЙЗТФЧОЧМЗПИЙПС

(b) Расшифровать текст:

ЦСЛВАЧТВИЧГЖБКШМТТЙШХМЗЛФЦФНПЫУХЙЙЕЫЬЙВЦЦЖННШСЫСЛРЪТЖККРЦЬПБХЙАП
САОЗЗЭТТИЙАНХСПЫЧФНОЫЪААИЦЦХКЛХНСЗРЯЫКЗЗХЩЙПЯАЦУДПГЫЬНПХНЫКЙАНРС
РЛТБСЛЕКТИМБЩКДКОСТСВЙЧТХИЖСЧМВЦЦФТФЭЫМОРДЪАНКЕНЕАИЦЦХКЛХРЦМВДЦЗ
КХЮЩЦНАЧФЧЕЕЭКХЙЛКРПРМБЩЦДИЫКЯФЯЕРПСЛВЦФЗДЪЩУЗКОРХСИЯЭЦЫЯБКХДОЕЦ
ФНКОЭТСВЮЙЙЕППРСДЙБЛОНЙАЪСОЛЮХМКОПФЙППХГРЗПШУРЗОВЦЦЪЗЮЩТСВЮРХЙЛЮ
ДЛЗИХТФНЯХГЩКРЩЭХСНЛХЯИЙЖОМЙИДТТБЛЯНСЙИЫТПВЛХЦФМВФЦНРЩВЦИНЖЧРУНБ
ЯЦЙАИЦЦХКЛХНСЗВЖОХЗКШМТТЙШХМДЛХУИДИЫФСНЫЫКБСРЯРСТПЖЧФНОАЫПРИБАИЗ
ОЕЦПЗОХНПЫЕКМЙПАЮФЙМДГЫОТАБКТПЯОЭТГЕДЫИПЩВШМДТЮРОТБВШМДТЮРХОНБЩМ
КМГЦЦЗНЦУЛММБЩЦНИОСИБЛГЛТРМБМАОЛЯЦЗМПЭХЧКЕДДУПЙБХЛАЛГКЯФЛЧРХТБГД
ХЙЛГНЙГЛФЦЗПВЬЩЖЪХШУМЖЗЫЙМСЗЫЙЧПКШБЙОНБМТКГЮЩЦНПДФЙМЩЛНВРЕЮЦВАШЮ
ЦЦЙПШФСНФЕЦЩНППЛПЖЯОТТКЕИЦЛЗКХЩЦПВЕРПМОЖКТПЛЕМЙПГЗЦСПЩВЦИОЛЮЦВЗЯ
ХНПЛВАКЗННАРЪТПШЩСТЫАЦИНЯБУАМЛКРХСРСУЧЦЕАЦХБВМУЙДКДЪЙМВХРХДИХРСС
ЛХТМБШДЦОЙДЙТЬОЗИЦЛЗКГЦИНЙЫЮОЗЖЭПОЙДЮЩРТГЫТПДПЛНХСЕЧНХСЕШБЙРЯШОМ
ИЕФЦИПШЬЩЖДИПРЫБКШЩЛЛКБЖУНАГНЕДУВЦЦПВФЦЖКЛЦХЫСЛФЛТСЛХРЦЫФЬТТСЛГГ
НМЕЭЦЗГПЭХЙЙДЮЩРМВАЫКДКИЦЛЗКВЦЬДИИУТОЛЕЪАВБШОЙБЛЩЪЯИОВШТРЕЮЫХБВЮ
ДМЦДЧНХЫЯЛНЕКАБШТГЕШЦЦБВКУРМВЦЦПНОДКЙПТЖКЛВИАЫПММБУЦЗЕЖКМГВЮЯЙПК
ЖЖЕННБМЧЗБХЩЖДНЭЖЭЗВЦУЛЦПБЙФСМГЦЛАЗЭХЙОНБПЕМРЕДЖНБАЦРФРЧНСЫЗБФФЛ
ЗШЙЯКПЖУЧОБКЪТВНШЭЦЗПППППНГЫУЖДФБШЧХИБКПЫКЫТРННБПУНЗЪУХМВХНПЗЗХЕЦ
ТЙЫХЧСРИЦЛЗКХЦЬДИДТМОЦЫФХЛЛХШТЛМГНИКЛЩРПБЛЩЪТЛРААЙЛРКАОТФСФЧЕЕЭЩ
ПДДДЧТКПШССПРЩХТРППНЗНМБТЛКОПФСДДЯНЫСВЮДСНКФГПКВЕЩТПЛЭШТРПЖЩФДБА
НЗНТЖМТШЯЫАМПЛЭЦУКВККЫДНАЦНАЛГЦИДВЦЦУНЗЪГЖКОПЧФНОШМАЕЕХГЙАЛЮДЬЗВ
ЦУЛСЗЫЙЙВИЫУМХЛШЛТЗЙШУТБШ

2. Разложить на множители числа:

(a) 539333909838761550824413211159

(b) 908597720053258000145572808631739796461470115987700813627873

(c) 8157884498334636821335998129258758369238390345957317676777979918555087539253705247370861 37

(d) 1059964387494742592649093090998260524320320470709069430834072469009636040301959310374471216565744090475984124021513009381

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 396679254030703010908182247609941426859427673866143680322250166016066480368 59$
- $e = 17$

Сообщение:

- $M = 199317395159154068429848334112867370005224901538773080259479962709318576337 59$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 317296319201791903830581592298420048531$
- $q = 254708556259769206401241641346270757917$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 397833566992969406002136400917532076545526629033478286896956334041359613953 5$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 214309256147115886298763001318041705511$
- $e = 3$

Зашифрованное сообщение:

- $c = 213401209093221003650642980129243164172$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 1749451571270251985893241954920074196 91$
   - $g = 22969300783893880005696941057669105514$
   - $y = 11002631190748824104124664079310097 4529$

   Секретный ключ:
   - $x = 59306473289030433122527699253037114916$

   Сообщение:
   - $M = 10017983118742069506863611612796799 7599$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 12490630821302971954368264276024945 2211$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 31933700681443786563142745299721348 5889$
   - $g = 22600045456168594380049314551355776 4827$
   - $y = 14568259242199805323179027446369672 0617$

   Сообщение:
   - $M = 24101330189879258409486883826680061 4570$

   Подпись:
   - $a = 20852792915975186407268082828328869 3772$
   - $b = 22343738373971721347785974133745287 0602$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 631$
   - $g = 539$
   - $y = 588$

   Сообщение:
   - $M = 532$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 289$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 13$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 72

1. (a) Расшифровать текст:

ЮЬАЕЧХЪЧЬХЯЪЮЧСЫДЧОТЭТРХДТЮЯЙЮЩЫШЫСАЬЫЮШЫПХГРШПЮТЭУЪЯРПЭСХХОИШОИ
РПЭСХХЫЪФПЯЭУЧЬХЯЪЯЫРЫЪТЪСЫОЪЫЬАЮЯЙПЭЩХХЬЫЮШАУХЯХФЭСЪЫЮЧФЪЫЬАЮЧЦ
ТРЫЬЫЯАУХЯСЧЯЫТРЫЫЯТГЧЬУЪХЪЫЯТГЩЫЦЪСЭТЦЬТЯЭЫПХДРЭХЪТППЩЫШЫСЫЮЯХЮ
ПЫТЦЮШАУХШЬЭХРЭБТЩХЪХВТХПИЕТШПЫЯЮЯПЧАЬЭТЩЙТЭЩХЫЭЫЩПРЫСАЮЯТВЬЫЭУХ
ШЫЪПЮПЫТЦЮХЩОХЭЮЧЫЦСТЭТПЪХРСТХУТЪХШЮЪСТПХГТПСЫЯЙХПЮХШЙТПЪТЛСЫДТЭ
ХОТСЪЫРЫЯЩЫЕЪТРЫСПЫЭЪХЪЪЮОИШЫСТПЯЙДТШЫПТЧСТЯТЦПЮТЩЫХОЭЯЙХЮТЮЯЭИА
ЩТЭШХПЫЩШСТЪДТЮЯПТЩЯАЕЧОИШТЖТЩЪЫЛОЭЛВЯЧЧАУТОИШФЬХЮЪПЮТЩТЪЫПЮЧХЦЬ
ЫШЧЮТЭУЪЯЫЩЬЫЩХШЫЮЯХЩХЫЭРПЭСХХЧЪФООШХФЧЫРЫЪЕТРЫЭЫСЮЯПТЪЪХЧТЮШХОИ
ЬДТПЮЧЫРЫДЪХЩЯАЕЧЭЫСХШСЫДЙЯЫОЯЛЕЧЫОЗПХШОИЧАСЮШТСЫПШЫЫЮЩТЭЯХЪТПХП
ЕТРЫЮЮТЭУЪЯХСТШЫЯТЩОИХЧЫЪДХШЫЮЙЮДХЯШЮПЫЯЬАЮЧАСЫЧЫЪДЪХЪАЧПЯЫПЭТЩ
ПЫЮЬХЯИПШХЮЙЩИЪТЬЫЪЫЪТЕЪТЩАЮЬЯХШТЯЪТРЫПЫФЭЮЯЫЯСЪОИШЪЭАЧХЮЯЭТЩЪЪЫ

ЩАЮПТШЙХДАФЯЭТФПЫТЬЫПТСТЪХТЬЫУШЫПЪЪЫЩАЩЪТПССЙЧХЬЫСТРЫЪСФЫЭЫЩЪСПТ
ЪСГЯЫЩРЫСАПИАДХШЮЭАЮЮЧЫЦРЭЩЫЯТХЩЫРЫДТЪЙФСЭПЫЮАСХЯЙЫЮПЫЦЮЯПВОЫЭФЫ
РЫЧЫОТШПКЯЫПЭТЩОЯЛЕЧЪЪШСШЩТЪБЭЪГАФЩЫЮЙТОЫЬЭТЧЫЯЫЭЫРЫПИЬХЮШХХФЩЫЮ
ЧПИПЩТЮЯТЮРЫСЫПИЩФЬЮЫЩПХЪХЬЭЫПЪЮЧЫРЫЩЮШЬЭХТФСТРЫЮХШЙЪЫЪТЬЫЪЭПХШЮ
ЮПТШЙХДАЮШПОЫРАПЫЭДШЫЪЬЭЫЮТОЧУТЯЮСХЯАЩИЯЬЭХДТЮЪЪЧЫЭЩШТЪЧАСЧЧЪАУЪ
ЫЯЭЯХЯЙШХЕЪХТСТЪЙРХХЪЪХЩЯЙЩАЮЙТЧЧОАСЯЫХЮПЫХВШЛСТЦЪТЮЯШЫОЫЬЭТПЫЯТ
ДТЮЯПТЮПЫТЩОИШЬЭХЧЩВТЭЫЩЬЫЯЫЩПЬЭАЮЮХХЮЫШСЯЫЩЬЫЯЫЩЬЭХТВШПЭЫЮЮХЛ

(b) Расшифровать текст:

ХЦЕЖОМФДСМЛЫДКПЙЦБЭЖЮВИМАФЦЯСПЦЯЖЗРГВЗУЙКЬЪЖРГУЙИГФНАПГХЫДЩИХАЫС
ГЛЯВОМЕАЖППЩЩЖМПГАЫШЙГЮЗУГЦНГЙПСЯЗЭПЩЯБПЛМВАПЙГЫДЙЕИДОЖИЦЯЙМЖЭЦЧ
СМЛЩБПЛМВАПЙГЫДЛСЧЩМТРЧДЛТРХЮАСЩТНМЖПСЯЖЬРХЭАМЖСЬЗГЖФЦЯЛМЩЯЖЬГХГ
ШЖХТЩЫКВЧДЬЖЙЕТГЬКЬБФЛЛГЦВЙАХГШЛИХЪЗУМЧЯГЖМШДЬЕГФТСМНЧЯШПВПГТНМЕ
ЭДММЛЯЗУЪЩЯЗЛАОЬВЖЛХГДЩГТЯИПИХЙАЙЙМФЗРРГТЫИСНЩГОГШЭДУОФДШЖЧФЩЗГГ
ТНЮШИХГДСЩРАДГРХББТПХЫЖФЦМЮЮЖККЯЗРМЛЩШМВВЫДОЖЮЦЩПИЪЙИЭЛМЩЭГМТЩИШ
РХВАЗГЩТЖЬЛСЯБЙВПГЭОГУЯЬЖРФХЖФБХЪЪЖЛГАДФРЧДИПЙГЫДШРХВИММЛЦШУЪШЫА
ЕАМБТПРЙЯЖЙЙШНЮЛМУЮЫГМЯЦБНМТЯЪПЗХЕЮЧГЧЮЫГЩШЯАПБХБДТРШЬЮЧМУВВФБТМ
ВЙМЩЭЫОЛХЮЫЛОШЩШЬКФЯНСГОУСШЗБЯЬЙАВЭЮИАПЮЮУГУЦГТИОЬДОКФЦЕПТЧЮМФЕШ
ЫЮШРХТЫИФМБЫНМФЩЮРОПЖДЗСШУВЙНХШГЛМУЩИЭПЙИЫССОЮБПАЯЦВРОПЦЭЕГНЦБОЖ
МДШЙВМГТОИХЮЫЧХМЬДГГЮЦЗЛММЬЮЧМЩЫДГЙЛЦБПКФЯФШРХЮЫГЩЩЦЖРГТУСЮРХАДК
КМГЫЛМКХЕСМНЩШЖРМШЪЖПГЦПЖЛМВАПЙГЫДГОМЭЫОЖЛЯЩЕЙШИИПЫЩЯЧЬЙХЕЮЧГЧУС
РЖШЮГЬЗПШЩГОЛЩЮИНХЦЪЙЛХЫВЬРХГНТНХШГЛМУЩБЙПГЙШВОПЮЧЬЙХИЫОЪФЦЩМСЦБ
ЭДМЙЯЖЖБХТСММШГЫСЖОЮЮНРМЬЫОМФВЧПЙГЙДКАМВЫММШГЮЯМЦЩЗМКФЦЗЖКМЪЗУАХ
ЫДНГФХГУГКЯДВЧМВИГМПЫЖКИЪХЭГГТЭЫОПЪХТВПУЦБТМЩИЮТРХФДТГЧХМЛИЙЯОЖЙ
СЯВОГЩЯИТКВЪЮОАТЩЪЛМЩЯЖЬЗЮЩГЙЙУДГЕЖЧУЕЖОМХГЖЗСЯВЖЛЛЮИЙМЩЩВЖЛПУЗЙ
ЙПВСЖБХБДГЛВАДИАТЭЫОИФЩВПЯМХИЭЦЙТЖЙЛЙМЭГЙШЩЪУЖШЯВОМЕУВЖПЩЦЕПВЬЯЪ
ЛИХЭЫОВФГЗЛМУДЪПКЪЭСФАПХЫМЖФАБПЧЛЫЫШГТЯШЖИЛУЬЧРГВИСГФНАЙУПЮШМЖЛЯ
ШТВТЩГОЩУЩАППУЩЮГРЧЦЙДМТНГЬУЯЬЕЦМФЩШЬПЩБДЖЛВТСМЖЙЯКССФГШРГЧЦЪЙПЩ
ЯБЛМУЦГЕЛЩВИСЖСТДЕОВЪЮГЩШЯАПБХБДТРЪУАПЙЦЫЫЙАСЩИКХЩЯВЦЙЩЦЙГЖЛЮЗПЛ
СЮВРМЛЯОЖЙШЫЭМКФЦГЖПСЯБЭИХЬЗЛМЙМЛТЙХУЮТРТЯЕУЬСЯВОВХУИЭКВЯЗУЛХУЮМ
ЖШНЧЬЙХВВПРЧЦИЭЛЪИЫОЖМЮДПЛЦБДТЖТЮЗЙВЩЩАГППЬЮТГМФДСМЙЮЫПЯМКЗЭЯВГТ
ГПТЦЪИЛУЩЭЕГШНЕСЖИУЮММФЮЫШГКЯШНПУЯИСГЩНШТЖТЩЗЖБХБДГЛЦБЮО

2. Разложить на множители числа:

(a) 549092923336321010822234120057

(b) 144966321188735935536104146158776807545320831190315241808780 7

(c) 11912862260150053889903556170401307211922610018070801161503700739594431706139239292138261 13

(d) 10191004297565102498768199838819375057835193633208518580197477158324779068291023527739126691248021589340385574446043809 83

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 61606813520909713402758129787503326652517820614211270133172617732165907563373$
- $e = 17$

Сообщение:

- $M = 516719488505964069926501942940603520666182275510670346638059628878049868447 28$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 19259377173712343047298493840392518484 3$
- $q = 18078231086931849494123729008947394161 1$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 13503912382023326291200233343745739521083220429906900906969288922301257646779$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 178501941907255530494866454528417522711$
- $e = 17$

Зашифрованное сообщение:

- $c = 148962728499584712582750814970642008992$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 233413699716520600064142099851329270361$
- $g = 128153238043924007193773302426920518501$
- $y = 241925646693026039310694031751238187 66$

Секретный ключ:

- $x = 840793386285755264391881642232640368 38$

Сообщение:

- $M = 137913112791028573589065537291686564120$

Использовать следующий случайный параметр для создания подписи:

- $k = 133532448032035963126543690839609192517$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 218922355394503582562907896716702172411$
- $g = 139098767099603817140670981713060613705$
- $y = 148920072205520354530227242165810530721$

Сообщение:

- $M = 209084450957761745267536094223884455842$

Подпись:

- $a = 156202939837553080378450246426941716392$
- $b = 184128750692006106680152072851147563112$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 823$
- $g = 499$
- $y = 271$

Сообщение:

- $M = 280$

Использовать следующий случайный параметр для создания подписи:

- $k = 125$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 14x - 5$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 73

1. (a) Расшифровать текст:

ТХГНЗЛГРИЗФЭОКНРУФКДЭЛУМИКЩФРФЗГЗТРЖКФЗНКМТЗСМРПМТЗСМРЙМЙНКПЗКЕТ
ФЮРМТРОЗММДРТЗЧКСРНПРДТФЮСТЗТДНУФТРЕРСРЖДЛУАЖЖЗПЮЕККНКФЗГДЙЪЗКСТ
РЕРПАУДЗНЮКЩСРЕНЖЗНПОЗПУЕНХГРМРЛЕРТЗУФЮАКСРЪЗНЙОРКОЖРНЕРООПЗГЭНР
ИНЮГЗЖПРЕРУФТКМПРЧРФЗНДЭТДФЮУПДРНАКЖРМЙФЮЩФРХИПЗТЗГЗПРМЖЗПЮЕКГЭН

КЖРУФДНЗПЭЙХТКПХУДЗНЮКЩСРУСЗЪКНДЭДЗЙФКОЗПКЙСТРМНФРЕРФТМФКТРПДКНУ
УКЙДЗУФКЗОЩФРНРЪЖКЕРФРДЭУПЗУСРМРЛПРЛУРДЗУФКАКУГЗЙОРНДПЭОТУМПКЗОД
ЭЗЧНКЙУКОГКТУМПЗСТРУФУЮУОРКОХЩКФЗНЗОКПЗЖХОУПКОХИЗМРЕЖПКГХЖЮХДКЖЗ
ФЮУЕНДДРИФЭЛУФРТРПНЮОРУФРТРПХЪМУФРТРППЗЙПМРОЩФРПЗУОНКПФЗГЙЪЗНЩФР
ПЗЖРГТЭЛНКЖОЗПМРПЮЙДЗЙЙДЗЙНОЗПЖРГТРЕРОРНРЖШСТЭФРУФЮГРЖТРУФЮОРНРЖ
ЗШМКЧОЗНКПХЪММГШМУФТКППСЗУПЖРТРИПЭЗТЙОЭЪНЗПКОРКГЭНКПЗРЩЗПЮСТКФПЭ
СТРКЕТЭЪОРЛСРФРЕЖЪПКОШЗПОГЭНПЗОНРДИЗППЗОРЕПЗСТКЙПФЮУДЖХЪЗЩФРСРДЗ
ЖЗПКЗОРЗДУКОГКТУМРОФТМФКТЗГЭНРЕНХСРКЩХДУФДРДНУЗГДКПРДФЭОСЗТЗЖУДЗ
НЮКЩЗОДУЗЯФРОЗПОХЩКНРУФТКМХЕТАОРУКЖЗНПРГНХЩМЗРФДРТРФУЮРФОЗПКОРНЩ
НКЙТЗЖМФРНЮМРСРМТМКДПЗСТЗОЗППРЧРФЗНУПКОСРОКТКФЮУКПЗЙПНУЩЗЕРПЩФЮП
МРПЗШУМЙНЗОХПХПХУДЗНЮКЩСРНПРСРОКТКОУДКПРДФДКИХУОЩФРДКПРДФДЩЗТПСТ
РМЙКНФЗГПСТУПРРГКЖЗНРГЗЫАУЮДСЗТЗЖДЗУФКУЗГХОПЗЗКУНХЪФЮУФЗГПХПЗУЗТ
ЖКУЮСРОКТКОУЯЧГФАЪМСЗФТПЖТЗКЩРФДЗЩНРПУЕНХГРМКОДЙЖРЧРОУЗТИХУЮФРПУ
ОРЕРУЗГУОМТХЕРОДКПРДФММОПЗГЭНРРУФДНФЮФЗГРЖПРЕРДФТМФКТЗЩФРЖЗНФЮЕТ
ЗЧСРСХФНДЙЖХОНЙГТЗУФКМЖЮЩКЧЗСРДКЖФЮУУМ

(b) Расшифровать текст:
ГПШЪВЩМВШООЩПМФТЩЖУРОПНЫУРШНЦЯЭТГХОДЧУДОШЫЛПСПЧПМФВЪЖЪУЩЭНРЦПМФЖ
ЧЛПНЕШПЦПСЗУИЩТШЬЫТЦЦЙХТФБВЕМЦХПЫРЦЦЙХЙМФГШМДУПФСЫХОШТЧЛУЪПФУЕЪЖ
РЭЖЦИЯШПЬЛПЧФГФЖЗЖСЕНСЙАФПХЖЫЖХРФМТРСЙЫЖЛФСШГХУЩХЙПЭУШТЩФСТУДЧИЩ
ЖЩЛОФФМРЛРЖЕШПЫМЫЭЙХПЩВЕМПЪРЛЩЖЪЦООСНОШЫПЯООТМХЛЕМОЦХЖЫОЖОТПДЦКО
СРНСЖПРШОНЧЖПШОЭМФФЯХЯЙОНЭЯТХЙЬОЩРЕШШДУЖЯПМОДЭМЪВГЩПУУПБЭКБЩХСПС
ЕТЧЧЛУЪОМЦЖТШЙБМШЙШЧТПСМОМЫОЦХПЬПФЦТЫФМОМБУЦИТФГЦСЖЧРНШЭБУЦРПЦФЫ
ЙПООЦШЖЦЙМЛМШЛЦУШТМЦЧЭЛЖЩЧУЕЕЩШГШЩКЗСТОЯЩУЖННУОПГПЗЖЫЙУФОШОРРУШЛ
ШФНПННУОПРЦУМНСЫЗЬЯЖЛФПЛЙХРПМРЦРСУОНПНПСНУЙФУЦУЖШВШШЙХОХОЦМОРТОТ
ПЪХЖЫЖХФЛЪИЛФГШСЦЗСЬЙУЧЛЫУРЫПЬГЦЦЧЦЙТФНПОМУУСННШЙХШЪФГЫЖЦУЙХЯМОВ
ПТЧЩУЧЬНОДШСДРЙПРДУЙАЬРКСЭЗНЧЛТТЦИЖЬПКСНЧЖЦЧУМЙЪВТЬЙЭФУМПШЧУМПТР
ЕПМЦЧМЭЗЙЛРЪПЪОГЧПНООТЛЯЛНЭЕЦЗСШНЫУЖОПКФЕГЖНХСТТЫШТЬГРЛЩМВШООЛЬУ
ФНЧЖХЛТЧПЩУПЫЛЦЦПЩСЦЧУТМЩЧЛШННУЕЧУЦТЙЫЖЛФТПННПТЬГЦТРЪЙАЛЕОПФФКШТ
ФФУЪЖУЧГШЯАХДЭРЦХСШВЦИМПЖТФОПЧРСЖНТЧШЭЩСРРИМТКЛМЖЙЯЩССВЫКЙЬЭФЛОМ
ТНКЭЦПФЭТЭОМЦФНПСКЖЧЭКУИЧШНУОШЖКЦЖЦТЪФМЭЗННТФЙШКНТПООЕЦПНЙПЩСЦШЙ
МОРРГЫЛЦЦЖТПХИЙХТХЧНШДЫШИЫУЪВТФИУФОЦОНУЕШВХФРШТЧЛЩТУДТЬЫОУОНЭОМО
СЕПЩШМТТДИПООРЫЛЦИЦСЦТПЙУЗТМРЮРНЙКГУЭНРУФЬФРНИЫЛРЦЕМЕШЩДЩПКОМЫЙК
УЙНОЪВЙБЙЯЛМШГНРРЬЭРУГХЙМФГШОЧФУЪЖЙФГХОЩРЛШННУЕЧУЫТЬЩПКООШГУОТЖТ
МФТОПЖЧПХЕЪБОЫПТЦФРЙУОЙЦЬЦШРЪГРСЙЫЭКРСПРЦЧУЖГЩСЖОИРИОШНРЙОЬЭРЭЖЦ
ЛЦШПЪЬСИЖХОЩИУШСОЛТЬГНЮДЫФМОГТУНСЭЧПСИЗЧПЩШЙИНГИПВМРИЛШННУЕЧУЩРП
УЕЦТЙМОРЙОЬЭРЭПЬГЦЦЙХЕКЛСТРШФГШИЛСТТГЪФСРЖЩШГПОХФРЪЙКЛМЧТКЧУЪЖЪО
ММТРСЙЫЖЛФСШГХЫНШЙЙШЯВЛРУШЬПЕШПЩПЭФЗПЛТЭУШГХЮЖУЛШЛРШТЪОИМПМОУЖТФ
ЛСЬПЫЗЙУТЪИПТГ

2. Разложить на множители числа:

(a) 71170620064700042569249691605 3

(b) 7858716173681696011484673574493426916490314350755565102750 63

(c) 1180248908532114307221947862388916401831932930490996311262550763820090945272345332519400379

(d) 1412269256351084988212034556809266404435321970781873985159253237973849825060994254732404023442427802836251425177510524377

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 92158792726170128817905518763690946380816711119543209621402467832424175993491$
   - $e = 3$

   Сообщение:
   - $M = 53989966766280537870195962798324089604844634023242876583630269309744128414496$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 28855400181915599047011003363335124853 1$

- $q = 263792728033744019516979785887620278911$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 770846665318690420398990897261701437784700421295633670673055243599463756806 0$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 190958831072663561775904481962699966801$
- $e = 3$

Зашифрованное сообщение:

- $c = 916328221167233681548608000937422889 89$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 32450869517065323682399984924648758324 7$
- $g = 14739691373440878460666768167461685817 5$
- $y = 11830076649155926234179418486759451692 1$

Секретный ключ:

- $x = 67289685391328476886586878208524277101$

Сообщение:

- $M = 26323160945643292775556211805423162673 3$

Использовать следующий случайный параметр для создания подписи:

- $k = 99633507723875088837754813474220908661$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 33146951480870010943716755433597279085 9$
- $g = 10677546495617160602061923743207046052 9$
- $y = 11266036431791765067141797257279152431 8$

Сообщение:

- $M = 21890335949216235956425250362283716821 3$

Подпись:

- $a = 10933685031650988429179209511340117228 4$
- $b = 21742767740037175823702075440424560379 9$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 563$
- $g = 329$
- $y = 337$

Сообщение:

- $M = 45$

Использовать следующий случайный параметр для создания подписи:

- $k = 523$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 5x - 3$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 74

1. (a) Расшифровать текст:

ТБУЮБЯЮФМЧТИГФЮСАЮФХВХЫМТХЪЭХЧСГФГТИШЕЬШЫЮБВХЩЮЭЯЮИХЫТБТЮОБВЮАЮЭ
ГЮВЯАТШЫБФЫХХЭХЮСАЙТЭШЬЭШЭФЮБФГБТХЫМШЗШБЪЮАЮЯЮЧСЛЫЮТЗХАИЭХЩТМОУХ
ЮБТЮХЬТЮЦВЮЬШЮЧЩЗМХЬВГЫГЯХЯАШХЕТТЮАХЭСГАУЯАЬЮТШЫБЪУХЭХАЫГГТШФХЫЬ
ГЦЗШЭГАЮБВГТЛБЮЪЮУЮЭЮГЦХБУЮАСЫХЭЭЮУЮБВАЮБВШОФЫШЭЭЛХТЮЫЮБЛХУЮСЛЫШ
БЮТБХЬСХЫЛБВАЛЩЯЮЫШЭЫЛЩЬГЭФШАЭЯЮЬШЭЫТЮШЭТАХЬХЭЭЭЛШЮЭЭЮТЭЛТХУЮАХЗ
ШБШЫМЭЮЮВЧЛТЫБЭХЬХЖЪШЩТЛУЮТЮАЯЮФЫХЬГЯШБМЬЮЮВСВОИЪШЯАШШЬХЭШХУЮЮЭТ
ЧУЫЭГЫЭЬХЭСЛБВАЮЯЮЦХЬЮЩБЪЧЫЮЭВТЭЮЫШЪЦХВБЭФАХЩЯХВАЮТШЗСЛЫХИХВТЮШЕ
ЫХВВХЯХАМТЮВГИЪЬЮЩГЭХУЮЬЮЫЮВХЖЕДАХЬДАХЬЮЭАБЯХЗВЫЯШБМЬЮШБВЫЗШВВМХ
УЮТЯЮЫУЮЫЮБФХЫБТЮШЧЬХЗЭШЬШЫЮБВШТЛЩУЮБГФАМЭФАХЩЪАЫЮТШЗЭФХОБМЗВЮТИ
ХЯАХТЮБЕЮФШВХЫМБВТЮНВЮЗВЮЧБХАХЬЮЭШЩДГЩЪЪХЬГЭХБЮДХБВЭЮЬЮЭХЗЭЮФШБЖ
ШЯЫШЭЯХАТЮФХЫЮЭЮВЪЫШЯШИГВЪБВАЮЬГЬЬАФТИХЯАХТЮБЕЮФШВХЫМБВТЮЭХЧСЛЫЮ
УЬШЪЮУФЯЮЪЮЩЭЛЬДХЫМФЬАИЫЮЬЬШЭЯЮЕЮФХВЪЦХШЪАЮЫШЭЪГНЕХСАГФХАВЬЮЭХИХ
ЯЮЬЭШВБВАЛЭИШЯАЮЬЧВХЯХАМЮФХЫХЪТЬЬЮХУЮЯЮТХБГУЬФХАЦВМТХЦЮТЛЕАГЪТШЖ
ЕЗВЮВЪЮХХИХТЛАГЪТШЖНВЮФЮЫЦЭЮСЛВМАГББЪЯЮУЮТЮАЪЗВЮВЪЮХФХАИВМТХИХТЛ
ЕАГЪТШЖЕЯЮТВЮАШЫЮЭЮСАЙБМЪЮЬЭХНВЮЧЭЗШВЮВТХЗЫХЬГБТШФЮЬЪЬЬЮЦЭЮСЮЫХХ
ЭХТШЭЭЛЬЮСЕЮФШВМБЫБЪЮТЮЭХБЫШИЪЮЬБВАЮУЮФТВМЯЮСЮЫМИХТЮЫШФХАЦВМТХЦХ
ТЛЕАГЪТШЖЕУЬЯЮЭШЬОШЭХФТВМХЬГТЮЫШЭХВТШФЭЮХИХТЛАГЪТШЖЛЧЭЗШВЭХВЮЯАШ
БХЬХУЮЯБЯЮАВУФХЦЮЭТЮВЮЯШБВМТБХЬХЭЮТБЪШЩЕЮАЮИЮЕЮАЮИЮТБХСГФХВБФХЫ
ЭЮЯЮЧТЮЫШИМСХЧЗШЭЮТЮСЭВМБХСШБВАЛЬВЮТАШЙХЬШФАГУЮЬЭЪЮЭХЖФЮУФЫБШЯАЮ
ЗШЯАЮЗЭГСВОИЪБЪЧЫЮЭЯАЮЗШВТЯШБМЬЮШЮВЫЮЦШТТБВЮАЮЭГЬЮЩЯБЯЮАВТБХСГФХ
ВБФХЫЭЮВЛСГФХИМЮДШЖХАЮЬЯХАХТХФХЭТЯЮЫЪШЗВЮСВХСХТАХЬХЭШЭХВХАВМВЮЧТ
ВАЦХЯЮХЧЦЩТСХЫЮУЮ

(b) Расшифровать текст:

ЭЦПАЯЬУХВЦЙИШНИГРШЙЦИНСЯЦМЧТВЯЬУХВШИНЦПЦЛНЧВФЙЙШЯЬИЦМВЬЧНБКЦМУЦК
ЦЭЦЖФГЙФШВХГТШЗЭЙОЫПЬГММВВНКЧНЯЯНЬВЬЗЬПНЦВТПАЯУИМДХГЗЩВБАЙЩЛГАЦЧ
ЛЪЗУПЖЫЙСЧПЦЙЦЬКЯЭНХОААХПБЮГСТОЫВРМДФЖТЭЯЮИКНЛФЛУСКЯЭНОКЯНКЛВЮАЙ
ШЯЯЖБЧЛИНУЛИФЙЙЪПЦЬХЧВЮГЫПИМДСПОЗЬАХКЫЛГННЯЬЧЕЕЭНБЦЛПРУБВЙЧШЦЛБГ
ЧЖОУАРЖЕИЬАХМЯЛЛПКЫЕИЪЛЭЙСЩЛЭГРЭЖВОЙЪЩВЕМХЛЮТШЬЩЮАМЪШХЭЬЬЛОНУТДУ
ЙРТХНЮУМЛБГЧЖМБГЬТКИНУЬШТЦРЪКЦИЖШАУГЙТПТАЛХДВЖУЧЕГЧЧПЮВЭУПЫФЛШОЩ
ПЙЧВМФГРПЗВАНМКМТЦЬНЯМЧЖМБЙПХПАЙСПХЬЯЬЬЛЧМЙПИЬЗЧЭХЫАЧШПУЙКУФГЙЧЕ
ОХАРХЛГЭКБИЫНУЩНЯМНХПЦЬФТОГЧТЦВЮЯУЧЛВЦХСЯЦНАЩНЩМЧМИЦИПШЙЮАЗВМЩЙТ
ЕМЩМРЧПЦЬЙШКЯМАШПУАЬХОУАРЖЕИМУЫИЦВСТАЯМФШБЩСХИКЦЬКЫКМДЧФЕШЭУХЩЫК
ХШФЩНЧЖФГЙФТХЦНПШЙЮАЖЪЕЮОЗТБЩУБФЗХЙТШОЩЖТЬВТНШЬЛЮЭАЧРЬГМФНЭИФТОН
ЗУТМБЙЬПИВЖКОРПФКПОГЦЙЧЛГАЖПОГЛАУМЦМЬЬЛГЦТПЯШГХЧЙЯГЦЬНЯЮНПМБГПСК
ЩЗТПКЦЯУЧВВЙЦЕКЦЗУПЙААЧЪВЮЯХПВУГЬПЕИНУЩЛВНУЪЛЮИНПМБГТЭГХАТЕРУАЙШ
ЙЬНБЦВЮЙКНЛАЛУФДЖНПХЕЩМФШИЮАЭЖПММЗШЫХЙРРКЯМЧЖЕФЙЦЩЛХМПЭЫУЙРИПЦЬЦ
ЬНЯЮУЩОАЙЭХЫВЭНЧВЪКЦЬЕШОЧУЗДКХМБМГФШПУЙХЫПУЙПЦЛЬЙЙШЙДТКХЛУАПЭОАЙ
РЭФЦИНПЙВАИШМБГПСШУЩЧПЮЦИКЦВХЖКЧКЯЙЧЩЕВНБФЛЭИКФЗЯЭУЬВААХЖВФЙМОЛБ
ЙЗЖВЯЕУЬЛБЙСЩЕЙОЧЦКЦТЧШМЯКХМЕЬЙЦЖБУЕПШВЩЗКЧКЯЗКЫПЯЙТЪКЦИНЯЛБЙЭШИ
ЩАИШДЬАЬТИЩЙЬПЯЩЯТШЮМЖУБПЯМЗПИНГЬЩВБАЙШЙЮЙГЛШЬКХМЕИНУЧМБМТШЛВЕУЪ
ЮЩЖКНЛДКХПЗЯЗНЩЛХЙМЪВЮГКЦМБЙЦТИДИКНЛАЛУГВЮГТШОГЛНФЮМЖТПРГАЭПКУЙЧ
ОЛИАИШБЯБНХМЯЭЧШНЬЙТМЛГЕПТТЭГРШОГАООЛВЖШРЕЬМУЬОУЙНЯАЯМФШБЩМЧЪШЪК
КЫЕВЭНЧЛАМЙРЕАЛНБЕЮНЗШВЪЛТЕКЦНЖЬЫЙЕФППБИЙЪВЩТТПМБЙПХПМДСЭОНАЗЫВЭ
ОЗТКЯЭЧШКЮОЬТИГАЖЬШЫНБЫГЦЖКСКМЗНМВБНКХЙЩЯФЪЕГЙФЕЯГЧПФЮДЯЧШПМЕТТВ
ЭЯЧШМЮГКЦРТАХПГЦУБЫЛГВРШАЯТКХЛУАПЧРЧИУЛШЬЙТЧЕЭНБЦРВЧКОПБН

2. Разложить на множители числа:

(a) 610389686954939646813979367719

(b) 14739699407527261927948254728113751063805555428015022672163 63

(c) 9805141698584236549439865668752147945774533083486069064462579473888908947855098169764737 49

(d) 1108085968213320657267084054158685014143516780207322811199944651010606372966275633612948642697500931069513180596169488641

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 6983196672092030910683678187274563897063947519636583253039799576850000390974 9$
   - $e = 5$

   Сообщение:
   - $M = 664845841896443999052578575808994194649583527689283034499394490882942132048 93$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 249198546441719648845815274709226976009$
   - $q = 319179062636277254322466316033487657149$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 449170421657215558334231926990342850766154644963330380956871601352371715828 00$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 155598629460401939087532257136994347997$
   - $e = 17$

   Зашифрованное сообщение:
   - $c = 445245258744607703229563861579443553 23$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 331396074750212302115031768058904971537$
   - $g = 307141883537454217336164464607724925016$
   - $y = 131385496096627978005326607949953610160$

   Секретный ключ:
   - $x = 214384152313212396495699491959702833806$

   Сообщение:
   - $M = 330716387095088337035980016731695130687$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 100788720340278048916221278408825312939$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 271182130624647286219536345615887966933$
   - $g = 974370418185271350276462237736468093 39$
   - $y = 163546021294637827834982279394083121374$

   Сообщение:
   - $M = 213901458486241664841899043325340127027$

   Подпись:
   - $a = 248290814337915055992707987684807496844$
   - $b = 175338773734827406666482515526997437429$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 661$
   - $g = 160$
   - $y = 319$

   Сообщение:

- $M = 505$

Использовать следующий случайный параметр для создания подписи:

- $k = 589$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 13x - 15$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 75

1. (a) Расшифровать текст:

ЯЫЕШЗТАЭЬДЬЪЕЯГКЖЗЩВВОЙЕИЕЪВИЕЩВЕИУИЬЪЕШЬИЖЬОДЕИЙЯХЩИЯВЯИЬЪЕЗЕЩД
ЯДЫЬВИВКЭШТИГЕЙЗЬВБЬДИЩЕЯМЕЮАИБЯЬЯКЖЗЩВВБЗЬЖЕИЙЯХЙБЙЕОДЕББЯИЩЕЯГ
ЫЕГБЕГГЗУЯЩДЕЩДИБЕЗЕЖЬЗЬИЙВИЕГДЕХЫЯОЯЙУИГТЖЕЮДБЕГЯВЯИУЩДЬАДПЬВШВ
ЪЕЗЮКГДКХЯОКЩИЙЩЯЙЬВУДКХЫЬЩКПБКДЬЮГЬЙДТГЕШЗЮЕГЖЗЯЩЮВИБЫЕШЗЕГКИЬГ
ЬАИЙЩКЫЭЬБЯЩДКЯЪДЙУЯОКБЗЯЩЕГКЪЗДЯЮЕДДЕГКЖЕЗКОЯБКЕБЕЙЕЗЕГПЩШЗЯДЩТ
ЫКГВШКЫЙЕШТЕДШТВЩДЬЖЕЮЩЕВЯЙЬВУДЕАИЩЮЯИЩИЯВЯИЕАЬЪЕЗЕЩДЕАОЙЕДЬЯГЬВ
ЕЯЙЬДЯЖЗЩЫЕЖЕЫЕШЯДЕПЩШЗЯДЕЙЕГДЬШЬИЖЕБЕЯВИШТВЖЗЕЯЮЩЬЫЬДЩЕЛЯНЬЗТИВ
КЭШГЬДДЬЕЙЪЕРВЩШЕЪЕИЖИЬГЕАБЗЬЖЕИЙЯДЬШТВЕДЯИГЕЙЗЕЩДЯКОЬДЯАДЯБЗКВЕ
ЩБЕГЬДЫДЙЖЕИЕШИЙЩЬДДЕАЕМЕЙЬКОЯВЯДЕЪЫИЩЕЯМИЕВЫЙДЕЬРЬДЬГЕЪЫЕШЯЙУИО
ЙЕШТЩИЬЕДЯЮДВЯБЕЙЕЗИЙЕЗЕДЖЗЩБЕЙЕЗВЬЩМЕЙГДЕЪЯЬЯЮДЯМЫШТЩЙЕГДЬЕПЯШЯ
ЙУИЖЬЗЬЫБЭЫТГЕШЕЗЕЙЕГБВВЯДИЬШЮДГЬДЯЬБЗЬИЙКПЩШЗЯДШТВЕДЬИБЕВУБЕЛЗД
НКЮИБЯМБДЯЪИЙВОЯЙЙУЯЩЕГДЬЖЗЕШКЫЯВИУЕМЕЙБВЯЙЬЗЙКЗЬЖЕКЙЗГОЯЙВКЖЗЭД
ВИЩЖЬЗЬЩЕЫМЯДЕЪЫЯЩИЕОЯДЬДЯЯИЙЯМЕЩЕШЬЫВЖЕОЙЯЩИЬЪЫКБЕГЬДЫДЙЪЫЬЕШТБ
ДЕЩЬДДЕЖЗЕЩЕЫЯВЕИЙЙЕБЫДЯБКЫЩЬОЬЗБЕГЯДЕЪЫЩВВИЕЙЬНЪЬЗИЯГИЭЬДЕХБКВЯ
ДЕАЖГЛЯВЕЩДЕАЖЬЗЩЕХЩЬИЙЕЩРЯНЬХЩЕЩИЬГЕБЕВЕЫБЬИЯПЩШЗЯДТГЗЮКГЬЬЙИЩЯ
ЫЬВИБЭЫТАЫЬДУДЕОИЕЙОИКШЬИЬЫЬЪЕИЙДЕЩЯВИУЫВГЬДГЬДЬЬЖЗЯЙДЕХЩИЬЪЫПДЯ
ЬПКЙБЯЬЪЕДИОЬЙИЬГУЯБЕГЬДЫДЙГДЬЕОЬДУДЬДЗЩЯВЯИУЕИЕШЬДДЕБЕВБЯЬЮГЬОД
ЯЕГЗУЬЯЩДЕЩДЬЫЗКЪЕЪЕЕШРЬИЙЩЩБЗЬЖЕИЙЯДЬШТВЕДЕЫЗКЪЕЪЕЯДЬЭЬВВДЬИГЕЙ
ЗДЖЗЬЫИБЮДЯШПБЯЗНТДЬЩЕЮГКРВЯИУИЖЕБЕАИЙЩЯЬНЗИЙЩЕЩВЕЩЕБЗКЪДПЬАБЗЬЖ
ЕИЙЯДЕГЯЗШТВЖЗЬЗЩДДЬЮЖДТГГЬЭЫККИЕШЯЬГКЭЬИБЮТЩВОЙЕЮДЯГВИВЯЙЬЗЙКЗЕ
ХЕЖТЙТГЕЯЫВЙЕЪЫПДЬЪЕЩЗЬГЬДЯШТВЯЯЮЗЫДТЯВЬБИДЫЗЖЬЙЗЕЩЯОИКГЗЕБЕЩДЬИ
БЕВУБЕВЬЙЖЕИВЬЕОЬДУЯМЖЕМЩВВЕЫДЭЫТКЫВЕИУГДЬДЖЯИЙУЖЬИЬДБКБЕЙЕЗЕАШТ
ВЫЕЩЕВЬДЯЮЩЬИЙДЕОЙЕИЕОЯДЯЙЬВЯЯДЕЪЫЖЕЫЩЯЫЕГЙЗЬШЕЩ

   (b) Расшифровать текст:

МЙЪЕКГТЫЙЬЯЯЪЭЯНВЧЧБЙПЪЙТДБЪИКМПФДЬЮЛЦКЩЙВХЙКЕВФЭЕЖАЪКДГЙЬАЪЙЯЬБ
ЩЖЗЪЕЬИБЩЛДАЙСЭВАКЩЗЖЙОРБВОНРЖЯЕМЪЭБЛРЧЧВИДЩРЯЖКСЬЕЗВЭЛЕШПЩЗЩЙОЮ
ХЖЛЕЩЛШЦИЦАБЗЕЭЫДЦЙЩЮКЯЛОЗВЧОЮЫЯАЙЪЖЯЮНЪЕБЙНЬИЙЖЕФБЩИЕПЖЙЧЕГБИКЛ
ЧЖЯНВЧХБЙЙСЖЫИПЭГЕЮЛЬКЖЙНТЮДГОЧФПЖООЗЯЗЕЯСГГЗЦЗДГАЪЫЕЛЕЧБЩЙПЯЯЕН
ВНЮШОБСЛЪЛКФАЕИКЦЙТМЗЪЕЬИБЩЛЫОЙЧЫЙЙПТЮЫАКИЭЕКНЪКЯНЩЭЫЕААЪЙЬМПЩЛД
ЙРЬЭДГЗНЮЭЖЕУИЕЯЗЬМВЭВЬЗЙИЛЫЙЯКЛШЗРГООЗЯРВРБДЙЙЗСВАКЩББЙЯЩЗЩЙВЪЪ
ИНЛЮЮВЧОЮЫЕООФДЯЖЛНЮИКЛЦЗАМПОЗБЙЙСЖЫИПЭОЩТВЩЪТЖЮДГЯЛВВКЩЙДШМЙГПС
ДУИШШБВГОЮЕЯКЛЭЮГООЧМОЩЗЪЕЬИБЩЛЫОЙЧЗЖНЩЭЗШЛПИКЩЙЕБЗЛГУСЙЕЭЕРДЙЙА
ЪОЕНВЧЗЖНЩЯЭВГПИЫИГИФККААЪЙЕЭКЯИЕЯЮЧЬЕЭЕРЖТЗМЬЮЫЖЛПЗГИЛЦГЯЭКЦМЮЗ
ЕГЪТЖФСДЕЭВЦКГЦЖЫЙГЙБЯСДЦЖФИЗЭБФЫТДПЪБДАКДЮВЯНЯЬЕЮЛЭИЕМЛНГЗЙЙСГБ
АБФЖЕБЗМЭАЕШМЖЙПЬЮШЖВЩЖЕЮЛЭДТУЩЮФЩМЕЧБИААЪЙЕЭКЭГЮЖЛЩЮАКЛЦСВГЯЪЛ
ЬСАСЙИГЙЫЗВОФФДЪЙЯЪЙЙГДПЗЗЙБЫЗВИЛОЙЙЧЕОЖБОДШБОКВЬЮЗЭИЦЗГАКРЖЙУПЗ
АДНЩБЗОАХИКЕЬНЮХИЙЯСТДГВРЪЬВЙСЖЖЙПЪДБЙЯЮХЕЬВШЮВЧКСИКЮФСЫЬЯИФОДАМ
ЬЗЩАБССУГЯЩГКВЙФРЩЦПЬТЯЖАЧАДОЙЮМПЕОЦАВЙКЦЗВГПЗМЭАЯЭЮЮИВДХЙЕМЪЯВО
ЖЪКЙЭЖЭЕТКЛЮЗВЕРСЕЯКНФЛЬЬВЮЗЙЙЮЮХБЙЙЪВЕНЯСРВЙКЩЮЙАЮСЪТРЕЮЙЯНЩЫЗИ
ЦИХГЮЙСФПЬЛЙФЕТМЛНЙВГОИЗЖНЩФЫДЕРУЕЯТЯЫЙЯМРЮКЙЭЕФЯЬИШЫЙЕТВЧЖГЭЛУА
ЩИЕСИКЮФСЫЖГОЩЖЕАЗЦБГИЕНМЫЧМЪДКЮНШЗЙИШШГЮЕЛШЙЮЬЛХЖЯЕЛНУЩЖИЪКЩЙВШ
ЖГАНСЖЯГКСЕЬЯИСЖДЙЕРЛЯИКДМБЛВЫЗИНЩЫЙЯЮИДДБВЗЪЫЯМЛЧЭЙЭООЗХУЖЦМБЙЙ
ЩЭЯЛЛОМЩАЦСЫВИВЭМЖЛЛЮБЩЖПИККЮНЪЯБВКФЧЩКНЪЛЯЭКЪЕИЖРГЮЩЙДУЫДГВЩИЯМ

КЪЪТЖЛОЬЗОЮЗОДЙОФДУИШБЫТЛГСЖЯРЕРЗВБКЪЪТЖЛЫЙЕГДОЮИНЕЪИИИЛСЫЖАФЮДЬ
ИЕСЖКЗШЫЙЕМПЗОВЩБСВБЕЛОЕЕУВЩЖЯЕЯЪКБЖЕЦЖКЖЗЪЕЬИБЩЛПТПЪКГАВЮЮРАКШИ
ЗАБЧЬЙЧЯЗЭЙГЗЩЮГОКОКЙЛВГМЯКЛЧЗЭГПИГДЙАШЮЪЙДЩЕЬИТЪЖИЙЮГБАМШЩЭЗВЯС
ЖЬВКСЛЕИФЮЗГЦРТЮИЙНЪГ

2. Разложить на множители числа:

   (a) 105681716316325946920137780 5689

   (b) 999196401705329481019339369507421874073577743985661320045227

   (c) 1793109921058452922561001328547788385518322113120281876341746385056822669413553545735000441

   (d) 161104760408497756876030547571342248659274997720816161789964896922485860175419353202672306350867322115558437141692360688 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 708671487416995138436867362068649571451784071460964507213320878825421604781 79$
   - $e = 257$

   Сообщение:

   - $M = 25511286848276969867737056066952297740738013728697767092480800039166101545584$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 269785947670973986532243453787834542573$
   - $q = 294237944349319607429096415354967319657$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 74557388599847205917739974512130314697052144389072140711972597751603311679557$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 173996869314682046389568893589280886391$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 151406948336598361654027277443133055262$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 32127916881218267965762103320422 6830041$
   - $g = 29145435825574862320961518459156417 2116$
   - $y = 14714490828992343592294175396229196 1019$

   Секретный ключ:

   - $x = 80439660298502636038298736083024872357$

   Сообщение:

   - $M = 78012544528405116262023897338309481098$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 30147278574533106722255940818831560 1131$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 20090947050654694659947986723109440 4833$
   - $g = 11185439545136807998947015059524100 5493$
   - $y = 92552978557442215734455333843318590624$

   Сообщение:

- $M = 14900330761643878542120993410128913841 5$

Подпись:

- $a = 13821595319744024907266913856149207989 5$
- $b = 28330516288157541117955513297242744339$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 857$
- $g = 765$
- $y = 238$

Сообщение:

- $M = 293$

Использовать следующий случайный параметр для создания подписи:

- $k = 333$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 15x - 15$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 76

1. (a) Расшифровать текст:

АЫИУЯЗЭИЖЪЖЮАЬЕААИАМДУРЪЩИАЕЗЖЙКЛПГЙЗЖЬДЖАДЖВЖРВЖДЖЙКЪАГЗЭИЖЪЯГР
ЗЫЛАВЕЭДЛЪУРЭГЯПЭДЖКВГЬУЪКФЙВЯГДЕЭРЪЩИАЕЯЕДАЕЭЙДЖКИКЙЖБЬЭДВИЭВЭК
ДЕАВКЖЕДЕЭЗЖДЭРЭКДУЖКЗИЪАГАЙФДЖГПЙЗЛЙКЙФЗЖВИЛКЖБКИЖЗАЕВАДУЖЙКЕЖЪ
АГАЙФЛЙДЖБИЭВААЖЩЕЮАГАРЗЫАРЪЩИАЕЩУГАЙВЛЙЕЭЭДЭЕЕЖЙАГФЕЭЭАЙДЭГЭЭАЩ
ЖЗИЭЩУЪРАБЕЭВЖЫЬЙЖГЬКЖДЬГДЕЭЕЭЙВЖГФВЖЛИЖВЖЪЪМЭНКЖЪЕААВЖКЖИУДААЪЖ
ЙЗЖГФЯЖЪГЙРЪЩИАЕЕЭЖЮАЬГЕБКАЪЖДЕЭЙКЖГФЖЗЙЕЖЫЖЗИЖКАЪЕАВЬЖГЫЖДУЕЭДЖ
ЫГАЙЬЭГКФЬИЛЫЬИЛЫЛЕАВВЖЫЖЪИЭЬЕВЖЕЭОЗИАДЭКПКЖРЪЩИАЕЖЙГЩЭЪЭКЙКГЙЮА
ЪЖЙКАЦЕЕЭЫЖЕЙКЛЗКФАЯЫЕГЭЫЖЗЖПКАЬЙДЛЦИЭВЛЪЬИЛЫЛЙГУРГЙЪЖЭАДЫИЖДВЖЗ
ИЖАЯЕЭЙЭЕЕЖЭЖЫГЕЛГЙАЛЪАЬЭГЙЪЭГФАПЙЩЭЫЦСЭЫЖВЖДЕЭЗЖЕЫЖИЕЖБКИЖЗАЕВЭ
ЪХКЖЙДЖЭЪИЭДДЭЕЙАГФЕЖВЖГФЕЛГЖЪЫИЛЬФЗЖЕАЮЭЗИЪЖЫЖЗГЭПЛЗГАГАРАГЙПЛЪ
ЙКЪЫГЪГЦЩЖЪФНКУЬЭЪВЬЭЪВВИЙЕЕЭНЖЬАЬЭЪВДЖГЬЯДЛЮКУЙЗИЖЙАЬЭЪВЖКОДКЭ
ИАЖКОДКЭИАИЖЬЛЗГЭДЭЕАЕВЖЗАЬЭЪВЛДИЯЛДЛДИЯЛДЗИАЬЕЖЪЗЭЙЕЕИЖЬЕЩЛЬЭГЛ
ПРЭДЭЕЕББЭРФЗЖЯЩЛЬЭРФЭЙГАНЛЮЭДЭЕЕББЭРФЪЙЗЖДЕЭРФКЖЮЭЖПЕЛЪРАЙФЕЭЙВ
ЖГФВЖЪИЭДЭЕАЕЭДЖЫЗЖДЕАКФЙАЕЭЗЖЕАДГПКЖЙЖДЕЖЦЙЬЭГГЖЙФГЭЮГЕВИЖЪКЭЪ
ЕЭЯЕВЖДЖБЫЖИЕАОЭАПЛЪЙКЪЖЪГЩЖГФРЛЦЙГЩЖЙКФЗЭИЭЬЖДЕЖЦЙКЖГЙЪЭГФАПЙЖЙ
ЪЭПВЖЦЪИЛВНВКЖКЖЩЭИЭЮЕЖИЯЪАЪГЗЭИЭЪЯАВЖКЖИУДАЫИЛЬФАЗГЭПЖЩУГАЛДЭЕЙ
КЕЛКУДГЖЗЖДГДУЙГАДЖАЗИЖЙЕАГАЙФЪЙЗЖДЕАГЙЪЖБЗЖЭЬАЕЖВАЬЖЫЬГЙПКЖЩУГИ
ЕЭЕЪХКЛДАЕЛКЛЙВИУЗЕЛГЬЪЭИФПКЖВВЖЪЗИЖАЯЕЭЙЗЖРЭЗКЛЫЖГЖ

(b) Расшифровать текст:

АТЪДЙАШЗЧАЩЪВЦАЪЩЭДВЯХЧАЯЩМЦЦГВЭЪАДЕЖНЫЪВШСАЛДШЯЩЭВЧСЫЬГЦЭЭИГМСЮ
ЭВЧЭЬЫГХЭХУУХЭЦГИВФАЕЬХЮБДГЧЩЪГЖЖРШЯДЦБЫВГЦФАЬВЬЮБЬГССЮВДЪЫЪЪХФ
ЮЭБЭСЪКСХЧДКЭСЯЖВИЛЧЕЖШШЩЪВЯЩЯЮЪРВФЮЪДШЪШАЧШЦХИЗТЪДЪЪОЮБЬИЫБЙУАШ
ЗЧФИЛЧЕЖШШЭАЪЕЭЖЫГЯШЫШЕЩЧБЖЗЭЫЛЯЖЭМЬЭЛЬЦЧКЗЕШЖШГЪНЭВИГЫФФАЕСЭГЪА
ЩЭЕЖБМЩЮЖМФЧЯЭЫОВЕЭБЦБШЮВТЩЫЪЭОЧЯЖДЪЧЦЖЗШСЮГЭЫЛЭЬЪУАЕЪЭИСДВГЪФВЛ
АТЬКГЭЫСЫЙЗЬЛБВГХЭАРЭЯВЛЭЮТЬШЙЯШЪПВГЫБГЭАМЭЕВВЭЪЫЙСШЩБГГЧАХЯЪЦЪС
АЧБАЕЖЯШЪХЙЭХЧДЭШШЯБЪВЫЩЪГЯШЫШЕЩЧБЪЬЪЫЛАЭЦЛЛШЬЪХЭЖЪЪОЧЯРИМЧЧАНЖУ
ШЪЯЧЧЩАЧЧЧЯЭЕЬСХЙЭХЧДЭШШЯБЪВЩЯЫЙБТЯШЪНЩЭЧЗИХЫЫЬЬНЪАЛАЧАЕЭДЖЬЭЖЗШ
ЯББЬЦФЕЕГЛКЮЖЦШЪПРГПУХАЫПЬЫЭДШББДГЛЭГЖЗТЪДФЯЦВЩЛЭЫЩЪГЪЦВЫЪВФВЬДЭ
БСЩАЧШБШАЖЦФГКЭЛЭЦЪГХФАЩАНЭДГГМЧЯРИЦЗВЖЩШШЧАЯШБЙЛБВРЮЭЩЧЧЕИЪЩФМЛ
ОЩЭЧЖНХЩЫЪВЭЩЖЯБТЖЖЙЗХЬЭЖАПЬЫАДШЩЮЖВТЬДФЪЦВХЯЪЦЪСЙЗЪКЬВГЦФАЬВЬЮШ
ИЪФЯШЙЗТЪШЭЗЪЧЩЬРЩЭЕЖБЩЭЧЕАТЮБОАШСХЙЯСЪШБЭСЫШЕЭМЗЫДЖНЭЮЖЖШЫАЛБВР

ЖЬСЫЖДКАТСЯЖАТАПЩГНВБЕЗПРАЭГЫБХАЗФЭЮАВУУШКЖОЭФИРУЖШГГМФЭЬЮЛЭЦЪБХ
НФЖЧЖУДЖЧПБЩАЧТБШВЯРЧЮАБЕАХЙЭХЧДЖЮПТБИГМЬБВЭЮГЖОУЫЛЪЖТЪЫЙЪНЭГЖЧ
ЧВХЭЩТХШЭЪЩЭДВГЪФЬДНФЧАЛАЫЛШДИЧЗШЦЭСЯОЬАЩЭЙГИПЫДЮЭЦКДВЬХЦВГЯМЩБД
ЪЧУАКНЩЯБСЮЦЭЬАЧЧЩЖЯБТЖБКДЭАЕАБЧФЭЖАТСКЭБЬФФЭЩШАЧААЩЯБСЮЩЯБСЮЦБЖ
РЯЫЩЪГЯШЫШЕЩЧББЩВМАХЖУЫБГЛКЭЬЖЬГМЭЮФВШАЕЛДУБШЙЗЭЮЬКЪОЭЯЖЮОЩБГЭЭА
ВЭЪВЛАЬЪЧЛАДНЭАГМВФЭЯЭВОЬЕРЖОЭКЭЕЖНЖЬАТЪЫЙСНЪЧЭАМЭДГЪОЫГФЭТСАЖЧЧ
КБЕГНЪАЛАЫЛЫВЭМЬЖГБЧФЦЖАШСББЗЭБЫЪВФВЪДЭБЭФЖЕШБЫГЖФЬЯАЧЫФХЕЭЦЬЫЭЪ
НЭЖЙЗЪФЯААШАПЕВПЮГАЗПЪЯКЪРЬЫВЭЫЙШЯЫХЧДФГФЭЮЖЖМЭШЫГЩЯШЬЧШУЫКЪХЧХЬ
ЕЭТАПАТАЮЭЬЬЛДГГВУШБЗПЮШИСЫББББЗПЩГЭДФЭДВЬХЩБДЪЧУАКЦЭУШКДЪЧДКИЩСР
КИЦЧАЛЗЭЯЪЬАЫАЕИНЧКЬЪЭСТЫВЕТЩЫДЗПХААЯТРШЫГ

2. Разложить на множители числа:

   (a) 787491591925282180265943640133

   (b) 1028696339101614947256976171957543642435774850603764763164813

   (c) 157903051638762863928312817241435157049621938705480598521668576758659949707875963679943633 3

   (d) 774628652280247358565905566489741089307599542613990060991817842551243242167248291685741834148706724350778397499423264889

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 55649863016722374237770439626035212596418874678164005508044073822428949471191$
   - $e = 5$

   Сообщение:

   - $M = 49895028953339247808586392045560556714776660856310416995737952713124283861583$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 214861589886220463386926397009507206371$
   - $q = 311903500518872084432424167291137147393$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 57576154116107086498262219151440510294453266090412985896114049448864595918291$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 213079911575405151476157950765188782161$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 180503571453970064179678442963432968907$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 29230621956535017400776089675484841527 7$
   - $g = 12313805918451526791245077870533571003 2$
   - $y = 20484429456559463883485127340055850122 6$

   Секретный ключ:

   - $x = 88469750661047624617960018168647928627$

   Сообщение:

   - $M = 30379757067707110960937804533337518268$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 89637632507641609642895873187878024653$

   В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 219956204874427701192752169232260897271$
- $g = 107229009962075839180220055249284361516$
- $y = 153235561733408572348409121072894108335$

Сообщение:

- $M = 715433824657969375711115861010966541 57$

Подпись:

- $a = 218205588889113853986181408061812512085$
- $b = 154487084248089188298456016706419710681$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 641$
- $g = 249$
- $y = 50$

Сообщение:

- $M = 300$

Использовать следующий случайный параметр для создания подписи:

- $k = 481$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 11x - 13$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 77

1. (a) Расшифровать текст:

ЩЕЭЗСЖЧЕЖДИЗЖЗЧГВЪГЫЭЩВВРЪДЕГЭЖНЪЩЖЗЧЭЭБЪЧНЭЪЧЫВГЪЧАЭВЭЪВЧЖУБГУЫ
ЭЬВСЩАЭЧЩЕИШБГЪЮЩИНЪЖЭАСВГЪЭЦАШГЪДГЗЕЖЪВЭЪШАЧДИШМЪЧОЭВЧРБГАГЩРЪЕ
ЪЦЗДГЖАИНЮЗЪМЗГБРЖЗЕРЪЖЗЕЭЯЭЦИЩЪБЖЯЬРЧЗЭДЪЖВДЕЪЫЩЪВЪЫЪАЭДЕЭЖЗИДА
УЯГДЭЖВЭУЖЗЕВВРКДЕГЭЖНЪЩЖЗЧЭЮЯГЭБЦРАЖЧЭЩЪЗЪАСЩГАЫЪВЖЯЬЗСВЪЖЯГАСЯ
ГЖАГЧГДГАГЫЪВЭЭЧЯГЗГЕГБВКГЩЭАЖСГЕЪВЦИЕШЖЯШИЦЪЕВЭЧЯГВЛЪШГЩЖЭГЦНЭЕ
ВЭЦГШЗШИЦЪЕВЭГЦЭЗЪБЦРАБВГЫЪЖЗЧГБДГАИЩЭЯЭКВЕГЩГЧДЕЭЬВЧНЭКЪОЪВЪЩЧВ
ГЧАЩРМЪЖЗЧГЕГЖЖЭЮЖЯЭКШГЖИЩЕЪЮЭКДГБЭВИЗВРЪЧГЬБИОЪВЭВЪДЕЭЧРМЯЯЬЯГВ
БЭШЕЫЩВЖЯГЮЫЭЬВЭАЪШЯГБРЖАЭЪЭЫЪЖЗГЯГЖЗСЗЕЪЦГЧАЭЖГЖЗГЕГВРДЕЧЭЗЪАСЖ
ЗЧВЪДЕЪЖЗВВГШГВЩЬГЕЩАИЩЪЕЫВЭЭКЧДГЧЭВГЧЪВЭЭЯЕЪДГЖЗЭЧРЖЗЕГЪВРЦРАЭЧ
БЪЖЗКДЕЭЬВВВРКИЩГЦВРБЭЬЖЪАЪВРДГЦГАСНЪЮМЖЗЭЯЬЯБЭЩЧВЭНВЭБЭГЦАЩЗЪАБ
ЭЭЛЯЭКЦЪЕЪШГЧВГЭЛЯЭЪЯЬЯЭЩГАЫЪВЖЗЧГЧЧНЭЪГКЕВЗСЖДГЯГЮЖЗЧЭЪЭЦЪЬГДЖВ
ГЖЗСЖЪШГЯЕЖВЪЯГЗГЕГШГЧЕЪБЪВЭЦРАЭЖБЭЩАДЕЧЭЗЪАСЖЗЧВЪЖДГЯГЮВРБЭЭГДЖ
ВРБЭДГЩЩВВРБЭЧШГЩИДЕГЭЬГНАГЧГЬБИОЪВЭЪЧЭКШАЧВГБШГЕГЩЯЪДЕЭМЭВГУЗГБ
ИЦРАЭЖЗЕГШЭЪБЪЕРДЕЪЩДЕЭВЗРЪШЪВЪЕАБЭГЕГБЗЕИЦЪВЦЪЕШГБЩЦРДЕЭЧЪЖЗЭЧГ
ЮЖЯГЯЩГАЫВГБИДГЧЭВГЧЪВЭУЖАЪЩЖЗЧЭЪБЦРАГЧЕЧЕЖЯГЪИЦЭЪВЭЪЗЕИЦЪВЦЪЕШЖ
ЧГЪЧГАСВДЪЕЪБЪВЧИДЕЧАЪВЭЭЭВЯГВЪЛИЖБЭЕЪВЭЪЦИВЗЯЕЗЪМСУЭЫЪЖЗГЯЭБЭВЯ
ЬВЭБЭТЗГЖАИМЭАГЖСВЪЖЯГАСЯГЧЕЪБЪВЭДЪЕЪЩДЕЭЦРЗЭЪББГЭБЧЦЪАГШГЕЖЯИУЯ
ЕЪДГЖЗСЧЖЪЦРАГИЫЪЗЭКГЭАЭЯЬАГЖСЗЯГЧРБВМАСЖЗЧГЖАЭНЯГБАЪШЯГДГЧЪЕЭАГ
ББЭБГБИЕЖЯВЭУАИЯЧРКБЗЪЫВЭЯГЧЯГЗГЕРЪЬАГЦЖЗЧГЧАЭЧЗЮВЪЭЧРЫЭЩАЭИЩГЦВ
ГШГЖАИМЩАЧГЬГЦВГЧАЬВЭЦЪЖДГЕЩЯГЧГЦЕОУЖСЯЖЧГЬБИЕЖЖЯЬИГЩВЫЩРЧЬМЪЕГБ
ТЗГЦРАГЧВМАЬГЯЗЦЕШГЩЖЭЩЪАЩГБГЩЭВЖАИНЧГЮГЖЪВВЪШГЧЪЗЕЭЖБГЗЕЧГЯВГВЗ
ИМЭЦЪШИОЭЪБЭБГАИВРДЕЭНАЭБЪВЬЧЗСГЗЭБЪВЭЯГБЪВЩВЗЗГЗМЖГЗДЕЧЭАЖИЯГБЪ
ВЩВ

(b) Расшифровать текст:

ТБЫНДФДФФШЧЧФФУЧБАЭНВЙЭБАФГКФЭАМАЬЪПНСАЪСЙЩЪЯНМВЦЗЧКУЯАУАСЕХХЮКЫ
АЪБЪФЧХДЖЪЯШЪАБДФЙУВЕНКШБЧЪНЭЯЧНКЬЧБШУФЭЯЭВЬНЮШНЮАВТЮБОЮЧБЬЪЬСЖЧ
ГЯТИСЮЧЫОФАДЩМСЪЭЫЮЩАЮПЙУЯДЫЖЭЫЦШИЦВЯПЮЭАУЪВАЧУПНСЪЦЧДФГБЭЯЖЧФЕИ
ЧГДЪНЛБВПАВХЦЬШЖЧЮШЙЭЬАЧУЧДГБДБДЧХШЪЧХФКЫАШПОАЧУПЛЯЧЦЫОСЪДЖУБАЯП
ЭКЭГШЮФВКПЙЬАЗХАЬАЬЪКСЧЯЧУЧЯЭШНЫЧВФОЛГЬШЯУББВТФФЭЬФКЫЧЯОЙБГЬШИВЦА
ЦПСЪГПЗЧИГЫЮЭЪЮТВФВДМИЧГДЪФЬАЙПМЬЧЭЬБЪАУПАЬАЫФКЫЧЯОЙБКЪМНФЧЛПЮЪЭ
АЫШЮАЦФМКЭОАКЫЕЬШОЭВАНКУФЬСЖАДАХДЬЬВЭЗФЬЩФЛЯЪФПАЗЪЫЦБЬАДЩМСЪЭЫЛЯ
АЮПЙУАЭШВЧДОТОЭДЙЫВФФАЪКБЪФВДАОФМБЪЮЧЧЮБЕЬШИЬДЕНАФЯЬЧПЬЧДФЙФШЯШЛ
ЯАЛХНАЮВЖБШЪФЧКСЯАИЙФАУЕЖЬАФПЙЬЬВЬДЬЮЯПЛЯЧЦЫОСЪЭЫШЦГДШЗЭЮЯФМКДНЦ
НЩДЧЪОЛРЪЭНБЯАМЗФЯЯЕИЗДАЮИЧЪГЬЖЬЮЪЩПТЙЧМДЖЧЭШЮФЬЦПНБОЬСТЩЪЗЫОЯКЪ
ЧНЧЦЧХДСКБФСЧИФПОЬНЗЪПРКЬЯМЦХАЪУФЯЯЕБСЪЯШИАЬВЫЙКЮЪЬКХЮЪТЭЪЪГЬЪИЪ
ЮТЯЪЩЮТИФШЦЭДЫЪЯПЭКЭАЧДЗФУЪДЬЯЪЧФФХАЭМУЯЪФЙЭФАЛМЬНЗТГЫЧЯЧДЩАФМФФ
УЭНКЯАЦТБАЬЩХЛВХЙПЮВФЪОИФЯЦШЭЯАБШВЪАФЬШЖЧГЬШЧЮЧЫОЭЮЪХКАДЪЩМЭГЪЦН
ЭУЧЫБУЯЪФДЮАДПНЬЪЭТНЛЮАХУАЧЭЧЖЯРГЬКЪГАЫБУЮАУИЭЭАОКШЬЩФНБВАУЙКЫЪФ
МАЪФЕЕЬЭЪХИЬЧГЬЖЬБВШНБАХШЮЧЯЦШЖЭДАЪКТАЯПЖЭГЯЭЗАГЭИЭЭБНЬНБФАЦНБЭВ
ЫНЫДВТЮБОГЛКЯЪЛПЛВХЙПЮЬБЧЪЮЭЮЮПНБЧГТАФЭАЛЗЭЬАЬНЛЯГЬКЪЪБШАЮЪВББЯЯ
ЕИЭЭВАОПАФАТИЗЪВШЖЧЮЬЭЗЩАЮББЯДНХДЕЧХШЛЯФЪХШЬНЧТАЭФАХШЬАБЪДБЯНПЙФ
ЪЩДЮЪЭЪЧДЖЧХШНСЪВПЛЭХАШЙЖГДШКРВЛХНЩЙЧХКСЧЬЭЗФДБЬДУЧГЬДЬЩНМБТАДШЯ
ЯЖАЦОЭДЪЦКГЧЪББЫЪЯШЯУФЧХДЖЧХШАУРКФКНФГПКРЗАОДЪЪГЖИФШЦЭНЭУАИЖЩДАМ
МЧЛЪТЙФАЬСЧСЭЪЧДЩЬАНКЭГАЛБЬЯАНКЮВЧОЛЭЙДПЙЧГФШБЫЕБЪБУФАОДБЧЭИМЦХА
МКЯКЧХКРЕДЪББЬЯЧЦЛЯЪГЬПЮЧАЛПАБЧЯБСАЩЦПИЧЯТДЭУЕОПИЪЗОБШГДМДЩШЦЕЕДФ
ГЬЗЮВЧОЗТЭГМКЧЮЯПЙЧЪГМКРАЦЧКЭГБШМЧФЭЩПТЙЧМДЬГЧЦОЭГДЪЙЬАЮМКФЯЯШИА
АФПОФВЧВБЬАУЕЗЭЪЦЬДЩАВПЙРЕВНПУФЪРБ

2. Разложить на множители числа:

(a) 820320227093493363309344236099

(b) 1297874402166252087953940942113557378464189541934237654921917

(c) 1341314712478443150637758773452110348767489654592484165506405487400627921367117178278221989

(d) 184159369954795105184846998805041633703606304935304523082325270487724052538465928048377667709713620619105186596328138893 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 10101757683081041902295389736304770490310790960263209342358690545393952623349 7$
- $e = 5$

Сообщение:

- $M = 28638619588338253508086132813261624550743100147283122193603057539846630299770$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 290733746626627735695233146316880093383$
- $q = 21717314746767208100945569637499961471 3$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 14039985602134371597185712353180079702610676357308578215768223623063389628794$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 20485828499198936546102882828923312029 7$
- $e = 17$

Зашифрованное сообщение:

- $c = 18692358921153287214270076464170394898 5$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 30255720699237642620476452498324656207 9$
   - $g = 13433327611445812658793237126759098545$
   - $y = 24935345055954544028335377997169440880 8$

   Секретный ключ:
   - $x = 21893622192528120879554469984929892019 6$

   Сообщение:
   - $M = 16280454206542461660977736513424991071 6$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 13912709658738777746186932774276889865 3$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 27748401638472147499502522344729113345 7$
   - $g = 13428084655922769922970110962296998121 5$
   - $y = 43285966263405335718816517939562398575$

   Сообщение:
   - $M = 10247398464899098150183982539706459741 3$

   Подпись:
   - $a = 66369980035257292450902646555788865698$
   - $b = 24980959099906553590732032612282499766 3$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 929$
   - $g = 206$
   - $y = 72$

   Сообщение:
   - $M = 655$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 111$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 15$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 78

1. (a) Расшифровать текст:

АНПЪЫТЦЫПУБЫШЬЬЭОМШЪШЬТХЫШЧМТОПХФФППЛЪХТФШЦПЧОЧЬТМЫПШЮТАПЪЕЩПЪПМ
ПВЧЕМЫПЫШХОЬЕМСЬЕМЩШХШЧЬШНШТНХОТСХШОПТЛЭОЭЬЫИОЧПШРТОЧЧМПЫЬЖЫТХЖЧ
ШЦПЧЩШЪСТХФШЦПЧОЧЬЧТРЧПШСПЪЧШУФЪПЩШЫЬТЬТЯТУТЫФЪШЦЧЕУЦШХШОШУБПХШМ
ПФЛЕХЦЧПСЧФШЦЦПЫАСОМЩПЪПОЬПЦЩЪШПСРХШЧТСШЪПЧЛЭЪНЫЦШХШОШУЫМШПУРПЧШ
ИТШЫЬЧМХТМХЫЭТМЧФЭСЦТБЧТРЧПШСПЪЧЧЯШОТХЫЖШЬЧВПУФЪПЩШЫЬТМПЪЫЬЯМОМО
АЬТЩЬТЫБЫЭЧБЫОШХРЧШЛЕХШТЧЦШРТОЬЖЧЩОПЧТЩЭНБПМЭБЫЬЖЦЪЖТТМЧШМЧЕРТМШ
ЩЪПОЫЬМТХЫЖЦЧПТЫПЪОАПЭЦПЧЬФТСЦПЪХШЩШЫХЭВУЬПТМЧФЭСЦТБЫФСХФШЦПЧОЧЬ
ЭОШХНЧВСГТГЬЖФЪПЩШЫЬЖОШЩШЫХПОЧПНШЧВПНШТСОЕЯЧТШЛЗЬШЦТНШМШЪТЬЖЧПБП
НШЧШЧОШЛЧШЩШОЭЦЬЖШЛПСШЩЫЧШЫЬТРПЧГТЧШЬЩЪМЖЬПТЯМШЪПЧЛЭЪНПЫХТОШЪШНП
ГПЫМШЛШОЧТХТМШЬОХПЧЧЭИЛШХППЧОПРЧЭИФЪПЩШЫЬЖФЭОСХШОПТЧПЭЫЩПХТЛЕОШЫ
ЬТНЧЭЬЖТМЧФЭСЦТБШЛШЪШЬТХЫФРПЧПТЫФСХПУЫХЕВЖЬЕЦЬЭВФТМЫЦШЦОПХПЧПШЬЩ

ЪМТЬЖХТМЫЩШОХПЩШФЧПЭЩЪМТЦЫЦЕЫЛЭЧЬШМГТФЦТТЩЭЫЬШПЫФСХФШЦПЧОЧЬВНОПЬ
ФФЪПЩШЫЬЖФЭОЛЕЩЭХТЧПСХПЬХТБПЦЛПХШНШЪЫФЧПЧОПРЧЫХМЛШНЭОМОАЬЖМЬШЪШУ
НШОМЧПУЩЪШРТМПЦМТОХТТЛВФТЪАПМТФТЪНТСАПММШЫЖТШЬЩЭНБПМШЬЫТОТЦЫЧЭЦЬ
ЭВФМШСЪСТХТМЧФЭЗЦТБШЫЬМУЫЩШРХЭУФШХТЬЕЧФЪПЩШЫЬЖЧВЭЧОППВЖЫОЫЦВПУЬШ
ББШЧЦОПХЬЖЯШЪШВШФШХТШЬЫТОТЦЫТХТОШРОПЦЫЫТФЭЪЫЧЭФШХТСХШОПТМШСЖЦЭЬФ
ЪПЩШЫЬЖЧЭЬШНОЬЭЬМЫТХТЫПНШЪШМЧСТФЧЭХЫЖТСЦШХБХЫМТОШЦБЪПСМЕБУЧШНШМШ
ХЧПЧТЧПЬМЫТХТЫПНШЪШМЧЩЪШОШХРХФШЦПЧОЧЬСЦПББЬШЫХШМПНШЩШОПУЫЬМШМХТЦ
ШРПЬЛЕЬЖМЩПЪМЕУЪСМПНШРТСЧТЦВПСОПЫЖШЫЬМЬЖЫЧПНШРПШЬЩЪМТЦППМШЪПЧЛЭЪ
НФППФЪПЫЬЧШУЦЬПЪТЬЦТМШУЫФТЩЭВПФОШМШХЖЧШТЫЬПЧФЦПЧЧОТЬПЛПЫШМПЬШМХЛ
ЕЫЧПИЬЭОРПШЬЩЪМТЬЖЫОЪШЦББШЬЕЫЬЪЭЯЩШЫЦШЬЪТББШЫЬШЛШИЛЭОПЬФШХТМШСЖЦ
ЭЬЮШЪЬПАТИЩЪТЫЬЭЩШЦОШЛЪШЫФСХФШЦПЧОЧЬВ

(b) Расшифровать текст:

ЗЗЖВЭНПЙСНРПЯШФУЗИЫКХЗЗЭТИПЖЧЦХКТЬССЕФФЭЛФААТЕУЙЖЧСОСФЖЮНТУКОФАЩ
ПТРИББИЛУЭССЫАЩПСУЖЭЖСЖМББЛЙФВПКНТУКСУЦСРСУАЭЙРРХЯКЗУЦСУУЗЬЧРФФТ
БЛИЩХЭЧТТЖЧЧЯУЖЭХИПЕВХЖЖЕКЧСТТЮНХЮТАЗСГТХЙИПМФЖИНТТУУУОЭОНТЙЮУФФ
МЧФСДТЦССИСЭЦХКЦЭСЦУТУКМУЦСУЕФАЮХСУЦЧРФУХСЮИПСЧПСОМАПЦНМЬУМСРГНО
РЖЬУМУКЯУПСТЯШЪЗНБШНРЦЭХЦАУЭЬЛФПВЛИУЖЭКБИЙЬУБДЛЪХЦМЧРКЗПТШЙИДЧЗП
ЛКУЭЫОРЖЪКИРФЭЭФНЙЦСЛСФЭЮМФЙТУЕРФЧРППЙЮУТЖАЮХСДТХСИПУЯУЬЛЦФФИФФЬ
ЙУЗМЖЗСУАВЗЛЖМЫЦЕНЧЖЭИЗЖЯКППЙЦЖЮДНБКРУМЮНЫКЦФПРОУЭЬЬЗЕФЙРОФЛНЕПТ
СТНТТЫКЕУСФНПЗЙБЧИСЙЯБРКЧБКЫЗСЧТЛСТЩХСДМБКОДЯЗКЗПУЪУЬЖАЭЦХПТСНОУ
СЫНРХЦВЗКЕПЬШОПЖЧЦИНМЕШТРОЪУРКПАКМДЯЗКОКЛЩХИСТАЧЛКУЭЭИНУЭУУЗСРШУ
ЕХЩУМЖТЯУЖЗХЭФУРЖЭЛЗЗРКОФДЙЪБЛЩЙЫПСФТЯАМРЦЫКРПЙЭЧФФЖЪЭИНЛЬЧЮЛХСУ
ЛОМЯМПЭЬЪКРКРЧПНДИЯШЖХХЪАЫНЛАУДРВЩУРУОЧОХРУЭЧСЕПЬШОУЖЧЛЦКЛЩХИСТА
ЧЛУОЖКХМЛЩЙИТКРЭНКФАПЦАПЭЭЗЮЖЮУЕРИЛНЗЗПЧМЗНМЫТИЙСЩНСУЦЬУЕКПАНЕУО
ЭХИХЛЬРРЪЙТУЦТИЬННРСЮУЗУОЩЗФНЙЦЦФДТФООРЬУНЛУОЦРСФИССРЗУЭЗСЖАУХЦЕ
ТШЗЫЗЕЪИСТТУНИРЦФЫРЪЖЫЛОХЙБРСЪИЛНЫХЕВЦФДТФИССПФЬНУЙУРЦСФЧЗКПЕКРС
ДЫЧТРЭНБШОХУУКЬЗУЯНПРПСНОЙУЧТФЮЧЯЙРКОХРЦЗЦЭТЕОУЭРХКСВЙИПЙТЙУУЦФХ
ОЗЙУУУРЗЭГТТТАЧЛФЙСКОКОЭЙЦЪСЭЦЕЗПЛНЪСТАССФФФРРПЙТУНРХЭНТТТСУУЩПЯ
ЦХЗФЪЙСТТТУБЩЦЭЛИХЦФЖТРЕЯПЛДЙБМТЙЧДУМГЙАЦСДЙАЧРЭНЖЧСХРФТКСЛВЪСЛЦ
ЭФСГФЩНЕЗЦСУКТЛЧРЦТИЬННПМЫРСПЙАСЦФХЛЖСЕХБУДРВАЧУКСВЭНЯЦЭЖУЗСЖНХХ
ЛУКЪМСФФСНЦЧТЗРЕЯУФМЛЪФУЗФКЗФСТЯЖОЕТУХЛРЦЫКРФТТУНФТБКДСФЧЦОНФАЧИ
ТСЬШБСТЪЧЛПЧЮУФФФШЦТРИЭЖУФАЬЗСЙЖЯЧРРРЮШХКМСУКЮРЧЦИГЙЬЗСЖОВУЪЗСЛЖ
ОЕТУХИПЖЗКДНЗЭХСЖМФУХДЙЖРСПУЭЗСТЫЧЗФДТНРСЪИЛЗИЩСЭМЕУЕВЙЦГТТССНМБ
БТТМАНШУПЭЗШРСЮУФМОЪТКЖИФХЙУАЭЙРРНЯШНРВЦ

2. Разложить на множители числа:

(a) 778601349217922325860994841691

(b) 71603695617138690449625011853497768807166876949124508306170 9

(c) 82647815261766122857365766507466927450525458808400502207040375987967547737604433670444105 1

(d) 13907515963805098997327296972197231702922673204913338566917488604144709289518859347550719789473345793002657741575990967 11

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 659059845314941090326624421065412972310290670613550782217392563628981761618 99$
- $e = 17$

Сообщение:

- $M = 669484882239005470488132190635186469971650853928298632415249420766432861035 9$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 22464086935608766191642537535025091724 9$
- $q = 26849090059319496474582428434216844429 9$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 13036125969367364339426142223437661026151651192019388884005010580162207891326$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 190978899924182308939126120582648433959$
- $e = 5$

Зашифрованное сообщение:

- $c = 25368738627509226836727953287366445281$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 26080564526321348841337641179916249615 1$
- $g = 77967958045543823401644868998312029227$
- $y = 16417686766960642497999293552956972248 8$

Секретный ключ:

- $x = 16125716967387279842607753423886693882 9$

Сообщение:

- $M = 22430442200316764186941361870001044757 2$

Использовать следующий случайный параметр для создания подписи:

- $k = 14350195689359569504812307613805317177 9$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 25427053112732779774457500114702533463 7$
- $g = 21946852623559587968841923838396639420 72$
- $y = 11931095169904780470230235098304667911 0$

Сообщение:

- $M = 15742186835991463836389482069010541646 4$

Подпись:

- $a = 23508306131596412568409548241126092687 7$
- $b = 29909835085704410564389620256132887836$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 647$
- $g = 151$
- $y = 552$

Сообщение:

- $M = 200$

Использовать следующий случайный параметр для создания подписи:

- $k = 341$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 10x - 12$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 79

1. (a) Расшифровать текст:

УЮУТЫЦЪЫШЬЩУЫЦЭБСЕУРЭЮЬАЫБЩЪЫУФЦЩЦЯАБМЯРЬМЮБШБДЩБЧЮБШБДЩБЧЮБШБСЬ
РЬЮЦЩЦЬШЬЩЬЪУЫЫЬЭЮУТЭЬЕУЩПЙЯЪБМЩМАБМШХЫКАШЬЪБЭЬТЩЬЪББЫЦФУЫЦМПАМЖ
ШЭУАЮЫТЮУЦЕЖУЭАЩЯРУЩКЦЕЯАЬХЪЫЬМЦАЬЩШЪУЫЫУБЭЮЪКЯЕАЬАУПУЯАЬЦАЭЩМЫК
ТЭЬДЩБЧБХЩЬТАКВБЭЬДЩБЧБЫУСЬЮБЕШБЫУЖУРУЩЦЩЯЭБСЕУРЬЭБЯАЦЩЮБШБЯШХРЯ
БЯЪУЖШЬМУСЬПЩСЬЮЬТЦУХЫАКЬТБЮУЩЬАЮТЬЯАЦЭЬТЙЪЦАУУСЬЪУЫЭЬТЫЩЦЦЬЯАРЦ
ЩЦЫЯРЬПЬТУЯАЩЯЪЬАЮУАКЫЭЮЬТЫЩФУЫЦУБФЯЫЬЧШЬЪУТЦЦФЦАУЩЦЫЕЩЦЭЮЦЯСАКЬ
ЫЦЭЬТГЬТЦЩЦЬТЦЫХТЮБСЦЪДЩБЮЯЭАЦУЦЭЬАЬЪШЩЫЯКЯЪЬХРЫДБСЮЫЦХЬЫЫЙУЯЬЩТ
АЙЯАЬЩЦАБАФУЮЬАЫЙЧЭЬЮАЫЬЧРЬЬЮБФУЫЫЙЧАБЭЙЪЦЯРЬЦЪЦЫЬФЫЦДЪЦЮУХЩБЫЦГ
ШЬЯЙЬЫЦЬАЮГЦРЯКЭЬТГЬТЦЩЦШЮБШУЭБСЕУРШЬАЬЮЙЧЬПИРЩЩЦЪЭЮЬЗУЫЦУЦЭЮЦЫЦ
ЪЩРЯРЬМЖЧШБРЯУЛАЬЭЮЬТЬЩФЩЬЯКЬШЬЩЬАЮУГЕЯЬРЫШЬЫУДЭБСЕУРРЯАЩЯШЮУЯУЩ
ЦЯЬЖУЩЯШЮЙЩКДРЯЬЭЮЬРЬФТУЫЦЦЯРЬЦГЯАЮЖЦЫУЪБЭЬТРУЩЦПУЩЬСЬШЬЫБШЮЖУЫЫ
ЬСЬПЬСАЬЧЯПЮБУЧТРШХШРХЩЦУСЬЭЬТЮБШЦЦЭЬЯТЦЩЦЫЯУТЩЬЫЬПИРЦЩЬАДБСУЮЯ
ЦЪБЕАЬПБТУАЬПУТАКБЫУСЬРЛАБЪЦЫБАБЮХТЩЯФУЫЯШЦЧШЮЦШЫУЯШЬЩКШЬЮХПЬЧЫЦ
ШЬРРЙАЗЦЩЦЫШЮЙЩКДЬРЯЦЩЦЯБУСЬЮЬРЫБЮЯАЮУЭЫЫБМЦЮХТУАБМТЬЫСЬТЦЫЦХЫЦГ
БЯЭУЩБФУЫЮТЦАКЯРУУТБЖУСЮУЧШБТЮБСЦУАЯШЩЦЭУЮЦЫЙЯБЫТБШЦЕЧЫБМЭЬЯБТБП
УЩКУЦРЯМЮБГЩТКПАМЖШЦЪЬЦШЮЦЕЩПУТЫЯАЮБЖШЬАЭБЯАЦАУТБЖБЫЭЬШЫЦУЬАДЙЮЬ
ТЫЙУЬАРУТЦАУЪУЫШЦРЫБШБХЪЦЕБРТЮБСЬЫРХСЩЫБЩЫРЦЯУЩЦДБЦБХЫЩЯРЬУСЬЪБФ
ХЩЬТУЦХШЮЦЕЩЬЫРЦЯЯАБЭЩУЫЦЦЕАЬЛАЬРЙЯЫЦЪЯТУЩЩЦЯРУААЙЪЬЧЦРЫШБХЪЦЕБТ
ЩЯЬЩТАЯШСЬЩЬРБЖШЫУАЮЬЫБЩЦАУПЫЦЖАЙШЦЭЮБЯЯШЦУЫЦЭБЩЦАБЮУДШЦУЫУРЕУЯА
ЫЬЪПЬМЭЬЩЬФЦЩАЙЯРЬЧФЦРЬАЯСЦЫБЩЬАПУСЩЬСЬШАЬЮФЫЦШБЫАКЯАЮБМРУТКЪБЯШ
ХЩЭБСЕУРАБАЪЬЩЬТЬЧШХШБТЮЦЩУУЯПЩУМЭЬСЬЩЬРУЦЬЫБЭЩЪУЮАРЫЯАБЭУЫЦШЮЙЩ
КДЭБСЕУРБУГЩЫЮЬТПЮЬЯЦЩЯХЫЦЪСЩРЫУХРЫЙЧСЬЯАК

(b) Расшифровать текст:

ОСМГФЕРФЖЮОТЩПАИУЙМШСУЖПЛРЙОЗДТЖЖИОЬНСЖМОУЧТКЛЕЦЙЛОМХПОНЙОИЖОГМР
ПСУМУБМЖСПУИТЦЙОЬВЙМКГПФТЖУЯОСБППХУШГЖСЖМЛДПЕБЛОРЖЙПСМТОЛЭСПЛОМЗ
ГБРПЦОКЧУТТПМТТЩБЛГЫЖИППЫУДИОЙПФИВПТЖКЮЦПКЧЙХУДТЭЕЖЗОДТСНКФВЛМЕР
ТТОЬТОИЗООСЛКНЖЪСПЧЯХЭЮМИЧТЛЕЦТУЮЕШПТВРПРУКЛЭОПКТРЧТОИУЙНБНОЙУИО
МТЕКЙШЙМКВЖОТЖЗМТОЖЧДТМКВПВООКПРГБЛЙОПИРТХУКНЙМОБПСМУБЛЯПЖЯКПЕФА
ЕУТУМЕИЦЭЮСПЦЛКМФСЙЖЦЙМТЯЛГСЬИСУФУБГЙЫЖНКЙРРПНЛЦПИИРТМПЧЙЦЭЙДГРЙ
НОГЙСФЕОСФЪППЕЖАУРФЖНЕШЙОЙКПРФЙИЛЪЙДСРЧДЗСФЖЙАЕДТИЮЛЖЫЖЙНПЗПЮВПЙ
ОЙЫЖФТНУЗИЖЙИЙХРБШЙПЖЯОРФЖМВУАЕКЧЭОРДТОРЙМООТГНКИПЖИУРМЩБТЛТНЙЕР
МТШМПТОЛРПХЙОППРПХИЩЖВМИОУСДНФКЕБТЖЙГЧДУМИЙЕДТИИУЗСЖПЖУТПЩТПЦЩЮБ
СМОЛРЖЖЗИЛМКДЕТПЙЛОРИЖОСЛТНЙЕГФФЖИУТГБЛЯЙДКСФИЙОЬГЫТДМЬФТНТСЙМБ
МЖЗПЙПСУЖОЕЛФЖЛОТЦЙЙОРТЛИЕТЦЭЙДПЕОКВИЦЭОЕСУЖЙИЖЖИОЬУЙСЛЕОМЖЮСЛФЙ
УЛГСЖНЕВТОИЕЗИФОЕНКЖЙИУХОИРЭЙЙЮНПЖОБОГТИМЗЙПДБНЖФМЩТПЙЪБНЖЕЖАЛФЫ
ЩБЕКЕЬОЬРТЛИЕТЦЭВЕОТЯФВВФЙЙООЦЖЛЕСАНКЖЖЦПЖЗУАЖЕПСТУБКЧМЯЖОДИЖЯОС
ХТОРЖПЖИТПЗЕЭОДИТОСЬЭФОСЖНЙВЕОМЩЖИНММБНЭОЙБВЕТГПШЛМГАЕГОЦЙЕТМЕОТ
ПЙТОЬЦТУБЛТОИОЬШЦПЮДПЖФФКТОПМЕЖСКАЕУХЖЭЕНЧЗЙЕЗЙМДДЖЖЙТСЛТСБЕТТДЗ
ШФХЭПМЖФЖОЬТОИЗВВЙЩБНТЦГБНЖКЖЗИФХУППЙЦЭБЕЩЖВМИОЧВЭБВХЛГЛТЦСДКУЙР
БРЭУПЙИНВУЧВЙИОКВНФЭЪИГСПЮНФЖМЪБМЙОКДЖПАРФЗПББЖИОЧЙНПЬЕНПЖТБЖЖС
ЙЖКОЙНКГФИУШТЖЕЖМОУЧТКЛЕЦЙЛОМХПОНЙОИЖОГБУЩКТУЖАИЧМВЧЛВЯОББМЗПМЗФ
РОЙЕНТДПВИЦЭБЕОХГКЮПЦГБТТЦГБНОТТОЬРТУППЙПДКЛПЖФКТШСЙБМОТЯКВМИЖЗО
ГИСПГНЯТЗЬНЙМШКОЧМЮГППЮЕНТЖЕВШЙНКНТТТООМЫЙОТЖПЭПВЙИЙОИИХМБДФВЪБ
ЙДПГЧКЛЗПЮОСЦТОРЙСОЧЕСТНЙИТЦЬЯЛГРУБЖОХМКБПИ

2. Разложить на множители числа:

(a) 588549823973395736474321591983

(b) 781988788904886077733008936419244140689875118288554225776001

(c) 86127315025292295835579929423040328647827180363268358737740545832093243000098566371449491 9

(d) 133621959850419409031284292204555551696018694818473947814232148119123169143651038867792190922167728432929250107040100296 7

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 438904589738270844339853002627162727073794958812942541590875344094307994705 63$
- $e = 5$

Сообщение:

- $M = 26285804951894194904329795732833799663572495184071836090110215939502269492197$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 23589328862093925460216293514472427739 3$
- $q = 19567024207435467315753344288400271573 7$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 29448421552714672063592742335538937078546239462081694667381147709431937591418$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 15931172125371048709257256419243450367 9$
- $e = 5$

Зашифрованное сообщение:

- $c = 30044857145371888904749570387732962538$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 33243701439497975932545075075399050946 7$
- $g = 17169804867612988143123362561689669955 9$
- $y = 22783415780507087962354251089616567913$

Секретный ключ:

- $x = 12725820895787094423639592989094249812 9$

Сообщение:

- $M = 16168508651094977772752087663342229189 0$

Использовать следующий случайный параметр для создания подписи:

- $k = 11063344381830617521272285865847912512 1$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 23335087265025713528170987065832357859 9$
- $g = 11520722699683285340175516858957777144 2$
- $y = 50033394449117476364656622468392381024$

Сообщение:

- $M = 13476231579210450926836877969328279943 4$

Подпись:

- $a = 50812760159446178331644821633557499983$
- $b = 54348420712820040503931390619556747280$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 947$
- $g = 481$
- $y = 792$

Сообщение:

- $M = 939$

Использовать следующий случайный параметр для создания подписи:

- $k = 243$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 5x - 11$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 80

1. (a) Расшифровать текст:

УЙКИЖКВКУЕЭЪЭИАРФЙВЯГЖЕПКЖЩЩУГЫЖЙЛЬИФЗЭКИМЭЬЖИЖЪАПЕЛЬЖЩИЖИЯЪЭЕЭК
ЛЬПАЛЬГЖДЛИЯЪЭЪЙКИАЕЛЫИАРВЖКИЭЗФЭЪЕЭОИЙКЪЖЪГЬЛДБЗИЖДЭЕПКЖНЖПЭРФЖ
КДЭЕЕЭЖКЙКЪБВВЖЭКЭЩЭЬЭГЖЬЖАЕЖЫЖЗИЖПЭЫЖВКЖЕАЗЖЗКЖКЩКФВЗЖЙГЛЮАДЕЭЪ
ЭИЖБАЗИЪЬЖЦАКЭЩЗЖЮГЛЦАЪМЭГФЬДИРГУАЪВЕЯФВВКУЬЛДЭРФЕЭКЖКЪЭПГЙКЪЭИЬ
ЖЙКАЦЗИАИЖЬЕУБЬЪЖИЕАЕЗИАЙЫГЫЖЙЛЬИУЕЭАДЗЭИКИАОЭКЭЩЭЙГЛЮАКФЕЭДЖЫЛВ
ЖГАКУЪЙДЖДЬЭГЭЮЭГЭРФДЕЭЬЖЩИКВЖКЗЛЙКАДЭЕЪЖИЭЕЩЛИЫЗЛЫПЭЪЯЬЛДГЙВЖГА
ЖКЗЛСЛЙВЯГЖЕКВЖЩЭСЭРФЙГАЗЖВИБЕЭБДЭИЭЗИЖКАЪДЭЕЕЭЙГЛЮАКФВВДЖЫЛКЭЩЭ
ЪХКЖДЖЩЭСКФЙЖКЪЭПГЙДЯЕЭРФЕЭДЖЪЖГЪЭГКАЬКАЗИЖКАЪКЭЩЗЖБЬЛЬЭГКФЕЭПЭЫ
ЖКУКЭЗЭИФЙДЕПГФЕАВЙДКИЭЩЛЭРФЗЖЪАЕЖЪЭЕАЖКЙЪЖАНЕПКЖХКЖЩЛЬЭКЗЖНЖЮЭЭ
ЙГАЖКЙГЛЮЩУЖКВЮЛЙФВЖЫЬЙГЛЮЩДЖЗЖЕЬЖЩАКЙЫЖГЖЪДЖЪКЪЖЭБЪГЙКАЖКЗЛЙКАР
ФДЭЕЙЗЙАЩЖВЯЕАРФЩЖЫКЭЩЙЛЬФЙВЯГКЭЩЭЗИЪЬЛДЖАЙВИЭЕЕЖЙКФЗЖИЯАГЗЛЫПЭЪ
КВАЩУКФЙВЯГЖЕЛЬИДЭЕЗЖЗГЭПЛВЯЕАКФКВВЯЕАКФДАГЖЪКФКВДАГЖЪКФЙКЛЗБЙЭЩ
ЭЕЪЙЭПЭКУИЭЙКЖИЖЕУАЬЭГБПКЖНЖПЭРФЯЪКИЗИАНЖЬАЙЖДЕЖЦЗИЖЙКАКФЙКЭЗЭИФ
ЙКЛЗБЙЭЩЭЙЗКФАДЭЕЛЮЬИЭДВГЖЕАКЖЙКЪАГЗЛЫПЭЪАЪУРЭГЕЛГАОЛЕЖПФЩУГКАНА
ДЖИЖЯЕДЭЙОАЯЪЭЯЬУИВЖЙАГАЖЙЪЭСЗГЖСЬФАЪАЙЭГАОЛЪВИЭЗЖЙКАЪЙЭЩУГЖЙЗЖВ
ЖБЕЖАКЭДЕЖКЖГФВЖЪВЩВЭЙЪЭКАГЙЖЫЖЕФАИЯЬЪГАЙФВИАВАЯЗЖЯЬГУНЫЛГВЪЯЫГЕ
ЛГЕЬЖДЙЪСЭЕЕАВЙКЪЕААЪЖИЖКУЩУГАЯЗЭИКУВЯГЖЙФЪЙЭЪЕЭДЩУГЖКАНЖЗИАРЭГВ
ЙЭЩЭЕВЪИКАИЛАЕРЭГЙЪЭГФАПЫЖИЦЦСЭЫЖЗЖДЖЭДЖКЙЛКЙКЪААЪЭЙКФЖЙЪЖЩЖЬЭДЖ
ЭБЖЩИЬЖЪГЭЫЖЕЭЙВЯЕЕЖЙГЪКЭЩЭЪГЬУВЖЙВЯГЖЕЗЭИЭВИЭЙКАЪРАЙФПЭДЙЪЭКЖЙК
ЪАДВИЭЗЖЙКФАЗЖБЬЭДВЛЬЫГЯЫГЬККЭЩЭВЖЭПКЖЯЫЖКЖЪАГЗЖВЛРБВЩКЦРВЬАЗЖПА
ЪБЙЭЩЭЬЖЛКИВВЛНИАЙКЯЗЯЛРВЖБЗЖЙГЭЬЖЪГЭЫЖЙЖЪЭКЛАЗЖЛЮАЕЪЙЩЖГФРАДЗ

   (b) Расшифровать текст:

ПЕГЭЗДАГЫЦАЕЭШРФБЩЪНЛЕЕЬДФБУЮОАЦМТБИЯЭЮДРБЖЯПЕАРЩЗЯБЧЭЗЖЯЭЫПРЫЯЫ
ДЦФРШМТХГШЫЪОБЮБХЧЪЯДШШБЬПЫЧГШЕШДССНРЮИОНЧБЮЬНДЫВЧНЪШЛВЛТЮСЪЦШБЩ
ЫКТХЗЙРЫФЪЮДСАЭЧНПВИРЦТХЬСПТЯАЮЗСАЖПНТЯБТРЯШЗЫБЭЫОХДРБЧЮСШЫЭСКХЯ
ВТЖЪЭГЮСПЫЗЙДРБЧИЧТЮЧЩДЮЕЪЮМХЯЭЬНЭДДЫПУШВХЭВЮГЬТЕЫЯЭТШПВИИЫЕЧТКЩ
ШВПОЭЫЯФМАСЭФААЦЩТМЕШАХРПШАЙЗДЫШСДЩШВЫРЯХЭШЗЮАЭЩБФВЪЭСХЧЩЙЙООАПС
ЧББХЖАЯАТМХЫДЭЗПЫЩТБЮШШЫЦЯБДЭНХДКЫГХЮГДСЫАЪЮГТЮАЩМТАЭЧЙЫЦГПНЬГГЮ
НЪЖАТВЮХЗТЛЪБЗТЗСБАРНПЪЩИФШЫГВКЪЭГЪДГЪКЭОТЮДЭДСЮЖЭЖЩОНШДЪЫБЧНЯБЕ
ИДПБЧЮЭЪБМЙМХАГСМАЯЭЪТЯЖВТГШЫБЪДФЧЕТЛЯПДЫТЯГИЬПХЛАХЛТАЬПСЙБЗХЛТА
ЭЬТРКЪПОЫЛЪШЙЪШБАТПБЕЫСТЦГЮСЫЮЯХАХЕЯФОЭЩЪЬМЯГГЦЙЫСЗЯПЮЭЭВКЫЛЩТИЪ
ГГССЫЮДХКЮАИШЗГШЧЮДЪИЧЮСЭШЗХКЬЖШДДПБВОЪШБЩТСЬБЩЫПЫЩВЫЛАХНААТЫЧЧЗ
ЭЦЭФРЧБЮЕОЧШЧДДЭЛВХДЮБЦТРТЧВХЙХБЯЭТУЮЭТВЫВЕХМПАЖТАПЫЩЬНСБЦЫРЯГЖЯ
ЗЧБЗЫПИЬЖХКЙАГЬПЫЕЭПТЭШМХКПДЪЩТДШБААИЮЖПЗСШЗТКТЯВЧМААЪЬТРКЪПБТДЪ
ШНЮББЪНЛВГФГЫГГПКЮЫЧТКТЮБЪДЮЧЭЯЫЮДВХЛПЭЭОЗЯЭИЩЪАДЪШЗЮПЧОДШБШЫПЮЭ
ИЛЙЭШДЫРЯПЖЧЖШВИРЦТХНХПЫЭГЬКТКЪЩТЯЕЕХМАДЗЫОЭХОТЛАЕЕЫИЧБУЮДЭЧЛТЛЫ
ШЖХКЙАГФАХЮГЮЫШБНСЗЯГГЪТШЫЖЙЙЫЮГЧНШПМХЙФЦЕТЛТЮЯХАХЕЯЬНШШЗТКЮЕГЦР
ЯБЮЭЖСЮЖРНШБЖЮКХЛЯЫЛЩАЪФМЧББИИХЖЧХГТЮЖПДШПЭДАТЩЧЕДРБВЩМПДЗЭДДЖДА
ВДШЧПДШШАЫРЯАГПЗЯПЖОСЛЛЯЬДЯГВСПТЫМЧПХКАСГЙЭВТОЫЭЭЪЫЩШВЪРЯГГЮСХЮЪ
ЯОЫДЕТГХРЗХФЩБНТМЮЕЕИИВГРДРЧЪАТЛАВИРЦТХГЬСЙФГРГШДЧХГТЕСЮМАДЩХРЙА
ГОКАКГЧРЬДЭОНРБЖАГЭПЖЬРХФГЫСТЙЕЫГЪБЮРНПБЕХКЮХЪШЫХКИЮЕХХЖЙГЦФГРСТ
ФЪЮСЫЮЪЯЖСГЧЮСПБЧЯЫФЕГДСЫЯЪЪРЯГЭЧОЭЫЬЭЗШЫИЮОЫЭГХКПШЯФСТФЦАГАФГРЛ
ЫЮЭЯЫЫЪЮДЫТЯЗАКАВЪХТЬББХМЯПИУМТДЗЪТКЕГЯЖЦКЭЦСАЮИЬЛЫЦВЧНЪШЛЪДЪЛИЯ
ЙАГЖЮДЭЧЭЯЫЬЖШДДПЭЖДРЯЫУЮЛЫЪЧЪДГЫАХМТГЖЮКИИАХКХВЕТМТФЕТВЪШИЩДЮЕВ
ИЛ

2. Разложить на множители числа:

   (a) 863590593161320740089554573339

   (b) 764233188173920101416641026216761257907263351617229513306261

   (c) 13884261834149108273491321795248660974067301235543156640730877599282069462339795448680511153

   (d) 840636802946766375290350383729828429512641516723683261360989662164534088023598018139164708170991045815064000603721377177

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 346629511130891148671706868149639946502364349549006015846653377286594814569 77$
   - $e = 17$

   Сообщение:

   - $M = 120082628446616131863272119694780585078133365438980080561781445222830529695 41$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 23888536295451809732956926066570499693 7$
   - $q = 27481900299034412020841514121430561806 3$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 35776394906572818388714854232623689489941971467428034034935058247638153253837$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 30733002387283143532621961542882579256 3$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 19343104808627153765857414630606450815 9$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 33422011220401964446080769819709778024 7$
   - $g = 32305010973064788738343820136323121285 6$
   - $y = 20873916554430314058391788859704614757 6$

   Секретный ключ:

   - $x = 25648820989826543936985542881057382503 6$

   Сообщение:

   - $M = 30857976943606561186040023694577756104 0$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 10122828607806027696619072700322996414 7$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 21592465321060840280570735729357019544 1$
   - $g = 87474497056765246972480785301874027 88$
   - $y = 44390182583195390567070810832785564833$

   Сообщение:

   - $M = 31191511252382293726816387955146753779$

   Подпись:

   - $a = 81083590013573471573927889932923857018$
   - $b = 13164665438743539346193721194590977815$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 787$
- $g = 433$
- $y = 404$

Сообщение:

- $M = 262$

Использовать следующий случайный параметр для создания подписи:

- $k = 65$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 4$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 81

1. (a) Расшифровать текст:

ПЮЯШХПЧЫЭЫЯЧХВЮШЫПВЫЬХЮПЮЬТЭПЬАРДТПХЕЦЧАТРЫЮЧФШАЯПТЭСХЯТШЙЪЫДЯЫЮ
ЩЫФПЪГАЮЬЫЮЫОЪТОИШЫАЮЯЫЯЙЬЭЫЯХПАЬЭПХШЙЪЫРЫЫЭАУХЩЪТЪХТЩЫТОИШЫЬЭХЪ
ЯЫДХЪЫПЪХЧЩХЮПЪЫЛЬТОШРЫЮЧШЫЪЪЫЮЯХЛЫЪХПХСТШХПЪТЩЫЬЭЫЩТЯДХПЫЮЯЙХСТ
ЭФЫЮЯЙЩЫШЫСЫРЫДТШЫПТЧЬЫСЪШЮЭЫЬЫЯХАЮШИЕШПЮЯПТЪЪЫЮШЫПЫЩЫШЫЧЫЮЫЮЬЭЫ
ХФЪТЮТЪЪЫТЧТЩЯЫПЬЫШРЫШЫЮРТЪТЭШЫОЭЯХШЮЧЫЩЪТХЮЧФШЮАШИОЧЫЛРЬЭЬЫЭЖХЧ
ЬТЭПИТРЫШЫЮЪПЫТЪЬИВЮЫПТЯВЬЫСЛЯЮЫОИЧЪЫПТЪЪЫПЬЫШЙФАСПХУТЪХЦЪЮЯАЬЯТ
ШЙЪИВКЯЫФЧЫЪЬИЦЬЫЭСЫЧЯТЬТЭЙЮЯЪТЩЬЭЫСЫШУЯЙЮЫОХЭЪХТРЫШЫЮЫПРЧЫШШТУЮ
ЧХЦЮЫПТЯЪХЧЮЧУХЯТЪЩПЕТЩЪТЪХТЮЯЭХДЫЧПРШФТЯЫПЫЩЧБЯЪТЬЫЮЬТЕЪЫСЫЬХШЯ
ЭТЯЙЛЮПЫЛДЕЧАФЪДХЯТШЙЪЫЭФОПШТЪЪАЛЭЫЩЫЩХЫЯПТДШРТЪТЭШАСАЩЛПЕТЬЭТПЫ
ЮВЫСХЯТШЙЮЯПЫДЯЫЬТСЫШУЪЫСТЦЮЯПЫПЯЙЪХЪЮЯАЬЯТШЙЪЫЪХЫОЫЭЫЪХЯТШЙЪЫЧЧ
УТЯЧРЫЮЬЫСХЪЧЫШШТУЮЧХЦЮЫПТЯЪХЧПЫФЭФХШХФАЩШТЪЪИЦРТЪТЭШСЭАРХВЮЬЫЮЫ
ОЫПЯЧЯХЧЬТЬЭТСЮЯПШТЯСПХУТЬХТЫОЫЭЫЪХЯТШЙЪЫТХШХЪЮЯАЬЯТШЙЪЫТПЕТЬЭТП
ЫЮВЫСХЯТШЙЮЯПЫСПХРЦЯТЮЙЬЫСЧАЬЯТШЙЪЫЩЪТЪХТПЕТПТЮЙЩОШРЫЭФАЩЪЫСПХУТ
ЪХЬЫСЧАЬЯТШЙЪИТЯЧЯХЧЫЛСЫЬАЮЧЛЯЮХЩИПЫЮЬЫШЙФАТЩЮПЕХЩЮЫПТЯЫЩЫУЪЫОА
СТЯЫОТЖЯЙФРЫШЫПАОТФСТШЙЪХЧЭАОШТЦЮТЩЙСТЮЯХШХСУТЮЯЫХФЮТЧЭТЯЪЫЦЮАЩЩ
ИХЯЫРСЬЭТЭПШЯЩЫУТЪЬИЦСХЭТЧЯЫЭОАСЙЧХЭРХФЮЧЫЦОЭЪЬТЧЫШШТУЮЧХЦЮЫПТЯЪ
ХЧТЮШХКЯХПЫЭИЪТПИССАЯЪЩЮПЫТРЫЯЩЪЮЧЫПЪЪЫРЫЬЫЭАЧЩХЬЫЪЫРЩЩИТЖТЫОКЯЫ
ЩЬЫСАЩТЩХЬЫЯЫШЧАТЩЫЯПТДШРТЪТЭШЫСЪЧЫЪСШТУХЯПЫПЮЧЫЩЮШАДТЬЭТСЬЭХЪЯЙ
ХПЫТЪЪИТЩТЭИРЫЮЬЫСЬЫСЦЯТРЫШЫЮПЕХЬЫФЧЫЪЪЫЩАЬЫЭСЧАПЮТЩЪТЪХЫЧФШХЮЙЬ
ЭЫЯХПЪИЩХЩЫТЩАПЮТДХЪЫПЪХЧХРЫПЫЭХШХЫЪТЪСТУЪЫЮЯХПЫЦЮЧЫЪТПТЭЪЫЮЯХАС
ДХЫОЫЮЯЫЭЫУЪЫЮЯХХЯЫЩАЬЫСЫОЪЫЩПЮТЬЫШРШХДЯЫОШРЫЭФАЩЪТТЫЮЯПЯЙЮЬЫСЬЭ
ХЧЭИЯХТЩЬАЕТЧФЧЭТЬЧЫЦЧЩТЪЪЫЦЮЯТЪЫЛЪТУТШХЪЫЯЧЭИЯЫЩЬЫШТХЮЬИЯИПЯЙЮД
ЮЯХТЫЭАУХЪЧЫЪТГРТЪТЭШПИЮШАЕППЮТЩЪТЪХПИЯЭТВЪАШЬТЬТШХФЯЭАОЧХХЬЭЫХФ

(b) Расшифровать текст:

ЖЙСМПЛШШЛПЙМЪФМЯЮЭЯХШКГВЧЯАИНШЛЖУИМГЮЦНЩРБЭЯХШДЭПХКДКМХЙДЫЛЦЮШЦН
МЛОФИПЛШЯОТХФГПХЙППФМЬПФДЙЯНЮВФВСЪЮУЗНЩЙПЛДЧЗЧЯНЮККИЮЪНПЕЖЯИПЗЛШ
СПЕКОКЦККШФПЫКППЪСПШЕУИЕРИМДНСЖПЬЙЗФФЯУСАХЛЖУПГПКЬЛЯЭПЭЩЙЛИЯЫДМП
ШЕФНОЯБЙЯМИЛЩЬКЬЕТЛШФЙЧЦДОКХЬЙОЛЯЕНЯИВЫЖЪЫФЫЗСБФИИЧЕЭЯКЩЛШМЮФИШЬ
КСЗЧЯНЮЩФЛЖЪВЦЕОИВПИАСПИХЗЫЛЦКБТКМЖПЫНХЛОЪЕУВЗЪТЙМДЧВМКПЦРПЮКЧАХ
ЗБШЛКЬЧШЛТЬДЮЩФВКРКХЭКЭИХЬИЗЛИЖКЧФТВКЮМХЕЙЪПВЛБЬБЭПКУВЙЗФФМХСПОО
ЩЬКОИПСОЪКУЫЧЧЛФЯАЪКППДЪОЩЬДЧЕФЛИЗЛШМЗФОГИАЩЕЙЛБНШТИГНШЩИИЗАХЬКЬ
ЕТВДЩВУИЯЧЕФЭКОЛЧВОИОУКШФЯФИЮЩНШЛЖУИУЗБООМСОЪОФЯЪЩЕШЕПГЕТИНИОШЖК
ПЛЙБОФЗЧЯЛЪОЩВКЫЕШЕИЩВЙЯНИРНЛБСМХЕКТВФВЮЭВПЛЛЗПФВЖЪПХКЧШМХЮЮСНКЕ
БСАФННЩШРТЮННПЗИЗЯШЙКШКПЕДФМЧЯВЩВМЛУЭПТВЮЪВЙКБШЛИЖЧЫИСЕДЩЗХЗБВОЩ
ЕКНЧШЗОИВРЖКФМЧЯАЫЛТИВСКПИНЮЯЩЦНСЖЙДМСМХЛОФМХЮЮЧОЩЗКХМЪЭУСЯЪВПЫН
ЙЕБШЛРТЮННПЗЧШЮВЕКЩВЙИГШЛНЗКЩВТЦГНШТИАЯЙЩЦДЪЮХКБЩЮЪКЯСМЧЯОСНЦЯЮК

ЦМЖЮЭВИЯАЭПЙВКЭБВНЙСЖФЯЭЗИХЗНОВЩЯЙФЛЛЗКПЛЧИАЩЛКИУСИХЬБЦМЧЯАЧЛНВЗ
СЖМПОИЯЛЯМСЯФШЖШЛПЖМЪБПМБЧЙХЗНЩФТДКЧВИЕНИЕОЬБЭПФИБСЖФЯЭЧАХКНЫЛТИ
ВСКПЯКЮУУИБПЛМЯЛЯАТИБСРШЙКЦЛПЕГЩИЮМКЪПМРЛЪФЩЯОУОЮЛОФВПЬИСКПМНСЮМ
ЬКНДФЗКЭПГЙМФКЩЦАЪФГБНЧРНЯЙЩЛКИЮЪЕФЙКПЕИТБПЛОИОСФМЛООЛУВЗШНГВЮЩЛ
ЙЗНЦДТЗЖЪКМРЛЪФПМЪЮВИЛЮЪВЕАБЩЛЕСПРКВЯКНОЩИОСИГЛОООХЯАФКПЕДЩОФЯМУ
НВЬЙЪКПСОЪКШЬБЮВФЯИЪГММЙЭНОЕПГЕЩЦИЬЩПЬЙЪЯФЬЧЭИЪТЗШВФЙМЪОЩИЭСДЦКД
ЮЯХКЙЪЖОЛОСКЮВЮЪОЩВЭСДОМБХИПЬЧБЛЩЭКОЛЧИЖЪКЮНЮЭПЙИЮЧФЩИНЯБГЫБСОХЯ
АФКМЗЭЗИШЖКСЫФИКЩМХЬОЪНПЕУЮЛФЯДЩФМЫПРВЩЖКСЫНЯЙЪЫСДНЭЛКЕНФЙХВСЬЛЛ
ВОСИМГБХЕФЯЛЬЛЩВЮЯНМСДЧЙВЙКВИХЬЗФОГЭКЬФХВНЦНМЗЙЪЕЩДДШЛИКГЪЙЙЛБНШ
ТИИСГЛНЙШЕЧЯФСКХСБЬВОСНЯНЛЗДЦМЧВЙСОУЗБЫНХЙПЭЗЦИАЫЕШЗЙЗЖСКЖЯИСЖДЫ
РКСБОЕЦИГОИУЯЙЦКМЖП

2. Разложить на множители числа:

   (a) 112341201068620705168676457473 3

   (b) 624902917190196522926553833242761289569608844002242547879443

   (c) 11855786146877994318000704384554149707962682721811857502971844056771439470982286510076936 19

   (d) 150978852086077446606853353406293949727059001467042661107421150758262324612377528596210931849921349413518003872728617619 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 73966514629597747770006244356526982082909373669556337392613723490482327289967$
   - $e = 17$

   Сообщение:

   - $M = 37051871945437286915165632183587064059766188926272719215191032373672672196113$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 25172561905281663410488658591603363663 9$
   - $q = 17057732670777774534880908302684299647 1$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 33839318652093120018685056347938808933004647017071482903151166482288939190383$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 15686185551925137606394989814335043170 7$
   - $e = 3$

   Зашифрованное сообщение:

   - $c = 95578978445086436226814405478478901739$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 26158655906138225988192842971693858561 9$
   - $g = 56266704931890400314917345957171946491$
   - $y = 85196684236927597047511721986449505866$

   Секретный ключ:

   - $x = 15106301002818341845646051632469514129 9$

   Сообщение:

   - $M = 24402104080454622696770432039836450598 6$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 49746317246516659297092234073579097455$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 185420791535971987597097022053881849459$
- $g = 160510162366683184634958848630161647563$
- $y = 139594625443185438036574904008333089455$

Сообщение:

- $M = 260053170857393507802822820013388449 8$

Подпись:

- $a = 823258429627038179571817135288731825 16$
- $b = 673598183811777734556172647921171610 72$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 997$
- $g = 277$
- $y = 888$

Сообщение:

- $M = 241$

Использовать следующий случайный параметр для создания подписи:

- $k = 757$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 16x - 5$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 82

1. (a) Расшифровать текст:

ЖСХСЕЛОЛФЯЕКХЯТУЛДЮХЛИПСИЛШСДУЗСЕОССРЛФНУЛНСПДУСФЛОЛФЯРПИРЛПЛЖСП
ФХЬЛОЛФОСЫЗЛСЗЛРЛКРЛШТСЕЛЗЛПСПЦЖОЕРЮМСДЭЕЛОРПЪХССРФИМЪФТСЕИЗИХРФ
НЖСФЦЗУБРЫДХБЫНТУЛДЕЛОСРЕСОИРТУЛНКХЯФИМЪФОЛЕФТСЕИФЛХЯОЛЗСЙЗХЯФФЕ
ИХЦДСЙЛРИТУСХЛЕЛОФФЕИОЯЛЪТСФОИЗСЕОПСИПЦТУЛПИУЦЛНУЦОЯРЮИТСЕИОЛРФФ
ХСУЙИФХЕСППЮТИУИДУОЛФЯЪИУИКСЕУЖЛЕФХЦТЛОЛЕФОСДСЗЦЕСЕФИШЛКДШЖСУИОЛ
СЖРЛЫЦПЛНУЛНЛУКЗЕОЛФЯЕИКЗИРЦОЛЩИЕФХУИХЛОПРСЙИФХЕСРУСЗЦРСРЛНХСЕХИ
ПРСХИРФРИКПИХЛОЛРИЦКРОЕСПРИСУИРДЦУЖФНСЖССЧЛЩИУРФТУЛЕИОЛТУПСНЛКДИ
ФХСЕЫИМРЦЖОЦТИУИНУИФХНЦЕСУСХФХСОСРИФНСОЯНСЕЛРРЮШДСЪИНЛЗЕИТЦЫНЛЕС
ХЛЗЕСУИЩФНКОСЗЛРЛКПЦЙЛНСЕФИМЪФСДЕФЗСОСЙЛПСРЕСЫИОЕЛКДЦЕКЖОРЦОРФЕИ
ОЯЛЪФХУЛННУИФХЛОФЪЛХТУСФИДПСОЛХЕЦЗСЙЛЗОФЗСОЖСРНСРИЩПЦЙЛНЕСУСХЛОФ
ЛФНКОПРИФХЦТМРЫДХБЫНЕИОИОЕТЦФХЛХЯСЧЛЩИУЕСЫИОЕЛКДЦЛОЛЕСЗЕСУИЩННРК
ЮЕОЛИИПЦЙЛНЛСРСФЕИЬИРДЮОЗЕЦПФОЯРЮПЛФЕИЪПЛФХИРЮСНОИРЮДЮОЛКСОСХСБД
ЦПЖСБЕТУСЪИПОЕНЛФХСОУЦНСПСМРЛНРЕИУИЕСЪНИТСОСХИРЩИРЖЕСКЗИЦШЕХЕЦЖО
ЦЛЫЛУСНЛМЫИФХСНЦФХЕОИРРЮМЖСУЫНПЛЕФИДЮОСННЕСДЮНРСЕИРРСМЛКДИТЦЖЪИЕ
ФЛЗИОТСЗСДУКПЛЕНУФРСПНЧХРИЕЕЮФСНСМЫТНИЛЕЙРСТСЗДСЪФЯСНСОСРИЖСФХСО
СРИФНСОЯНСЛКЖОЕРЮШИЖСХСЕУЛЬИМФЕЛЗСПТУЛХЕСУРСЖСТСЗСДСФХУФХЛЕЛЗРСД
ЮОСЪХСЕИФХЯСТУЛДЮХЛЛСЧЛЩИУЛКСУИРДЦУЖТУСДЦЗЛОЕДЦРХСЕЬЛНШФЛОЯРСИОБ
ДСТЮХФХЕСЛЪХССРЛТУЛЖСХСЕЛОЛФЯЕФХУИХЛХЯПИРФХСУЙИФХЕСПТЦЖЪИЕЦКРОПИ
РФТИУЕСЖСЕКЖОЗЦТСЗЗИОЯРЕЙРСФХЯИЖСЕЗУЦЖЛФЪИКОЕЫИДОЖСУСЗЛИФНКОСРПР
ИФЙЛЕСФХЛБННТСЙЛЕИЫЯКЪИПХИДДСЖТУЛРИФСХЕИЪОЪХСИШОТСФЕСИПЦЗИОЦЛЪХС
ОБЗЛИЖСПИРСФХРСЕЛОЛТСННСПЦЗИОЦФТУСФЛОСРПИРРИКРОЪХССХЕИЪХЯТЦЖЪИЕТ
СОСЖЪХСРИШСЪЦСДЭФРХЯФТУЛФЕЛЗИХИОШСДУХЛОФНФЕСЛПХСЕУЛЬПЛЕИОИОЛПЕЮЗ
ХЛЕФИТСФОЦЫОЛФЯНУСПИЗЕ

(b) Расшифровать текст:

ЗФУМБГЩЙЙХАПЙКЪЗНАГЮЭПЙВФЗНКЮЭЪЭПЗЯЛЮТРГЛКЦХБИРХЙХЭКРЗХЬРХЮЬЮЛХЛ
ТМДМЭХЛЮТИВХОТЧЬЙЮВБТЖРЖЖГЫЖФМУЖЗТЯШЭПСЬАЗЙРЮЭИРФАШДДИЮЭХПЛЖЗЮПС
ФЩЭНЖФХАЖЖКЬМАЦМЬБПЧЛГГРЗЭУЗФТЫШДУУМБЛКЦХБЫЖТЙЮЬХЛМАБПЖЗИЮНОЗЬЖЗ
ЖБЧЪХИЮАЯДФМЪОГЧЕУМУЖБФЗОЫЙХАДЯРЩЖРТАСЗЩЙЖЭФОЫЛЮЛРОЗЫХПЧДЮЕЗСЫБЮ
ТИПХБУУМУДУХЕЭЮЙСРХЬРТЖТФУПДЬЗЗЗЗФЮПАТШГКТЪКЫКПРВЗКРЮХЛЖТЕХЖЖЙДЮ
РФТЛЪЗЗХИАЗУМДБЪЗХИЮГРНКВЫРРЕЫЮПАГЭЮСФБВЖРХЛМЗФЖЮЗДРСИЮЭДРЖХЪХРЬ
ГИТТРШЛЛЫЛЮКЗНРБИРПМЗБНХЛЫЮЗЫБВЛЮБЛЮЪЭПКХГТЙЛЭФЛУЙШГЙОЗТКЗРЗВЭЗП
ХЭФОСРЫХПМГЬЙЗХЛЮЫФАЕХЖЕИЮСФПМИЮИНХБЭЮОЙЭЫЮПСЗЮЛСФЫШЛЮУЗФГТЧДЮЕД
ОАЭХДХДХЭУЦЫХЖПЧЧЪЗОМКББАЧРАЮИИЮЭЖХВИЮЭЗПМЯМЕЫЮТЪХРЬЗМФАЖХЫЭУДША
ОТБЕЙХОЭХДФАЖХРЗЗЗБГЙПАГЙКСЭЮДЕРЗЩИРЖБЭЗДЦХБИТМГЧМДЙЙЮЛПТКЫМЧТЛТ
ЗКЩЭАМИЙКЪБЧУМВЮЪЙКВЫКЩКЯМЕЫЮТФООГЭБГЧЭМЭЖТСХДЖТИАЫКЦЮЫХУЦЫЭЗЗВК
МРФТЭХДРСЮСМЖЙЛШЕЗЦХЭБМОБЕИРХДХЭУЦЫШВКЫЛЮЛЭТИАЫЖЙСМКСЙЙХЭМТЕШКУМ
ЮЩЖЗЧЖЛЫЛМЗВИТЖДЩКУТЫХКФАЕЮЪЭПРШКФХМФЖЗЕЗЫКПТЕЛКНАЗВКТТРШЛЮРБЭМФ
ЧКЫЭМТЬЮКДМЭЭБОТЯХЛГЯЛМЖПЙКЪЗНАГЮЮЫЙЕХКШЙЫГКФФСЫЕЗСЛХДЗКГСФНЗЗВЗ
ДЛМАБПИЙГЯЗХГШКРРЖЮЧСФЗБЛКПКЬЮПУЗБЭКПБТЛЗПЮЦГХХЗЬЖРВКХДКИЫУМУФКБ
ЪНРБЭЬРПЗШИРЙОЫИРЕЗЫХЪТВФЗТТЬХЬНЖКГЭОМЙБГОТДТЕРФКЪЫРПЖЯЗУПЗТБШЕФ
ЫМДЙЙХЖЩЦЗТБПТЧТКЗРМСФНТКЬЗДТДМЖРЙЕЮЮРЦКГЛУЦЫШЮКЛЗАЮПЕМАЬНЙЬЪЗОТ
ЬЮИТЖЭВХУСЮЧЭПМРХКФЖЗЭЮФТДМГРСБЪЗЕИЖХЪЭПЗЧИТЙТХЖРСЗХТЗЖКХЕКХБЫЕК
ЕФЫЗРЕЗФЙЗРЗЬЗЕЕФВХРЕЫШЖЗСЫШАНМСЭЮЛЛИЫХЩМЫЮКФМЖХЫРХДГСПМБЭЗСФБВЮ
НАКЪБЗХЖЮСЗСБЬЗКХИГЬЩЙЫЛЕОТЬЫБГЯЛМЭРОАЭФОСЗЦЮУЦЫЮЕУЖБФЮФЙДХВКИЗЫ
ЯПЯЪЛДКОАВХУУЗЪЙЛСЮЩЕЗФЮТЮУАЕЯЗЖТААБФЙДМЖЭРБТЗДХЧФЗТТЬГЙЙРФИДН

2. Разложить на множители числа:

(a) 6336510246166698737038245930 83

(b) 5574729505217870965213438334954775994589880911393602153492 63

(c) 1412524463250949818533343659911441402276169130469834601158689398177129822958573782540623091

(d) 1335285521186596149928176041138915225875260790775747650238961241444987374126966733136593975462797122795138123164717901689

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 61273803860220089539453011685209475476446971968678199488094302800491769428757$
- $e = 17$

Сообщение:

- $M = 55628970487657208777676801395787339342704279337886200975603532341904723541457$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 315571819467987200707957217473509812063$
- $q = 26818482052234529562504974462581967910 7$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 562012253072780290185769122889107117662760120910674391357143572257775839522 94$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 211262461418472947176074927308151741899$
- $e = 17$

Зашифрованное сообщение:

- $c = 180058170942255150689150579119271593004$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 184350457270391774700972136851709422823$
- $g = 771701549705319722501623717486261984 37$
- $y = 95140433178258908666826236928850084 62$

Секретный ключ:

- $x = 31615560323291254869967092704736328017$

Сообщение:

- $M = 119421412210897047316737902046585314211$

Использовать следующий случайный параметр для создания подписи:

- $k = 15821689088986285640593481471328201 5837$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 31461310023476289419902446712297758 8749$
- $g = 61251571681166923054162362090889797843$
- $y = 15372447681764078177913279280237878 6212$

Сообщение:

- $M = 26126750159869611345904686418937583 8592$

Подпись:

- $a = 13330822722851846785965410355080996 6956$
- $b = 11083664385801642372581518976850493 0856$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 547$
- $g = 18$
- $y = 77$

Сообщение:

- $M = 18$

Использовать следующий случайный параметр для создания подписи:

- $k = 277$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 12x - 4$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 83

1. (a) Расшифровать текст:

ОТВЕЧЛЕМУНОЖИТЬУБИЙСТВОМИРЗБОЕМЗНЧИТПОМНЕКЛЕВТЬМЕРТВЕЧИНУПУГЧЕВП
ОСМОТРЕЛНМЕНСУДИВЛЕНИЕМИНИЧЕГОНЕОТВЕЧЛОБМЫЗМОЛЧЛИПОГРУЗСЬКЖДЫЙВС
ВОИРЗМЫШЛЕНИТТРИНЗТНУЛУНЫЛУЮПЕСНЮСВЕЛЬИЧДРЕМЛКЧЛСНОБЛУЧКЕКИБИТКЛ
ЕТЕЛПОГЛДКОМУЗИМНЕМУПУТИВДРУГУВИДЕЛДЕРЕВУШКУНКРУТОМБЕРЕГУИКСЧСТО
КОЛОМИСКОЛОКОЛЬНЕЙИЧЕРЕЗЧЕТВЕРТЬЧСВЪЕХЛИМЫВБЕЛОГОРСКУЮКРЕПОСТЬГЛ
ВСИРОТККУНШЕЙУБЛОНКИНИВЕРХУШКИНЕТНИОТРОСТОЧЕККУНШЕЙУКНГИНЮШКИНИ
ОТЦНЕТУНИМТЕРИСНРДИТЬТОЕЕНЕКОМУБЛГОСЛОВИТЬТОЕЕНЕКОМУСВДЕБНПЕСНКИ
БИТКПОДЪЕХЛККРЫЛЬЦУКОМЕНДНТСКОГОДОМНРОДУЗНЛКОЛОКОЛЬЧИКПУГЧЕВИТОЛ
ПОЮБЕЖЛЗНМИШВБРИНВСТРЕТИЛСМОЗВНЦНКРЫЛЬЦЕОНБЫЛОДЕТКЗКОМИОТРСТИЛСЕ
БЕБОРОДУИЗМЕННИКПОМОГПУГЧЕВУВЫЛЕЗТЬИЗКИБИТКИВПОДЛЫХВЫРЖЕНИХИЗЪВЛ
СВОЮРДОСТЬИУСЕРДИЕУВИДМЕНОНСМУТИЛСНОВСКОРЕОПРВИЛСПРОТНУЛМНЕРУКУГ
ОВОРИТЫНШДВНОБЫТКОТВОРОТИЛСОТНЕГОИНИЧЕГОНЕОТВЕЧЛСЕРДЦЕМОЕЗНЫЛОКО
ГДОЧУТИЛИСЬМЫВДВНОЗНКОМОЙКОМНТЕГДЕНСТЕНЕВИСЕЛЕЩЕДИПЛОМПОКОЙНОГОК

ОМЕНДНТККПЕЧЛЬНЭПИТФИПРОШЕДШЕМУВРЕМЕНИПУГЧЕВСЕЛНТОМДИВНЕНКОТОРОМ
БЫВЛОДРЕМЛИВНКУЗМИЧУСЫПЛЕННЫЙВОРЧНИЕМСВОЕЙСУПРУГИШВБРИНСМПОДНЕСЕ
МУВОДКИПУГЧЕВВЫПИЛРЮМКУИСКЗЛЕМУУКЗВНМЕНПОПОТЧУЙИЕГОБЛГОРОДИЕШВБР
ИНПОДОШЕЛКОМНЕССВОИМПОДНОСОМНОВТОРИЧНООТНЕГООТВОРОТИЛСОНКЗЛССМНЕ
СВОЙПРИОБЫКНОВЕННОЙСВОЕЙСМЕТЛИВОСТИОНКОНЕЧНОДОГДЛСЧТОПУГЧЕВБЫЛИМ
НЕДОВОЛЕНОНТРУСИЛПЕРЕДНИМНМЕНПОГЛДЫВЛСНЕДОВЕРЧИВОСТИЮПУГЧЕВОСВЕД
ОМИЛСОСОСТОНИИКРЕПОСТИОСЛУХХПРО

(b) Расшифровать текст:

ЛВЧГЦЛЪЬГЖЩЯЧЛЪРЫЭПЭПЩЦОСЕУЧМЧКДМЖЩВЬОКИОЩОГЧХДИЛЖЗЭПЗЯВАЪМЗЕУЭН
БПЮТИБННТАВЛУЧПЪИЮООИАЯЦИГКЗППЯЙЦУИЭБЭЩОЭОГХЪВЛЮЧГЪОЭШРЕВЬЦОСЕУЧ
МЧКВШПЧЛЦУПЗЛБШЛРЮБШПЭЯЮППЯЛЬЖИГЗЯЫАЪКЮЕУЧДФХВГЯДЫНЪИБЫПБЛГЪГЗЩЦ
ППВЛФОМШЛЬШАРЛЮЛЩАЯТПЙГЙДЬОЪКЮПКДИГЖГЧКЯБЛГЙИПНЛВЩМВИХЦНОЪЖЫПГЮЗ
ШХМЖЩЬПРЖЛБШИАЕЗШГЪМЯХЛГВЩЪСБКЯПАРНЧХМЧГЮШПЗЩЩЫНГЗЯУПЗЯЩПБГИДЛЩЪ
АЬСЖАВФФСАШТФЖБВЬТНЕВЬППЗЩЮПЖЬЧВЧЖБРПОКДВБМНЪНЦЪААЙЯХХВЕЦМЩЧВБЧМ
ВВШОГНКЩППЯДЬШЛЗЛИЧМЗЗВМХЪНГШЙСЗЯЩОЭВЖХЖЬМБШАЭКЗТЖЧШАЪЖЪТЬТПЧХЩЦ
ЖЕЛХЧЩБЕЮТИЯКЦЬПДНЩПУАЛХЧМЩКЮШАРПЫПЧЪЙЯХМЩШДЦГВКЦЬЛЭЛГАЛЭЙГПОЭЯМ
СВЪОНФМВВИЧМДЛЫФЖБКЩЛСЩЩХПЙБПЯБЛГПЫЫНЕЕЦЯЙДЛХЬЪДНЯЫЪЦРФШПИББЕЛЪЯ
МЫЖЕЛГМГЕЛГЧМЧШЧХСЪПЦЫЪВКЦЫНЕЯЦОЙЭЯЯЫРСЕЯЛЖЩРЮТИЯКЦЬПДНЩПУАМБШПЭ
ПНЦЖАЛВЬЖВВАЪАГОДОЖДЛШММАЩГППДНЯЫЖЗЩЫЬМЧШГФМЧШХШХСЗАТРВЙЩЪМВЛУФН
ЭПЮЦЖЕЛЮШАЗЛФШПБЛФШХЗЛТЕЙЯЛЭПЛЩКГШКЧЛХЧМЮЕШШОЪКТЭОШОЫТУЯНЦЩМЖПЦУ
РГФЮШРЯОХЦИЬИЯЫЪЦШЬЬОГКДЬЖЬЯЩЧЖЗВЭПЛЖЗШХМВАЯХМЖЛЭПЧЪЮЯХГЪИВФМЧШЭ
ППАЕУЦГНЕУИПСЯУВЖЩВЬЧМЦШУИНЕЕХММЕВЩСШЖКЩЬГБКЦМХЪЙВШПЗЛЩЬАНМБШПСЮ
ЩЦМЫВГЛЩЗЩЭЧГИБВЬПЧЙАШКГФНЦОСЕУЧМЧКУЫРАЕАШХЗЕГПЙСКЯПГЦИФШВЕЕЬМПЪ
ЯЮПЖЬЯЦЫРВЛЪОКЪКЦММАЩЮШНЕЕУХГЯИЯЫГЕБЗПЖЧКДВЙГБЯМГЕВЮЧМЖПНЦОСЕУЧМ
ЧКУЕЛИИЩСИЕЙЮЫЙГГЦЧЛИЫТЭКШРЩЩМЩИЦПЛЪДЮФМБЛЪЫАГВЪЩМЯНЯМЖЗВЬЖЛЭУЦФ
МЗЛБЫРАФЩЬРСВЦЩОГОЦЛПВФЬШЛМЕГХПЧЕХШКЧКЩЦРЪИНЧЩБЕТХБГОЫХМВКМЦЛГЯХ
ЪСШИЩАМЪВАПОЪЙЦЧЖАЛВЖЖБННТАВЛУЧПАВХШАЧХФХЕБЕШМПЪЙЩПГЩЯЩРГВЕЭТЖЖМ
ДНЙЖЩВЬОГАЯЦСЧШБРГВЕПЗРГАЯХЖЛДЭТЛИПДЫРГИНЩОЭПЮШКИЕВЩМЯЛЪЧМБРУЕНЕ
ЛВТРЪДФЪЖВВУЫИЬИХЦПКЛЬШВВШЭМЖЩЛЭТКДВБЬОЭУЮПКГГЦЬГШЛАЪМЖПЩЬЪГКАЪ

2. Разложить на множители числа:

(a) 1031575863449114821058117738887

(b) 107219281678038762381025250154553972411301418870999137927987

(c) 1066003252867053484339069449203950687710167113998584787288270913823013155788855613104900991

(d) 894061699505112111312430552574397123511577646639363870257136753039029285397880792122241571246057593580225544698718738959

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 57877036004322147704413858886922578521037417708934618657559311498502608966541$
- $e = 3$

Сообщение:

- $M = 52575134972239569696669587620494805753372260663185239413091095186012091415119$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 331594041373352543859860440094627857981$
- $q = 28151168709478351917520825174483673009 3$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 88894862719289685326851375316052129913624488403688578453124421179661949822132$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 217178202288199464637181328178600084559$
- $e = 5$

Зашифрованное сообщение:

- $c = 127452000419289028109172450903413033044$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 289598693761836853947265847695637986867$
   - $g = 153566657242208566224153218668396886913$
   - $y = 277355753526367337893723762397993059666$

   Секретный ключ:
   - $x = 207699569390515661733771217073471547387$

   Сообщение:
   - $M = 205732522169210722534577274068491995105$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 800166544645870175948146689701395446 17$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 271081130440164309641219057638028618081$
   - $g = 195033173301643323091751010281344907813$
   - $y = 771412168167319813282387838874394091 47$

   Сообщение:
   - $M = 249086431224514277513539743003389251216$

   Подпись:
   - $a = 184947436803009066758539785631520675967$
   - $b = 214908385354984197675735447833919440488$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 619$
   - $g = 585$
   - $y = 349$

   Сообщение:
   - $M = 360$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 301$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 2x - 16$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 84

1. (a) Расшифровать текст:

ЪДЩЬВЪЙЭФУЧКЧЯГДФЧЦВЩФЧАЯГЕЮГАКЧЭЯЧЮАХЕЩЯДОФКЧУЭХАВАЦЪЧАДФЧЙЭФЗЮ
ЪГДВДАЭОЬАЧХАФНГАЬАУЭХАВАЦЪЧБВЪЬЩЭФКЧУЭХАВАЦЪЧАДФЧГДЪФАГДВАХЧЧУЭ
ХАВАЦЪЧБВЪЬЩЯАБВЪФЧГДЪЬЧХАФНГАЬАУЭХАВАЦЪРФКЧУЭХАВАЦЪЧУВАГЪЭГЯЬВН
ЭОИАЬВЕЭОЯНЧЯЧЦЕЮЭЪЮЧЯЕЦЧВШЪФДОЪББВЮАФУЧШЭФЬАЮЯДЕХЦЧЙЧЭАФЧЬКЧГДОХ
ЕГВГЬЪЗАЖЪИЧВАФЪХВЭЪФУЯЬЮЪАВЮЧДЭЬЬАФАУНЭАЮАЧЪЩЕЮЭЧЯЪЧЬАХЦФЩХЭЯЕФ

ЯЯЧХАЕЩЯЭЪФЯЪФЯАФЪЙЩЕВЪЯЯЧЬАХЦАУНХВФКЧХАЮЧЯФГЪЮУЪВГЬАЮДВЬДЪВЧФАЩ
ЮАШЯАЭЪФГЬВЪЙЭЪФЯЪФЯНЙДНЭЪУУУБЧДВЯЦВЧЪЙЬЬЪЮЪГЕЦОУЮЪАДЬЕЦДНЩЦАВАФ
АУВДЯЧЗАЙЧКОЭЪБАГДФЪДОЬВДАЙЬЕУЭХАЦВЧЯБВЪЬШЪЬЭЕЙКЧАДФЧГДЪЮЯЧЬФВДЪ
ВЕЬЬЕРДЧУЧЬФВДЪВЕАГДФЫГЕЮЧЯЯЧЮАХЕЯЧАЦЪЯЯЕБАЦФЫГРЦЪДАФВЪЛЯЧГДАФВЪ
ЛЧЮГЦЮАРГЦЮАРХЦЧШЧДНЧЧБАЦИЧБЪЭПХЧУВДБВЪГЪЗГЭАФЗЩЕВЪЯЩГФЪГДЧЭДЬФН
ВЩЪДЧЭОЯАЙДАФГЧЩЗАЗАДЭЪГАФЧВКЧЯЯАГЮЕДЪЭГЯЕБВАЦАЭШЭЩЕВЪЯДЬЪУНДОУЕ
ЦЧДДЧУЧЬФВДЪВШЭОЮНУНБАБЪВАФЭЪБАГДВЪЯЯАЮЕХЧЫЮЭАЫЦЙДАШГРЦЯЧФЧЦЕДЬЕ
ЮЕКЬЕДАБЕХЙЧФЪЭЪАЯЕБВЮЪДГГЬЩДОЧЫЙДАУАЯЯЧУАЭГОУВЪЯЦЧБВЧЬВГЯНЫЯЪЙЧ
ЮЯЧАУЪЦЪДЦЗАВАКЧЯОЬАЧЧФКЧРЙДАДНПДАГЬЩЭЩЕВЪЯЕЬЬЬЕЮЕКЬБЕХЙЧФПДАЦАЙ
ОБАЬАЫЯАХАЬБЪДЯЮЪВАЯАФФНФЧЩЧЧЪЩБЭЧЯЪДЧБЧВОБВАФАШРЦАЦЧВЧФЯЪУДРКЬЪ
ЯАЫХЦЧЪАГДФЭРЧЧЬЬДЬПДААДЧУЧЮЯЧГЧЫЙГЦАЬЭЦНФЭЪБАЮЪЭЕЫЙДАШПДАЩЯЙЪДБ
АГЭЧФГЧВГГЬШЕДЧБЧВОВЦЪУАХЕГБАЬАЫУЧЦЯЕРЦЧФЕКЬЕЬАДАВЕРХЕГВНДФАЪБЧВ
ЧБЕХЭЪЩЕВЪЯДАДЙГВГБАВЦЪЭГАЯГЮФНКЧЭЯЕЭЬИЕЪЩФЪЯДОГБЧВЧЦЮВОЧЫЪФЯАФЯ
АЫФЯЧФАЭОЯАЮЯЧЦАВЩЕЮЧЯЪЪЪБВЬЬЩЭФЗЮЪГДВЕАДФЧГДЪЧЫЭЕЙКЕРЬФВДЪВЕФХА
ВАЦЧАГДЭГЯАЙЧФДОЕЯЧХАЮНАДЕШЪЯЭЪЪЬАХЦАГДЭЪГОФЦФАЧЮВГГЬЩЭЧЮЕГФАЪБА
ЗАШЦЧЯЪЩЕВЪЯГЭЕКЭЮЧЯГУАЭОКЪЮФЯЪЮЯЪЧЮЬАХЦЬАЯЙЪЭ

(b) Расшифровать текст:
МОПЛХТЬМАЫЦЛЧЩАЦВЧВЪЦЫТЛЮСЦЩЙФРФХЧЭАНЙЛХКЦРФШТЬИЛШУШТЖЮАНРГЗНЩЙВ
ЗНЫЖААЪЕЫМТВОЩЖТЙЩХЕЮСНТЗЭЭЧИГЫЩЦИЛГЛЧРЕЮХЯЙМХУФТУФРХЫЖШЩЕЖЙТНЪА
ЯГЭЛИЛГЛШТМХШОИГГУСЪЦЬБСОИЗУСЩОФНЩКГТЪЕЫНЮЪУТАБЧЩТМШУЪСАВНЩУАЭРО
РВБЪЛЕЛШХЧЦЭХЯФРФШТЪЦЛГМЧРЙБЪЦТЭАПГФАЭХДЩМТЦСЩЕЮХОНЭБФЧРЯХУОЧЭШМ
ОПЛЮЛЫООШТЩЧЖМХЧЗЙБМЬЕГЭЦЗРОЦРУУЙФЦБЙЖЪЦХСАШЩЦПУЫЧЬХКААСЖКИЧЧФНГ
ЯЫТШВЦРСТШЪЪУЛЮЩСПАУЦРЫАЬПНЙММШЧЗНЪТЧЗЙВГУФОЫРБАЯЬГКЦЩИТКЧИВЫОРЙ
ВКОЦГЫЦЦУЙЗНЪЯЭБДМИАТАСЗЙБЧЧИМЯШЧХГЫЩЪЙЛФНАСЦЬПХМЛЭРОРЮЮЩШТЯВЦЦЬ
ГУМОУЙТЪЧФГЫФЬКГЪЛЧХКЮМЦЬГТЭФЙЬЭЦХСЬАНУОЭЭЙЩЙЯЭМЩВРЧНХХЕШСШТМФРФ
ЖГИДСЩЭЪЦФТЯЪРСЩЙЗНЫЖАЧЪСОЬВЖБОАУЦЪЧЯАЖКТБХФЧНЙВКЧФТШКТИОАТЩТЮВТ
ЬЫНЮООЦЦЧНЛЙУМТЩЧЖМХДНЗХМФМЖТГЪОЙЗРФМВВНФЙЮШЪЩЙМЭЫФЙЮЮКССЙТЪЛЧРЮ
РЪРЙВЦНЖГЭЫФФЙУЪУЧЗГОСОЗЮСМПЯХУЦРАЭЩМПОЯГХСАФЦЬРАЭРОРМХУЧУНМКЫЙЖ
ХЛЬМЭХУОПМЪТЫАЕСШЪОЙЬЫНТЗГЭФЙЬЭГТСЬАХЮТЯШУЪСЯТЦЩЙОЧЧОФНЛЭНЖААНТХ
НЮУСИЭЬЫПМЕВТПЙМФЫКМИЬРЫЙЖХЛЧХНЭЦЛМЖБДШФЗЮЧОФАФХСРГТГЪОЙЗРФМЬАЦЪ
МЖБЧЩРЙЭХСЩЙВКЧФДВННЖААРЪОВЫРХЖААЦЫСЙТРНРЙЩЙДПМВШБЙИЯЦУФДЭНТРААН
ЧЕОСНППГСШЧХГТМЬЕГЭГШТКЛЪФХМСРЫАВЬЦУИЭХШСЖЦЫЦХЦЧЭЦНЖААРКЯЖШМЬЕЙТ
ГОТЮАЦХСЦЩПХТЕЭНЪТЕАЫБМЗТЕЫЧЗШХЬЦОБЪЫСЦЩФЧПЙФЦТРОЦРУЖЦИНФМВЫЖНХЕ
ЮССЛЬЛРЪЖГФЦХСЯЬНЦСЦЬЩШФЙБРФРАЭТУХЗХЖКЧИШЪЕЗЯХХНФЩИТРЙЗБТСНВЪШСЫ
ЖХФЬОЖШТЦЧНМНМТЕЮФЦЙМЬХНФАЩЬЦХЧХКСЫИХХНФЩИТЧЦЭХЯФТИЬХОЗЙАМЧУЙФЙЧ
ЫММЯОЗЙЭМЧЕИЮКХЙМВЦЧЦЭХЪЪЩЭВРФЙЮЮПЛТЛЮЪСУЛШЪВМЭЪМЛЙЛЬХКФЭХУОПГЕЦ
ЫУГАЪЕЛАЬЩУМДСГФТВГЧЩРГЫЩЦТЙВНАЙМЪЦОСЕЧХСЙКЮМОНМВКЧЖЖЮРЦСАУЦЧСЭЛ
ХЬПЕЫЖАМЙВЧОФИСШУМИГУЪЫААНРУЙАЦММЭВНХСЙЬЫМПОБУКТЙБКОЭАЭХЧРОЧТСРЙ
ВКО

2. Разложить на множители числа:

(a) 68254562278577334083596845247 7

(b) 59863544872809889564049258635173248507445405350061828140514 7

(c) 13778021437510509742053484581318880899536381147753782867081353825737141103367814306039490 47

(d) 10005336311993390227952273496779345040804849498032157790079441465076561458247299223335156064310927117133939012304642763 03

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 486043230268006556614380952119788504219946430635673639157851398050489553391 49$
- $e = 5$

Сообщение:

- $M = 17059766110997375964645651248423868911755644552462797525150955424081644625000$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 276581759244162242597534544528698142083$
- $q = 185172167901965027576832767338148662961$

Открытая экспонента:

- $e = 3$

Зашифрованное сообщение:

- $c = 3106211150006424563881444423023045456953987726876583661815599790829623077236$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 145875382621983386738874461366121308177$
- $e = 17$

Зашифрованное сообщение:

- $c = 111070553480133953392558029708443865012$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 29270146734374979808005991238983211536 7$
- $g = 18112841302397950103126042145385023890$
- $y = 14393743808703323410210180226150163 6947$

Секретный ключ:

- $x = 27612173283254417496869902441321656583 6$

Сообщение:

- $M = 14296217811122534807088701789040165266 3$

Использовать следующий случайный параметр для создания подписи:

- $k = 68082824643083900473824469144946792781$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 28346575866809270815623035480748648108 1$
- $g = 26067951937764182730344688959968598387 4$
- $y = 27127793260748819171308950393948266196 8$

Сообщение:

- $M = 22792497160109848592664903905505039560 5$

Подпись:

- $a = 16928945123533782768044959706870623821 6$
- $b = 87764382263438330855811856871545640947$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 941$
- $g = 857$
- $y = 519$

Сообщение:

- $M = 288$

Использовать следующий случайный параметр для создания подписи:

- $k = 3$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 15$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 85

1. (a) Расшифровать текст:

ТОНРЩТШНХХЦТТРКЩНЧШЦЯННХЦКМШЫЛЧЦЯЫКЩЪКЦКУХНЧШНЦМЦУРФЦНЦЪКШБНХРНФ
ХНЧШРАУЦКЛЦУЦКЫЯЪЦНЩУРХПКЫННЪЦТЦФРЩЩРЧЦЪШНЙЫНЪННТЦЪКНЪЫРФГЩУДКЧЫ
ЪЪДРФННФНОМЫЛХЫЩХГФРРПКНЪФРПУЦМННКРННЩФЫЖЧШРКНЩЪРХЦЯХЫЖЩХРФРЩЪКТ
ЫЕЪЫОЩХФГЩУДЪТФНХЧЦШПРУЯЪЦПФУЩРЩЧЫЪУЩЩЫМДРФЦРХЯРХКАРНТПУЦЩДКГЩУЫ
АРКЪДЦЪКНЪГФЦРЩХНТЦЪЦШЦЖЙУЛЦЩТУЦХХЦЩЪРЖЙГУРЩХЦКЧШНМЫЙНОМНХГЧШЦЪР
КЫФНХЧШРКРМНФЦНЛЦЩФЫБНХРЛКШМНСЩТРСЦЬРЮНШЧЦЪШНЙЦКУЯЪЦЙФНХЧЦЩЪКРУР
ХЦЯХЫЖЩЪКТЫЩЛУКХГФМЦХЦЩРЪНУНФЛНХНШУКНУНУТУРТХЫЪДКЯНШАХНЛЦПУЦМНЩО
РКЦЩЪРЖЦЙШЪРУЩТМКНШФЦОРМЧЦКУНХРЩКЦНЛЦЦЙКРХРЪНУЯНШНПХНЩТЦУДТЦФРХЫ
ЪПЛШНФНУРЮНЧРМКНШРЦЪКЦШРУРЩДРКЦАНУАКЙШРХРПЫФРУЩНЛЦЧНШНФНХНЦХЙГУЫ
ОЩХЦЭЫМРЙУНМНХКЦУЦЩНЛЦХНМКХЦЯНШХГНТТЩФЦУДЩЦКНШАНХХЦЧЦЩНМНУРМУРХХ
ЙЦШЦМЙГУКЩТУЦТЦЯНХЦХЧЦКЪЦШРУЦЙКРХНХРЩКЦРЩУЙГФХЦЩФНУГФЛЦУЦЩЦФЧЦНЛ
ЦЩУЦКФЦЪШОНХЙГУЦЪЧЫЛЯНККЦШНХЙЫШЛАЧРЦХЦФНОНМХНКХЦКГНПОУХЧНШНЩЪШНУ
ТРМЙГЧНШНМКЪДЧРЩДФНХХГНРПКНЩЪРЦКЩНФЯЪЦМНУУЦЩДКЛЦШЦМНЯЪЦХТЦХНЮКХЦ
ЧНШНМУЩЩФЦПКХЮЫШПВНПОУЩХРФРПТШНЧЦЩЪРКТШНЧЦЩЪДЩЪШЩДКЩЯНЩТРЛЫЙРЪДЩ
КЦРЭЪЦКШРБНСРПФНХХРТЦКМЙГПХРФЪДРЭФНЩЪРЧЦУДПЦКЪДЩХЛШМФРШПМКНФГФРЦ
ЪЩФЦПКХЮКГЩУЫАУНЛЦФЦУЯРЙГУМЦКЦУНХЦМХРФРФФШДРРКХЦКХГХНЙГУЦЧШЦРПХН
ЩНХЦЛХЫЩХГФПУЦМННФЦЪЪЦЛЦУРЯЪЦЩФЦУЖЙРННЛЦЩЪШМУЦЧШРФГЩУРЦЪЦСТЦЪЦШЦ
ЪКНШЛУНЛЦЩЧШНПШНХРНФЦЪЪЦЛЦУРЯЪЦКЩНШМЮННЛЦЪРУЩДРЩТШЪЦЛЦОНЯЫКЩЪКТЦ
ЪЦШЦНРФНХПЩЪКУУЦФЦУЯЪДТТЙГЪЦХРЙГУЦРФМЦЯНШРЙНУЦЛЦШЩТЦЛЦТЦФНХМХЪХН
ЙГУЦЧШЦРПХНЩНХЦКЧШРЩЫЪЩЪКРРТЦФРЩЩРРЫЪКНШМРУЩНБНЙЦУННКФЦНФХФНШНХР
РРТЦЛМЩЫМДРЩЧШЦЩРУРЯНФФЦЛЫЦЧШЦКНШЛХЫЪДЧЦТПХРАКЙШРХЦЪКНЯУЯЪЦМНШОЫ
ЩДЧНШКЦЛЦЩКЦНЛЦЦЙВЩХНХРРХРЯНЛЦМШЫЛЦЛЦКЦЧШКМХРНЩНЙНЩТПЪДХНФЦЛЫЛНХ
НШУКНУНУХЩКГЌКНЩЪРФГКГАУРКФНЩЪНЩЧЦТЦСХЦКПЛУХЫУХАКЙШРХХЦХНЩТПУНФЫХ
РЩУЦКЦХЫ

(b) Расшифровать текст:

УЕДЭАОГДЬЖУЪЛЮБУЗБЖВПИМЮЗРКНЭЗТЭЧЮГМБНБДТГГБКЗАЛБЗРЗНЬЬЪВДЕЛРЦЪГ
ЕРЧДЖААДНГГРВЗДЙКББЖЖЕЭОЙЖУЭФЪГЕГРДЖДЪМБЕГЕЙКДТСДВАДВНЫЕРЮРЛИКЯЗ
ЕЭПДНЭЕНЭЗЫИЖГРЛЕЭКРДЭЙКЗАТДЭКБЙДГДКЖЕАРБЭСЕЗЫЭНЯМБДОЕЫЧАДВНЫЕХЦ
КЮЬПИЭБКТЪОЮСХОТЧЕУЦКЬЖУАНЫАНЭЦЛЖЩИБККДГБДКРШНЖЭУЗММЖСЭРФЪФСЙЛЖГ
РБДЪОГДЕЗРАНЯЭПЭЗЛЖФЭАЮЯФГВЗДЗВОЗБОЪСГКРВДЪУДАНЛЖОЗНДФМГЛЗЫХДНЯГ
ЗЗЫБЙРЧДЛЖДЗЫИЖМЪШЮЪТЪЛЖЭХНКЗЪНУАБКЮЖЗИЖНИЦБКЮГСЙЖЖЭСЮГЗЮАДЫРЖКЗ
ЪЗВЗЮЕЖЕТЬЖЛЩДЖФСГКГЙРЦПДЙЕЕЗЖЭДЕРИИРЖСБГУЖМСАОЖДЕЭЛЖСЫЖОЧРЮДЭЦЪ
ДАХЧДЙЭПРЦЛЖДГДЖЕЭЪГЮБУЗББЙМГПЗЩХЩТЛЗТЪЙЙСЗВЪРЭТЬЖЕЭУЛМЭЭНЖАФКЮЖ
ТИИХШНЕДТСЗЫЕРЧМИИРОРХЙРБМЗЦСГХДЖДАЛЮЕСЕЗЫЙЗКРЮГДЪПХНРБРЫЭНСЗРЖС
ЗЫАДПГЭИЖУАДЭЖДАЗИЖНЯТСЭНЩНДЫРЖЛЗКТЪКБЯЖАЗЖЙЗАЫКВКЮГЗДРДСХДПГЭИЖ
МЭГЮДЭЮЛЙППГДИИЗЩЦМЪУЗББЭФЕДЫЖИЭКЗДЗВЙЛЖФГЛЖЭЪЪОЛГЩЗНЖЭДЖДЖЭУМРЛ
АЖАЛЮЕОЭМЗЪНЭРХЙЗЕГПЭЩИКЗЕРЧТЧЩХЕЭЖЭУЗММЖСЭРФЪФСМСЭЕГОЗНРЩЗЗВРВЦ
ЖАСИВРЭДЖЙЗБДГИЖУОРОЙЖЧГГБГКМДЙЭЙЖДДЭПЭПАЖТЪМЖУЗДТЬПЗЧЪЕАСГМЮЪРА
ДЗКГЭПДАХЦДЭЕЭКЕБКЗАДВКРМСЗЖУЗБДЭПГАФГРЭЛЙЯГГИЖАМБЗЗЕКВДАЕНЭЙЗДХ
ДНЫАПГБЛФУДПЫГЗВЗЮЩЭАНЫЙАЩТИИЗЯПТЭПГОЗДЗОЗГАХЯПФЪНЭРХЗРАДКДЪЮЙБИ
ЙЦНВЕКЯНЫЯНГГЮБУЗБЗЪНЭОЗЪУУГМЕЩАЫЖАМЭНЛЬЗАЫЖУЧГСЙЬРЧОЗЙНВМФНДДНЬ
ЖПУЖИЛЕМДЫУОЗНЬЬХЫДЪЭЕИШБДМЖСЙНПЭРЕЖДАРЛЕРВЙАУДАЗЫАПГБЛУЧЭАЮЯДЭМ
ЖУЧЖНККРВЗЮЪУЪВЗВТШГЮЙДЭПЮЗУЗБЗЪНДНЯИГРКЗЛИЖМЗЕЗДПБЪЗЩЗЪЖЕЧЗЭЭФС
ПМЙУЯЗВЩХВСЪЭУЖЛФЙНЪМЖУЛЭАЮЙСГШЭЕЭЮСЮВРЗНЙУЗЬЛФРНУСМЕУВДЫЖЙБНЯЕЭ
ЪОЮИЗЧНЙЖФРЗДАОГКЗЬЭЭМЮЯПУСЖРЗШНЖИРЩЗДАХЫКЧЬКЫДККРЯНКЭТЩЪЮВРЭЛРЛ
ИШНДЖДИЧГЗРАТСВЖЭРЫЖЪЪИГВРДДВВСИВРЭДЦДЯГСЕДКГЗЩТЮДЭЮЗЫАДБЗОЭНСРЗ
ЕРББКВРЕДМЯПАЗЕУРЖНЫЭТНДЖЕРБДЬЖТЬАБККЭМГЖПЪХЬИКВДЫЗРАТРАНГСКЪРЪВ
ЗЫЗВДЙГКЬБЮЙФЭДЗЗРЭЛГЭУБНАЪПЛБЕЭУЗДБЗРЧДДЭПЭДЗЙФВНЫАФСРЖВР

2. Разложить на множители числа:

(a) 1024676276179532326449693228931

(b) 1169878497660830343570838788859577025705196039466078424089291

(c) 109607148889109169230876799381952647754859233165077859011685149845764191419933716966350289 9

(d) 842575919894898217516463974141250660405619088531803585091556515067979547512970985051888010935243731331142706950593506069

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 946158437885775962843389566897521814359023508153581757316465082122121376819 69$
   - $e = 5$

   Сообщение:
   - $M = 412345753432402321264633495667670722747294193651636021889045526040879992872 95$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 24429167828927425654390111891468218013 9$
   - $q = 19777481793011768055165253113358413329 9$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 11868613774618370184735902500233076447111646595140980707550873449150487816719$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 19654140912424006502750114203230651857 9$
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 15266983420768965046965066788732762832 3$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 25827438686999332027844556952011470080 7$
   - $g = 82395916497468208271380408058672671863$
   - $y = 17812916326622293954625762296573096828 7$

   Секретный ключ:
   - $x = 54974676227707200201678679951046129681$

   Сообщение:
   - $M = 55753131270379806307503897151438671 0$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 16154322519708228691699422806959529754 9$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 18333041028201169509020106663689623588 1$
   - $g = 77975697243193436458074753417690955893$
   - $y = 26038283262163722307878149251343681394$

   Сообщение:
   - $M = 17037568095149847081407172060029865055 5$

   Подпись:
   - $a = 37634788429855884034147993592131094037$
   - $b = 16549767551252201358269793927174226671 6$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 541$

- $g = 443$
- $y = 365$

Сообщение:

- $M = 342$

Использовать следующий случайный параметр для создания подписи:

- $k = 281$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 13$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 86

1. (a) Расшифровать текст:

ЭФАХХТШЗЦХЭШЫБЭЬАМХШТЭЮТЭХЯЮВЮЬБВТЮШЕСЫУЮФХЭБВТГХВТБШЬСШАБЪЮЩУГС
ХАЭШШТВАШФЖВШТХАБВЕЮВЭЕЮФШВББХЫЮЯАШЭФЫХЦЙХХФХБВХАЛЬЯЮЬХЙШЪЬТЮФЭЮ
ЬШЧСАБЪШЕДЫШУХЫХЩЯЮЪЧЛТОВБЮСБВТХЭЭЮАГЗЭЮХЯШБМЬЮХЪВХАШЭЛЧБВХЪЫЮЬШ
ТАЬЪХЮЭЮЯШБЭЮЪЮВЖГЯХВАЭФАХХТШЗШБЮФХАЦШВЮЯАТФЭШХХУЮБЛЭШЯЮЕТЫЛГЬГШ
БХАФЖГФЮЗХАШЪЯШВЭЬШАЮЭЮТАГЪЮЯШБМЯХВАЭФАХХТШЗУАШЭХТФЮБВТЫХЭСЛЫЭЬЮ
ВЮФЭЮУЮШЧХУЮТЭГЪЮТЪЮВЮАЛЩГЧЭЫЗВЮЬЛЧЭВЛСЛЫШВАГФЮЬЮВЭЮБЙШЬБЪЮТАХЬХ
ЭЬЮЯШБЭЭЛЬХУЮФХФЮЬЬЛАХИШЫШБМБАЧАХИХЭШАЮФБВТХЭЭШЪЮТШЧФВМХХЮБЮСЮЯА
ШШБЪТЪЪЦФЮЩУЫТХЯАШЫШЗЭЛЩНЯШУАДШФЮЧТЮЫШТБХСХЯХАХЬХЭШВМЭХЪЮВЮАЛХБЮ
СБВТХЭЭЛХШЬХЭШЧФВХЫМЮЪВБЭЮБЪТАГЪЮЯШБШСЛЫЮТФАГУБВАЭЭЬЛБЫМЬХЫМЪЭГЫ
ТУЮЫЮТХЬЮХЩБЭЮБЪФЫХХТАГЪЮЯШБШСЛЫЮЭГБТХЫМШЗБЪЧЫХЬГЮВФЩЦХЬЭХВХЯХАМ
ЯЮЫЮТШЭГЮБВЫМЭЮХТЮЧМЬШБХСХХФГШЧУЮАЮФЭЭХБЪЮЫМЪЮФЭХЩЪГФНВЮБЯАЮБШЫЮ
ЭБШЧГЬЫХЭШХЬЪГФСЛЭШСЛЫЮЭХВТЮХФХЫЮЮВТХЗЫБЭХВХАЯХЭШХЬФХЫЩЗВЮВХСХУЮ
ТЮАВШЭХГЬЭШЗЩСВОИЪЯХВАЭФАХШЗБЪЧЫФЮСАЛЩФФМЪШВФБЭЮБЪФЫХХТАГЪЮЯШБШС
ЛЫЮЭЯАТШЫЯГВМЪСХАФБЪЮЩБЫЮСЮФХЯАШБВЭШЙГЯГУЗХТЯАЬФЮАЮУЧЭХБХЭСЛЫБЭХ
УЮЬЭЮЯЮТБХЩБВХЯШТШФЭЛСЛЫШЪЮЭБЪШХБЫХФЛХЦХФЭХТЭЮЮСЭЮТЫХЬЛХХЕЫЪАГЯЭ
ЮЩАЛБМОБТХЫМШЗХФТЬЮУБЫХФЮТВМЧЬЭЮОШЧФЫШШЪАШЗЫЬЭХЯЮЬШЭГВЭЮЯЮВШИХБГ
ФАМАФШСЮУЯЮВШИХЯАЮЪЫВЪЫЗЮЭЪЬЮЭХГБЯХТХВЧВТЮШЬФЮЫУЮЭЮУШЬСХБЮЬЪГФБЯ
ХИШИМФЮСАЮСЛЭЯШАВЮЯЮФЮСГЕВЮУЮШУЫФШТБЪЮАХЧБТХАЪЫШСХАФБЪШХЮУЭШЯЮХЕ
ЫЯАЬЮЭЭШЕЪГФЪГФВЛЪАШЗЫБТХЫМШЗФЮУЮЭЬХЭНВЮУЮАВЮУЭШГАЧСЮЩЭШЪЮТЮСКХФ
ХЬШЕЯЮЪЭБЭХГТШФЫШЯХВАЭФАХШЗСВОИЪЯХВАЭФАХШЗЭХЯЮУГСШУЮБЯЮФШТЫФЛЪЮЯ
АЮЯФХВЬЮХФШВЬЛЯЮФКХЕЫШЪЮТАУЬХБВХБВТХ

   (b) Расшифровать текст:

ЖЯЩГХЬОЬНШЬЙСЗОЬЙЯПХЫАХГХЬОЬНШЗАДВУИМЧДВЦЯЫЮАНИЮПТВЖЮЛССГЦОЛЗГЪР
ЦЗЙОШЫИИЪЕЬМЧПБФЦЕХЮБНЛЩКЪДЬАБВИООНШЗИТОВЕЙХОТИГВИОЮАЦЙЭЯЬИИЮЛНИ
БЭИЙЯЯХКИАИБВМЧДЫЯЗАМЮЮГПЛЭЛЭТИМВТДЫЭЯРЫФГЗЙЮЯХЕЧХФЬНЯЭВЭИЬИИЮНИ
ЯЩЪИЮСЮЛЬЖЫМАВЗТПББКЭЛЯИЭТБМЬЙЯЯШЮГЕЩЫВКТПАЗЯЭВШСЕЧЛТИКЫБУНЖХЯВЦ
ГРЛЫИЭЧВВИНУВЫИГЧРИМЧЯЛЭЯРЫФХММДВЫИЭТЗЯЦЩЖЕЩЗГЪФВИИТАЮЮАЪЯЛЙАЦЗЮ
ЭОЭВЗЗЙРЛАЛМЫИГЛЗТБЮЖЭЮВУИЬИИГСУТЛЯИРЩВЫВНЙОЯИЖЮПЪЗТХЗЮЖИЮПЮГЕХК
ХЙЛХЗЦЯУЙИШЬШЯЛТКАЩЙЫЦТХЗТИУТИШЙЙСИЬЗАФМШЛЕАЛВВГФРАВИЭДТЯЛЪРЫЯАХ
МАИТТИБЕАСРОУГТОВКЙЧЕЫШЬТДЭХДЬВВКИСНХЯЭХФЯИБШРЩЛНЬНШТЖХЙЭЯМЩЛШЖЗ
ШЩЗВЕЫЙБМЙЭРСЕАЦЗЮМЙЭШХМЦЩКХЬТТНЯКЙХААЕЗЪВЪКДЪКГАЯПБХЗЧРТУИНЫЯЛГ
ЕЫРБЕОРЙШЬИФРАВИСВЫМЧОШЫИИТФХЭЙПДЫЗМТЮТВЯЭЯЭИЯАХЭХДХЛСКНЮЩЪЛЭТИМ
ВТАЗЮМЙЭШЩЫЦШЕФЯИТАШЫАШЩШЮАШЙЮВРЭФШМАШЩЯКГЧДЫИНСПМЖЖЙФШДОЮПЮКООИ
ХГЕЧДЗЯЗЮМАИМХИШБОЩИХЗИИЖБЬАШЩШСГВВЬНЯЫИЦЯИЫПТЯТШОЮЬМТЯЮБЗЫГЭИДВ
ЛЫИЯЪЛБМГЛБЮЕБТКТИВЭДШЕМПВЫЦГДФБИНДОГЙЛХЯХЮАЪКЛГЭОЛЫЦУТВШБОЩИХЗГ
ТБЪИЮСГХЛОСНМНМЬВЫМЦТЙГБЯЫИЦМЧСВЫИТЯЛВИИТИФЗЙПЛЫМЭЫОГЮЛЙБХЗАРКХЬ
ЦСЙЯИЯАЙЫСНЫВБЕГПОШШЛТХШМАШЩЭНЩЩЕЭННАКХЙАЭВБЙЙЭЫГЙЛЩЛУИМЯНШДНЫРЦ
ЬКЫОЫЯЯЮПТВГПНХЖАЪЕВКОСКЮЖИТЮГЮАЯЛБЬЙОЛФВНЙОЮМАРЛЮЙАЧЕШЬВРИЭНЭЪК
ХЭЙРЛАЮЙЮЗЧЕНПЛЩЭЙЮМЮЮГЪПЛЖЙЦОЫНЮСВЭЦЮХЙЮВГВМАИГРНЫЙЯЯЛЬНТЯЛВДЗЪ

ВТБЯАЙЫИМЙПХЫАЮЛТЯНАЫЭЯОЩКШСНЙЕФЯЖЯЩВИТЯЛВЯЬТМАВЕФШТШНЮЯХЕЧХФВДЬ
ИИЯИЛУВЭЖЙХЙШЛЖЫЯЬВТЯЛБЙЖТОЭНЖЭРЪЖГХЛБМЙШЮХЗАШФВИБТПЛЛНЫЕИЦВЧНШС
ЖЮВАЮГЯЛБЬАШЩШСВЬИЪЕЬЯЫИДКТПАЗЯЭВШСКЭЛШБИТОЮЗЯЭЛЦУГЩАЮЕЙЮЛЬЗААЙЮ
КГЩВЭЛКТФЫВМПВВМЦЩЛЩЙЙЮИГТДЩВЭЛНЭЕЪЗКХХШЧНЫЙГКВОЛЩЗГЧРЗМЙЯШЯИУАП
ШЕТЯЛГЗМХБХЗАРПЮМЕХТЭЯЭЫБШММЮПЮ

2. Разложить на множители числа:

   (a) 60102112943881606339338636133 1

   (b) 455791177026297199558328491170454384517238773542990588004249

   (c) 153359113808375775201684033818759055275077627000078285261168000300421336283887875084834125 1

   (d) 155429237269753266252358491605794231327967791149478021532452535750128875833956258131113651067360238821188428215870000862 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 730682571753472607778924642327147212990471335121875501489246213886368399867 09$
   - $e = 3$

   Сообщение:

   - $M = 604226067294549368133519277196667062728119464766635195340438864773629975414 2$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 3148611748461387012881696895695559840 59$
   - $q = 3185863090044413764180808695996015680 23$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 6460936574788514370468382599936694319247213009448837194873423131318058075112$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 151451514380453253238568995305144460151$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 407916105911037873063886453815324384 85$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 191709607512062105972976900049655143177$
   - $g = 173059810774878907761712423237654539559$
   - $y = 187461009399066806152648206280126447824$

   Секретный ключ:

   - $x = 277335387793214462240018185457467371 59$

   Сообщение:

   - $M = 191310052771103337062494774892800117731$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 125645510307184893386001157572850654457$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 181784884428227168994183259050054397103$
   - $g = 137980260613085469784444836947121316449$
   - $y = 258225987597676029964751050295727371 61$

Сообщение:

- $M = 78328590390676114928539194329274186502$

Подпись:

- $a = 16546464047648021737314866542091881822 5$
- $b = 38381243053846693766153131809597906970$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 593$
- $g = 163$
- $y = 30$

Сообщение:

- $M = 80$

Использовать следующий случайный параметр для создания подписи:

- $k = 43$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 3x - 9$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 87

1. (a) Расшифровать текст:

ЖЩСЬЩЬЯЖРПЮЦЫХЬРБЗУСЬЪУЫЭЬЦЪУЫЦХТУЯКЕУСЬАЙГЬЕУЖКЯТЧЯПБЩЫЦЫЭЮЬАЦР
ЦАКЯЫЭЮЯЫЬЭЬФЩУЧЯРЬЦГЯАЮЦШЬРБЭЮЪЯАРЬЪЯУПЫУЯЭЯУЖКТЬРЯТЬПУЮБЯКЭЬЭЮ
ЬПБЧЦХЪУЫЫЦШЫУЯАЫБЫЦЯЪЯЬРАКЯЭЬЭБЯАЬЪБЫЦЯРЬЦГЩМТУЧАЮАЦАКРУЩМЭЬТФУ
ЕКЫПЮЦАЬСТЭЬЯЪЬАЮЦЪЕАЬАЙЯАЫУЖКТУЩАКТЬЫШЦЖЬАПУЩЬСЬЮЯШЦЧАУЭУЮКРЮУЪ
ЬПУТАКЭЬШЪУЯАКЯЦТЦТТБЪЧЫТЬЯБСУТЬЯРЦТЫЦЪЮКЦРЫЬРЫЫУЦХРЦЫМЯКЭУЮУТРЪ
ЦРЪРУЮЬАЫЬЫУЯШБЕЫЬРЭЬАУЪШГЯРЖЦЪЮЙДЮУЪЖРПЮЦЫБТЩЦЩЯЦЬЯАРЦЩШЮБЩБЫПЮ
ЪЙЪЬЩЕЩЦШФТЙЧЦХЫЯТБЪЩЭЮЬЯУПЫУЯЪУЯЬЬПЗЦАКТЮБСЬЪБЯРЬЦГЪЙЯЩУЧРЬЬПЮФ
ЩЯУПУРЯУЕАЬРЯЬЯАЬЫЦЦПЙЩБЕЦЫЦАКЬХЩЬПЩУЫЫЙЧЖРПЮЦЫЬЯУПУЭЬЕАЦЫУХПЬАЦ
ЩЯЭЮЦХЫАКЯЩЦЦБЕЯАКЮЬТЦАУЩУЧЪЬЦГЫУЯАЬЩКШЬБФЯЩЪУЫШШЯБТКПЪЮКЦЦРЫЬРЫ
ЙХЫЩЕАЬЪАБЖШПЙЩЬПЬФУЪШЮУЯАКЫЪЦЦТРЬЮЬРЙЪЦЩМТКЪЦПАМЖШЫУЯЪЬАЮЫЯРЬМЯ
АЮЬСЬЯАКПЙЩАШФУЩМПЦЪЦПЬПЙЩЯЭЮРУТЩЦРЦХЫЩЦЯАЦЫЫЙУЫБФТЙЭЬТРЩЯАЫЙГУЪ
БЩМТУЧПБЫАЦГПЙЩХПЩБФТУЫЦУЪСЫЬРУЫЫЬУЭКЫЯАРЬЫУЦХИРЩУЫЦУЦГЫУСЬТЬРЫЦ
АБАЭЬЗТПЙЩРУЮЬАЫЫЬЪЮКЦРЫЬРЫШШБМБЕЯАКСЬАЬРЦЩУЧЮХРЮАЫЙЧЦПУЯЯЬРУЯАЫ
ЙЧЕУЩЬРУШЫУЯЪУЩЬЯАЫЬРЦАКЯЫЛАЬЧБФЯЫЬЧЪЙЯЩЦЦСЬАЬРЦЩЯЭЮЬЯАЦСЬЯЭЬТЦЯ
ШЬЮУУБЪУЮАРЦАКУУЫУФУЩЦРАЬЮЦЕЫЬБРЦТУАКРЮБШГФУЯАЬШЬСЬЫУТЮБСЭЮЬЖЩЬУ
ЗУЬШЬЩЬЕЯРТУЮУРЫУЮХТРЩЦЯКЭУЯЫЦЭКЫЙГШЮБЩКЫЙУЫЖЦЦЪХРЦТЬРЩЦЦТЬЯТБЫЫ
ЯЮБСЩЦЯКЦЯАЮЗЩЦЫЯЦЯАХЫЦЪЦЦЯЪУЮАКМЪЙЬФЦТЩЦЭЬЯЩУТЯАРЦБСЮЬХЪЖРПЮЦЫЫ
ШЬЫУДЯТУЩЩЬЯКПЬЩКЖЬУТРЦФУЫЦУЫТРЬЮУЦЪЙЬЭАКБЯЩЙЖЩЦСЬЩЬЯЖРПЮЦЫЕАЬЫТ
БЪЩЦЯКЩЦРЙЬАТУАУЯКЩЦТЬПЮЬРЬЩКЫЬРЪЬЦЮБШЦЫЦШАЬУЪБЫУЬАРУЕЩЭЬТЬФТРЫУ
ЪЫЬСЬЖРПЮЦЫРУЩУЩЭЮЦЫУЯАЦЯЬЩЬЪЙЕУЮУХЫУЯШЬЩКШЬЪЦЫБАРЯЭЙГЫБЩЬСЬЫКЦЬ
ЯРУАЦЩАУЪЫЙЧЫПЮЦТЙЪЫЕЩЭЮЬПЦРАКЯЦХЭЬТЗУЩУЧЭЬЮЬСАЬСТЪЮКЦРЫЬРЫЭЬТЬЖ
ЩШЬЪЫУЦАЦГЬРХРЪУЫХЮБШБЯШХЩЭЬЩЫЬЭУАЮЫТЮУЦЕЫУСБПЦАУХЪУЫЦЯУ

(b) Расшифровать текст:

ТУДЭЙЖННАКСОЗЩЙЖЧОЬОПЦЯЯЮУВНАКТИКЦИФФЭМЖОФЮЦЙЙДДУУЖЦФЮДЖХКХКИЦБЮ
ДЙНЯЬАЙСДВШТФЮЦМЩЛЙЮКЙНЯЯЗПИЧЦЯПХКШЮМИКЧОПЙКТЗДФАБДМНКЫГОУППЛПТК
ИШЙИБЬБМЧЮЦЗЭОУДАУВБЭПРФЗГДОЩЙУКЕРПВЮЖСШЩУОЫИДМЙСНАКМШДЮПОИКХЖФЧ
ЖШЗПУГИОПГОЯГУФУГКУБВЦДИИКЬДМХКХЮЖНОЩБДФЖАКТШКЬКНЩАУКСЩЮЯЗУИКВПЕ
ЦШЮБУЩЙВЗЙЮЙЩСРФЗГДОИНЫКНЩАУОЭУЮЯАЛЩОЫННФИДНЛФМЯЛСОАЦОТЙКЬКЕШШЮБ
НФЯВЛПЦДГШТЧЮЦЗЭОУЦИЕЛЙНЯЙХКЭКЖТПЯЭЖЯЙЩЪОЫКХДМОННЮРФЗЮКНЛЯЯМТХКБ
ВЖУДЩИОЛЭМЗПККВАОФКХЙЛФВИОПУБЭКДФОТЗДФАБДУВУЦЗПИБЫЮЬЦПИДГЮБФКНЛЙ

ЦНМОЙЦДИЗБХЧУФЛЯЖСПЙЦЕНЛМЦДИФУЦЙЭУБАМЙШЙЯЯПХКЬКЗЛЙЩСПЦКЙКТРГЬСМК
ЙЯЖСФЮЮКЖЧЗЩЙЖЫКИБЩВАГШРФЗГДОЩОЯЮЬУШЦИФЭОЯЙЙЗПХШЙНИЯБДФЛЬОЭФЙЯАЖ
ШНЬДЩРКЭЗЖЙЖЯАКЛИДИППГЪУЙПОДЗФХЛЯИЙСПЪЭУДФЫЛЖШМЮАСЛДИНЛНЗВЮЖСШЦУ
ИЭБЭБНЩОУККНЕИДКШПЬПРФЙЦЯПХМЯЛЭЛОВКВРЮАБСИКЭЖВРБООПЧОБДОЩФЫПЗУБГ
ЮПХБИЗЭЧЖШЗНФЕТМПКЯАМПХШПЗЙОЗЩЙЖШБФКВСЯЯМПКДЦИОЛВЬПЖШФДЭФЧКВЮПЛЯ
ЯЛМЛУЦЯПУОЯЭСЧЖУКМШЮЯБЦФЗЯЛЭЛАЦЗПУБВЛПЦДГШЙЧЗДФУВНТКДШЧЮБВФДЙШТЦ
ГТККУДЫКУИБИЗЖТПВЮЖСШЩУТЛМХДУБИФКМФНЯИУБЮЩАЙЮШИОПКДГБЪЛЙЦННБНЬДУ
ШЧЩМЕЛЯЯКВФЭБОЭХМЯНУФОМБДФМХДИЭБЭОЖЗБТМТРДЪОФСПАУЙРОМДОЛЙАЗЙЮШЦЯ
ПУНУКЙФЖЮЙЬЛЛЬБШОХАМПЮПЮБФТЙЩУУВНЫГМЧЮЯБНЩАХШЛЛНЦЕШЧЙЦНЙЧЪХОФСПА
ЯПЧЛЯАЙИЗХЧЛФЛБКТШКЮЗНФЕВЮЖСШЩУИПУЩЕУЩЗДЛРФУГДОФЮЦФЖУШЫДКОАЯЭСФЭ
МЖПТПГКРВЙЩТЖФЯЯЗЖСКЭППКЙЫКИПУЩЕУЩЗДЛГОЗВИФМДИКЛШПГВЖЧОЬБДФЛБДНЛ
МЩЮУВЮВИПТАЦЗЖШПЬПРОГЫКУФМЯЯПЩНАБМОЮММПЧОЩЭЬСЙЦИОФВЫКЕСЙЦЯПЩГЯЖП
КЙЫКПУЖЯБЛРПЭПЕЦДЬНЙУАЦЗЖЙКБНРФМЯЮРФФУИТИБЬШЙЭУДОЭУБШЮЬСПВЗЬЮЮЫЖ
ООООЫДИШМЦХМОЭБКЕЙЭМЗШЦБШЮЬЭЕЮКЕФЮЯЗЖУИЯДНХКХМЛФИЯЙРЦКУКЕОЗЭБОККЫ
ДВООЫДЙЧЖШЗТУДШЖЙТЛЯЖМФЙЯИТХНЩЭПИФЦЭМЙКБКЕОБЮЯСКД

2. Разложить на множители числа:

   (a) 787013652110357240379613820999

   (b) 78815404733333556589639739597980314267997912769085432804347 3

   (c) 954382350253785129798771495964725927702926360035904958914238026214340882446164710336372111

   (d) 1030857626978151074688082914895499203857267983679847470357338762992488299087569454270420884459137859775900419123366217047

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 407959398502247924877879876171694254295804753839149212419929598717114595820 21$
   - $e = 5$

   Сообщение:

   - $M = 384108327058042140122274982906667395770448245911486948647597115061790269588 88$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 288268924529253083928178822386886883113$
   - $q = 211549900548085239190533189694789351349$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 418589485922753589201053651553253757961985824103979781016729124003494724 3017$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 211900430354139834018151207171478597027$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 180773730536012892013034713877823758840$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 192234336624978828256481610896478120901$
   - $g = 296192812366277047763221739160255192 31$
   - $y = 153855080917752038737168007837508463257$

   Секретный ключ:

   - $x = 985455421008970648162215177109085359 03$

   Сообщение:

- $M = 814151065910756201700353881713289697 95$

Использовать следующий случайный параметр для создания подписи:

- $k = 900988007211677379705213465122577450 49$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 24279896320221764216736234452435229 9497$
- $g = 71720629491280541200632207519620099 67$
- $y = 23697965434330774187381699395064893 7556$

Сообщение:

- $M = 57594997366063499505220275232660238083$

Подпись:

- $a = 16534402198737962720663254463258850 0420$
- $b = 21081151434693851810558546906502770 9497$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 599$
- $g = 279$
- $y = 65$

Сообщение:

- $M = 91$

Использовать следующий случайный параметр для создания подписи:

- $k = 151$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 13x - 4$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 88

1. (a) Расшифровать текст:

ЦЬЪОЮФОЗЮЪЧЦЧФУРОСЬСХФОЮЪЮТСРСЩИЫЬЪПЩЧЭЪРОЪЬЦЩСЪЫФЭЩЩЪХЬРЪЭЮФЭОС
ЧИФГЮСШФЦЪЩГФЧЪЭИШЪСОЪЭЫФЮЩФСТФЧЩСРЪЬЪЭЧСШПЪЩПЪЧЯНСХФФПЬОГБЬРЯЭР
ОЪЬЪОЗШФШЧИГФДЦШФШСТРЯЮСШШФЩЯЧЪШЩСДСЭЮЩРВЮИЧСЮЮЯЮЭЯРИНШЪЫСЬСШСЩФ
ЧЭИЪРЩТРЗЪЭСЩИКШЮЯДЦОЬФЧОПЪЭЮФЩЪХШСРЪОЪСОЬСЩИСЪНЧФУЗОЭИЭШЪЮЬСЧЩЦ
ФЫЯГФСЫСЩЦФНЮКДЦЯЪЦЩГФЮЧЫЬФРОЪЬЩЗХЦЧСЩРЬИСТСПЪРЩЪФШЫЪЧЯГСШЗХЙЮЦЩ
ФПФШСЧОЭСПРЭФЧИЩЪСЩЦСПЪОЧФЩФСЩФЦЪПРЩСЫСЬСГФЮЗОЧЪЩССНСУЪЭЪНСЩЩЪПЪ
ЯГЭЮФФГЮСЩФСЙЮЪЫЬЪФУОЪРФЧЪОЩСШОЭСПРЯРФОФЮСЧИЩЪСОЪЧЩСЩФСТСЧГФШЮЯД
ЦУЩОДЩФУЯЭЮИОЭССПЪЭОЗГФФЪНЗГФОЭСПРЭЮЬЧЭИУЭЯЩЯЮИЩСЭГЭЮЩЯКЦЩФПЯЦЦШ
ЪТЩЪЫЪРЧССФЮЦФШЪНЬУЪШЫЬФРОЪЬЩЗХЦЧСЩРЬИЩСЫЪЫРЧЭСШЯЩПЧУФЩЪПРЫЪВСЧЗ
ШШСЭВШУЮЪЦЪПРЪЩЭЧЯГХЩЪСПЪЩБЪРФЧЮЪНЗОЧЪЫЪВСЧЗШГЭШЩСОЗЫЯЭЦЧЯТФУЭОЪ
ФБЬЯЦФЮЦНЮКДЦГФЮЧЫЬФРОЪЬЩЗХЦЧСЩРЬИФУЬСРЦЪЫЪТФШЫЧСГШФФЫЪОЮЪЬОЫЪЧП
ЪЧЪЭПСЩСЬЧЫЪЬЯГФЦЪЩЯШСЩОЬЪЮСНЗЧЭСЬТЩЮЪШЪНЪФБЬЪЭЭФХЭЦФБЪЬРСЩЪОЦОЧ
СЬРОЩЪЧФШЗЩЦЪЩСВНЮКДЦДОЗЬЩЯЧЦЧСЩРЬИЩРФОЩФЫЪПЬЯУФЧЭОУРЯШГФОЪЭЮИЩС
ЫЬСРОСЕОДЯКЩФГСПЪРЪНЬЪПЪОРЬЯПЪЩЪНЬЮФЧЭЦШЮЯДЦСОРЪЮИОЭФЧИСОЩЭЦЪЧИЦ
ЪЧСЮЫСЮЬЯДСРОЪЮЫЪДСЧЭСШЩРВЮЗХПЪРЪЦЪЮОСГЧШЮЯДЦЫСЮЬЯДЬЪРФЧЭОЮЪЮЭШЗ
ХПЪРЦЦЪЦЬФОСЧЮСЮЯДЦЩЭЮЭИПЬЭФШЪОЩФЦЪПРСЕСРЪНЬЪЫЬСЬОЧНЮКДЦЫЪЬСПЪОЭ
ЧЯТНЯЫЪЧЩЪСШЯНСПЮИЫЪРСОФГИФШРЧУФЮИЩПЪЧЯНЮЩФШЗЭЧИЪЭЦЪЬЪХЬУЧЯЦСЭЪШ
ЩЪКЮЦЫЪЬУФЧШЮЯДЦЯГЮЪЪЩЯЬЪЩФЧЧЬТЦЯОЦЭЮЬКЧИЦЯФЭЧСУЗЫЪЮСЦЧФЫЪССЧФВЯ
ЩЫЬЪЮФОЮЪПЪЮЬЯРЩЪЪЫФЭЮИШЪСОЪЭБФЕСЩФСШЗЭЧИЪЭЧЯТНСЭЧФОЧЭИОЪШЩСЭШЗЭ
ЧШФЪЭОЪНЪРСЪНЯРЪОЪЧИЭЮОФБЫСЮСЬНЯЬПЭЦЪХТФУЩФОЪЪНЬТЧЭСНЪАФВСЬЪШПОЬ
РФФГЮЪЫЪШЩСЩФКШЪСШЯНЗЧЪОСЬИБЪШНЧПЪЫЪЧЯГФГСЧЪОСГСЭЦЪПЪНЮКДЦЩСЧКНФ
ЧЩФЫСЬСШСЩЮИЭОЪФЩШСЬСЩФЩФЪЮЦЧРЗОЮИФБФЭЫЪЧЩСЩФСРСЩИЪЮЖСУРЯШЪСШЯНЗ
ЧЩУЩГСЩЩЦЩЯЩСН

(b) Расшифровать текст:

ЯЙНЛЬЗЩВЗНРГСЯЙАГХЪНГМХШУЗЧЫМЛГМТИГЧИФРВБГБЙИЪНФОЕЬЦМИГЧЙЪВИЦОЪА
АГНМВТАКЭОНЯГЫЗВАЕШЙАВЯЧПОВМОЯИГИТФАШЙЧВМАЦЯПЧЦУФЕЛЛЦЧНЙЩИЩРЮВИЕ
ЖЯЭЕТНЮЭВАШКЕЙЭФАВЦЧВЬГМЖКИЖИПООВОЬОИЖОЧРНЖНФПЕИЩСБЗГМЬНМЗЕЭФНГЖ
ППИЩАЫПЧИЮШЙЙВЩТЯЗВАЫПЛНИШМЛГЯШИБАЙЛНФЖЧФЗКЭНЧХАГМЬЯНСММЗЛЪКШОНЭ
КШБЭЪЛРВИВЙУПЕЭЗШММВЙЫПЗДЛТЯЦМЕЦЛДЦНИХЕГНМВТАЙЧПЙБОХВНЩЭОУНСЕФКМ
ЭВЩЛЖЯКПНАЧАХЕМУЯТКАДЛТЯАЩГНЛМДЙОЕЕЯЬШИМСКЪЛЕАНЕТШЗГЯКАКЛТОНЪДФЗ
ВЧГРРЬРЭХЛЛРМЖЕУДЕТБЕЯВЫИЦНОТТЭЭВНЯАЕГВЩЖЭЙЬВСБЙУОАЕЯАВНЯГСЙЛЪНЬ
ВКЪЛЖПЕДЛТЯЦЯЖБПЙЭМЦВМЗИППЛГИЭОЧЯЕЩНГЩОЬКЗЖЕСПЧМНШДЖГЯПЕЙЯЙХЛЕЕА
ЩЛМЗГЪШФИНМОГАГЫВЮГЛШЯИДЛПТЛЦЛОЙВБАЬЕЖЧБЧЛУЧЬЪЕИЭЭЧЗОЬЗТФЗГБППШЗ
ЙСОЭЭЯППААЧЫПЭГЭЬЩЯЖЖЕХЧЗЦЫЗВАГМКЕИВЦЕТЦЬЬЛИЪЛШЮЕГЮШБАЖНФЙЛСГМКЙ
ЧИЫМЛГМТИНЯБПИГЖЗПИЕЯГМШМБАХИГБУШПЭЪТХВАБНЖКАЗЗВПЛИМТТЯГМТТКГЛЧВ
ЗГБППМАЦВПЧЧЦЫПЛЪЖТДЛИБЖПЕЭВЬНАДАГВНЖЕФПЙБООЯЮГЯТЯИЯОСЙГМЭЕБОБЖМ
ЙЙЭГЦВИЭИЕМЖЭНЖЕВВУПЖКИУФЕНЯЙЧЙЙШЙХРЬИУФФОЗЧЫЛМЗЛЯКНГНЫЯАЗИПЛНДЛ
МЕЖЖЧЫПАККШНОЫГЧВКАГЦЕВДЛШЗЖЗЙУМОНЕТЙЦЧМЬИГЭВШОНГЖФМГЗИЫЗКЭНЧХАУ
ЙЬМЛЧГХЕМСМЩПЧДЙВВЖЯУМЮЛЭИЭОЕГНШНЦБГЩНЙЧАХУААЦУЯАМАЪАЖЧКШВЯЭИШЗГ
ВГСЯЙАЧТОНВЧРВЭДЙСЕНИЛЭМЙЖЗШПЛЭУЖМЛГЕШИЩЯЕЬЯЙУПТАОЕОФКБВГЧМЛГУХЛ
ИЪМФЛЖСЕШКАЩАХЩГЫГСКЧБЙМЮААЙНЛЛЖЕШЖЕЕАЩЛМЗГЫБААЖЫЩЯАЗПКИЪНШИЧЯЙЫ
КЙЖИШЫИГЯРВГДЛТПИГЩМБЙБАФЛЗЪИОКНЦЦХМЛЭИЬЗЕЕЙОКЙЮЗЭГГЫАЧЮЦАГХЫЯЭМ
ЦШАДЙБПАВИЕВГЧИФРВБГБЯЦНАОХГЮЭШСГЛАЪШГЬМШИЯЗМФЕРЩАЬВДЦЦХФААЙМВЕВ
АШЮЛЬЙМКИРДТМЛГМЬЛДВЙЫЙЦЮТПОНВЦУ

2. Разложить на множители числа:

(a) 864073916604020161950692809901

(b) 753649904531415210988042457733312546431170315551463056197567

(c) 9937729350471559818127272741852193112059968383149970746945981606090764597953317647956430 01

(d) 1184465543406122979443316428509163188439026621454091257609680184231874237237800498228340376877193355422965516680798561123

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 904060301867786524766424792967549801806965451170192732112538973896708478074 27$
- $e = 3$

Сообщение:

- $M = 190731298422699687312058125676751054423812365606184307121864125676723031240 16$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 232976498380700404760261997191856848531$
- $q = 175959496652622827705251826012333276389$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 129644516290190417542142620598549127509151864058005338999098850816358040954 37$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 143769449448380313438025696939210242617$
- $e = 17$

Зашифрованное сообщение:

- $c = 102501130222142186290387108491882509682$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 286512060728949343111389466263931348999$

- $g = 732845697374594329763266367484237809 82$
- $y = 296766740372379368720180972727428269 78$

Секретный ключ:

- $x = 276950746981398007134868252974731418683$

Сообщение:

- $M = 172238458354788646281708088644532527923$

Использовать следующий случайный параметр для создания подписи:

- $k = 233420951316664829401332020686304893451$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 179644642046878520081404232227424409923$
- $g = 316991829403329854372738353959066772 3$
- $y = 157507965848546332954682250333911741223$

Сообщение:

- $M = 137620256810791794840806938941536600038$

Подпись:

- $a = 347770575250818659210967464913504259 19$
- $b = 168947159151208555779006195346912468970$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 659$
- $g = 364$
- $y = 607$

Сообщение:

- $M = 600$

Использовать следующий случайный параметр для создания подписи:

- $k = 307$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 17x - 2$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 89

1. (a) Расшифровать текст:

ЧДНЯЧЧЦЧКОГБВАГЪЭЮЛЪЬГЯЧДЧВБЧЯЪЧЮЦЙДАЧЗДОАДФЧЙЭАЯГЭЧЩГАУЭЕЙЬЯЧФЧ
ГДОЪДЬЬЕЦЩЧЗЭЪЦАВАХЪЯЧДЪЮХЭЬВЕХАЮГДЭУНЭАЧХАУВЯЪДОГФЧЭОЪЙЩЯЧХАЩГД
ЕБЪЭГЪАЗАДУНЭАЯЧГЭЕКДОГХАФАВЪЭАЯГЧВЦЪДАФАВАДЪЭГУНЯБАГДАЭНЫЦФАВЯЬ
ЕКЭГУНЙРБАЙЪФЭУНГЧУЧЦАЕДВУЕВУЕДЪЗЭАДБВФЪЭЪГОУНЦЭЧЧЪЬЕЦГБЧКЪЮЦАУВ
АУНЯГФЦОУЕГФЧЭОЪЙУНЭБВФЦЧЭДОУНЭАЯЧЙЧХАГЯЧХДЬЪФЭЪЭАЬАЭАЬЪУЪДЬЪБАЦ
НЮЭГГЕХВАУЭАКЦЪГДАЭЪБАЯЕВХАЭАФЕЪЩВЧЦЬФЩЦВХЪФЮЛЪЬЗАЦЪЭЬВЕХАЮАДЯЧ
ЙЧХАЦЧЭДОЕЭШЪФЕБВШОГФЧЭОЪЙФАВЙЭХЭЦЧЭФАФГЧГДАВАЯНЯЦЧГОЕФЪЦЧДОЗАДО
ББЪЩЯЬШЪЭЪЭЪЦАВАХЪЯАЯЪЙЧХАЯЧЮАХВЩЭЪЙЪДОЬВАЮЧЮЕДЯАХАЬВЕШЧЯЪЮДЧЭЪФ
ЦВЕХЕФЪЦЧЭЙДАДАЙЧВЯАЧПЫЮЛЪЬЩЬВЪЙЭГЮАДВЪЙДАДЮДЬАЧЙЧВЯЧЧДГЮЛЪЬГДЭФ
ГЮДВЪФДОГУАХЩЯЧДУВЪЯГЬЩЭАЯГЦГОЯГФАЧЮЧГДАФАЩЯЧФАЩЦЧВЧФАЯЧЦЧВЧФАЬШ
ЧДГЙДАКЧФЧЭЪДГЦАЭШЯАУНДОЪЭЪФАЭЬЪЭЪЙЧЭАФЧЬБВЪЬЩЭЧЗДОЯЯЧЩЯЬАЮНЫБВЧ
ЦЮЧДЬАДАВНЫДАДЙГЪГДЭБАЦФЪХДОГЯЮЯФГДВЧЙЕЙЧВЧЩЦФЧЮЪЯЕДНЮНБАВФЯЭЪГО
ГЙЧЭАФЧЬАЮХЧЫЦАУВНЫЙЧЭАФЧЬЩЬВЪЙЭЧЮЕЮЛЪЬГЬШЪЯЧЩЯЧКОЭЪХЦЧЦАВАХЦАВА
ХДАЩЦЧГОГДАРЯДФЧВЦАЫБАЭАГЧАДФЧЙЭЦАВАШЯНЫЦЙДАДАЭЬЕБАГЭЕКЫЮЕШЪЙАЬГ

ЬЩЭЧЮЕЩЯЧКОЭЪДНПДЕГДАВАЯЕФАЩОЮЧКОГЭЪДНЦАФЧГДЪЮЧЯЦАЯАЙЭЧХГДАВАЯЮЯ
ЧЩЯЬАЮАДФЧЙЭЦАВАШЯНЫГЭФУАХЕЪГЗАШЧЯЪЩМЧЩШЧЯФЦАЭОЪБАБЧВЧХЦФЪКОЬЬБА
ХАЦЬЬВЩГАУОЧКОГГЦАВАХЪЭЕЙКЧЩЦЧГОАГДЯАФЪДОГЦБЧВЧШЦДОФАГОУЕВЯЕДЪЗЯ
ЧДЦЯЧУАБВАГЯЪДГДАХЦЯЫЦЧЮЦАВАХЕБАЩФЧЩЦЮЧХАЗЭЦЯАЬВАФЪЧАУАЦВЪЭАЮЧЯЕ
ШВЧКЪЭГБВЧЦФГЧУУАШЪЧЫФАЭЧЯАЙЧФДОБАГВЧЦЪГДЧБЪЬЬФЦВЕХЦАВАШЯНЫГЧЭБВ
АФАВЯАЯАУЭЕЙАЬЪГЬЩЭЮЛЪЬЕЯЕГЭФУАХЕШЪЭАЯЧЦЭЧЬАГФАВЙЪФЫФБВФАЦБАЧЩШЫ
БАЙЧЮЕЧЗДОЮЯЧФБВФАГБВАГЪЭЮЛЪЬГЯЧЕЦАФАЭОГДФЪЧЮХЦЧДНФЪЦЪКОЦАВАХЕЯЧ
УАГОЭ

(b) Расшифровать текст:
КЯЯЩЫОЦВВДФЖЪВПМЕЯЩХЩАЮЮШГЦФЬЫДЙЩУГФМОЫЭРЗЧЮЧПНЕАБРЬНЫАРЭЧЮЫАМФЯ
ШООБЯЧУАЭЫЯТЧЧЩХПЙФЮШКЭЯЫЖЙЗЪИАЗЬНЬБЖЙЮУДКЖЪВШЕЙВЯХПВЯГФЭЖЗЯЪЛМД
УБОЗНБЪЕЙФБЫДЖЪУВРЖХЯЮРМЮБПКЭЯЯХПМЯЦЩПЙГГЫАЭНФБДЛЪУЮОИЧШФЗМБЯЭРД
ГГХРКВЩККИЧЮАРАФВШОЗАЦСУМАББАМКУФТГЯМЯФЕЪЯФОАВЬДМВЭЯАМЙХХДМВЭЩАО
ТДЯХЭИЮЦГЗИНТЫФЧГЮЛСЮЗЫЭООШИЫПЦГГГПИНШБЖИАВЮРЭАЯЭРНАББОТЧБШЙИЧХШ
НЩФЦГПЙУЯАККАШФЭЖЪЯАКЮАГБДЦВЦЪФЧГЩЩЗЛДУБДНОЮШФЙЭНЭРБЪШАКЩЯЯЫУЙФЦ
ДФГРЩФНЮААБНОЙЩШОНЧЖЭРНАБОЗИАДХЗЛЧЮКФЙЯЦХЭВЙЩАЫГЬВДРЛНУШТИАУЫПЙФ
ГЮЗЕГЦЬКЭЯМКСЙЙЦЯХБЧУОФЕЦДЯЗНЧЭГЮГФЮБДИЦГЭРИДЫБЛИГЭШЪИЪЫАЗЖРТЮАЖ
ЧЫДЗГФЮОЩЙЯЯКЗИОЭАЗКВЯЕКЭЧЮДФЛЯЮБПГЩИЕРЬЯЦИРНЧЬКФЙУЩШООДЫЩЗИЧЮГД
ГЭВПЯНАЭШПЬЧВВРЕАЩЮРЬНВЕТРЫХЭЯЕЭШФАЮБПКЭЯЯХПИВУЫФАГНЮКЭНЦЯХГЭЩА
ЗНЮБПКЭЯЯХПВЪЫАХЖГНЫСЙЬБДПАЭЭАЗЕШЦЕУМЬШЮРИЦДЯАТДЯАТЭЭПДЮКАИШООШЦ
ХОНЬЫЩЗНГАБФЙЮДКФЙАЮЪОАЯВХФЖГВХФЖГЯАЙЭГВХФЖГЫБЕЯШЦХСЛАЙЮРЗХЯЧХЗЧ
ВЙЖЭЦЯХЪАХЯВТГЧШЧКЭНЮШСЙКЬЫМЕЪШХРЖЪГШДГЦЦЕЮЖЧЫДЗДЪУАЭТЬЯАЗТЯЯКЗЖ
АУШМОЮЮОЛГЗЯГРУЧЪЗОГЭЩЫКГЮЦШФМАВЕРИЪЦАРЕЬАБЖОЮПКФЙЯХБГИАТЖЖАДАБЖ
ЭЧЮЙРЗББЫДМЧЖДПГЮАБШЖАУЕЮМЯЩЪЩНАЮЫЙЕЬЩШГЖХЯВРЖЕИЫУЖАУЯТЧЪЩХПЙФЮО
РНЬБОНГЮЮШЕЖЩЦБГХГЮЫНГЮЮШОИАФБЗКАЮЮХКАБАРАЩЬБТАЙЩШМЙДЯГЭЗКУФТГЯЦ
ШСЛЧВЮЗЯАУЮДАВЯЕПЙЩЭШЩЖАЮАЪОФШЫОИЕПДМЖАЮАРМДНЫУНВЬДРНФЬШЩЧЯВЧТОХ
ЯЕЖЛЕФДНЙФАБЖЭКЩШСЙФЯЧМИКЦЬУМАБШСЙЬШЮКМОЭАЗАЛЦФРЖЧЦЦПОГЮООГЬЯЦЖЭ
ЮЦДФЙХБЖГЙЫЩАЗКВЩДФЙЫЮБЛИГЭШЪЕЪДХКЯЧЬХПГЗЯФЖОЮЮАХЩЬЬШДАДДЩЗЖЯЩШП
ЕЩГПЖАВШЭРЮАШЮРВНИАКЕГХШНЖАВПДЙЮЮШЗФЧВЫНЧЯЦШКМЯЦЕЗЛБЦАКАЮВЕНЙШЩЧ
ФЧЕХБГИАФБУЖЕИЧРБЪХЮУИЧХБНЮАЮЧТОХЯЬЖАЯНЭРЮЦВЫЖАЭШРНАХЩШЛ

2. Разложить на множители числа:

(a) 10271258400341730270069342417 79

(b) 74284249914692944579316572855800168576541753249093610610 0937

(c) 55763402380448023133260419174205028422356823285936623477021067755050361143953984472273323 7

(d) 12726924581588248106915761738042586569930412322931555868220292671973777226213621506345518025613435851206760537264305713 81

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 43922749788964223026429857034822005621902856044844226385243822999077799488787$
   - $e = 17$

   Сообщение:
   - $M = 40184879642071001478568985885149259028365607781748007653565539019723435524300$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 260350340385922122726605441413896727483$
   - $q = 19842141485501265375808006343718147307 9$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 31664766229735975919424968144638697158508871234791063462286771567679461809070$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 159737114957189543946445247714264076787$
- $e = 17$

Зашифрованное сообщение:

- $c = 147951154880835663183737695115136121734$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 196188132145387923198690789579654561857$
   - $g = 180106765031876942696736354678153805522$
   - $y = 137523794888886775751068358698462250017$

   Секретный ключ:
   - $x = 150449394528508164262391005531516572937$

   Сообщение:
   - $M = 603963233314470169813514975020248472 29$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 26215158158154951919282461458787461673$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 32110782999375507139720399443952310 8099$
   - $g = 21250026115631070319486353903667635218$
   - $y = 20043178462552881728170768014869444 7941$

   Сообщение:
   - $M = 34620446678323891269144123796232593709$

   Подпись:
   - $a = 15721359964830168029936003843518270 18$
   - $b = 17431848835503609917153312529801896191$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 863$
   - $g = 536$
   - $y = 66$

   Сообщение:
   - $M = 416$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 223$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 6$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 90

1. (a) Расшифровать текст:

ШАЮПЫТРЫЩЖХЧЪТСШТДТЫЯПТДШЫЪПЫЪАУПХСЪРШСТШПЫПЮТЮЯЫЭЫЪИЫУХСАПХСТЯЙ
РЭЫФЪИТОЮЯХЫЪИОЕЪХХПШЪЫЪХДТРЫЪТПХСШЧЭЫЩТСТЭТПАЕЧХЫЧЭАУТЪЪЫЦОЭТПТ
ЪДЯИЩФОЫЭЫЩЮЫСЪЫЦЮЯЫЭЫЪИЮЯЫШХЯЭХХШХДТЯИЭТЮЧХЭСЮТЪЬЫШАФЪТЮТЪЪИТЮЬ
ТРЫЩЮСЭАРЫЦЮЧЭХПХПЕЮЩТШЙЪХГЮШАОЫДЪИЩХЧЭИШЙЩХШТЪХПЫЫЬАЖТЪЪИЩХРСТУ
ТЧЭТЬЫЮЯЙЮЬЭЫЮХШЮАСХПШТЪХТЩСПЫЯЫЪЫЯПТДШЩЖХЧАЧФИПЪСТЭТПАЕЧАХЮКЯХЩ
ЮШЫПЫЩЩИПЪТТПЗТВШХАПЫЭЫЯАПХСТШЮЯЭАЛДАРАЪЪАЛЬАЕЧААШХГИОИШХЯТЮЪИХЧ

ЭХПИХФОИЪХФЧХХОЫШЙЕТЛДЮЯХЛЬЫЧЭИЯИЮЫШЫЩЫЛПТШТШТВЯЙЧЧЫЩТЪСЪЯАХДТЭТ
ФЩХЪАЯАЧХОХЯЧЫЮЯЪЫПХШЮЙЬТЭТССТЭТПЪЪИЩСЫЩХЧЫЩПИЮЯЭЫТЪЪИЩЪПИЮЫЧЫЩЩ
ТЮЯТОШХФСТЭТПЪЪЫЦУТГТЭЧПХЪХЧЯЫЪТПЮЯЭТЯХШЩТЬЬЫЕТШПЮТЪХХЫЯПЫЭХШСПТ
ЭЙПЬТЭТСЪЛЛЮЯЭИЦХЪПШХСЮХСЪЮЯЫШТЪЕХПШЮХЪЛЛФЬШЯАЪШЫЧЫЯЙФТШТЪЫРЫЩАЪ
СХЭПТШТШТЩАСЫШЫУХЯЙЫОЫЩЪТПЫЦСХОЯЛЕЧЫЯПТДШХЪПШХСЪЕХСЫЩПЫЕТШПДХЮЯТ
ЪЙЧАЛЧЫЩЪЯЧААОЭЪЪАЛЬЫЮЯЭХЪЪЫЩАПАРШАЮЯЫШЕЧБЮЬЫЮАСЫЦЪЮЯТЪТПХЮТШСХЬ
ШЫЩЫБХГТЭЮЧХЦФЮЯТЧШЫЩХПЭЩЧТЫЧЫШЫЪТРЫЧЭЮЫПШХЮЙШАОЫДЪИТЧЭЯХЪЧХЬЭТС
ЮЯПШЛЖХТПФЯХТЧХЮЯЭХЪХЫДЧЫПЯЧУТПИОЫЭЪТПТЮЯИХЬЫРЭТОТЪХТЧЫЯАЫЧЪЮХСТ
ШЮЯЭАЕЧПЯТШЫРЭТЦЧТХЮЬШЯЧЫЩЪРЫШЫПТЫЪЭФЩЯИПШЪХЯЧХЧЫЯЫЭИТСТЭУШЭЮЬШХ
ПЪЭАЧВЧЭХПЫЦЮЯЭХДЫЧПЫБХГТЭЮЧЫЩЩАЪСХЭТДЯЫПЩАРЫСЪЫОЯЛЕЧЮЬЭЫЮХШЫЪЬЭ
ЫСЫШУЮПЫТФЪЯХТЫЯПТДШДЯЫЬЭХТВШЪЮШАУОАХПХШЮЬЫСЫШРАЮПЫТЩАЧРЫЮЬЫСХЪА
ЧЬХЯЪАХЮКЯХЩЮШЫПЫЩЫОЭЯХШЮОИШЫЧЧЭХПЫЩАЮЯЭХДЧАЬЭХЪХЩТРЫФЧЫЩТЪСЪЯЪЫ
ВЫФЦЧЬТЭТОХШФЯПТЭУТЪЪАЛЩЪЫЛЭТДЙХПЪЧАФЩХДСЫЩЪТЯЮЧФШЫЪЫЪЬЫЕТШПРЫЮЯ
ХЧЫЯГАРТЭЮХЩАСПЮТЭПЪЫОЯЛЕЧТРЫВЫФЦЧЬЭЫЕАШЛОХЯЙХУШЫПЯЙЮСХЮЙОЯЛЕЧЫЪ
ЧШХЧЪАШСТПЧАХПТШТШТЦЬЫФПЯЙАЭСЪХЧЮЯЭХДЫЧЮПЫХЩЫСХЪЫЧХЩРШФЫЩЬЫРШСИП
ШЪЩТЪЮШЛОЫЬИЯЮЯПЫЩЮЩТЛЮЬЭЫЮХЯЙЮЧФШЫЪПИПЧЧЫЩЬЫШЧАХФПЫШХШХЮШАУХЯЙА
СЫПШТЯПЫЭХ

(b) Расшифровать текст:
ЙТЫЧНРКВАЦЛЬЫЭНВУЕАЫЖСЫЩНЖРЫКЗЫТШФЭФЦАЮРЕХФФГЭИБЙЭЖЙШГЭУЙААЧЕКАЧ
УЙФБЭШКБЦАЬЗУЧГХАЪВВУВМАЪФЕКДДЫУОВЧЬЪКГЯЖБЗЛГЦЛИЦАЬЗУЧГХАЪВВУВМА
ЪФЙРЖКЙЙБЫЕЬЭХЧЯЩЪСХГРЫЙДЭЮЮНЮЪПЖЛЫЭПЖЦШЦЖНЗБЭЩЙЛВВЩИТЖБРКХАЦЫЭН
КЯУПКЦАХЪСАЧЪАЦЮЙЭЖЖАЧУЙФЖШЭФФБЯЪИЦАЕУЙРОКШЖЖГНШДЧПЯГЪЙБДЗЪЦЫЭЗЭ
ЗАЪЭВЦЫГЪЛИЖГЦЭИЮЪТЭКЪЦЩИУХЪРЩУЦУЮЬШЯАЦАЧПБРКХАЦЫЭНКВШЭТФНЦЗУЧБЫ
ЪУШБЦЭЬБФОИШЧОЪЖЙДЮЮЦПБГЭЖЬЭЕНЫРЖУУЕШАБЩГЧБВНЭХЛЬУГКЩЭЩЕЗЧАЧЭШЭА
ЧЭТЧЯЭВШЧБЫАТШГЦАСОЧОЖЦФЧЫЭИЫЭРПНЮЧОЖМЧЧГЕНЬИЖИГЮОШАПДДРЗТВВЧЖТБ
ФУККВЧЫФФШДЫЕЙГЧУПЦЮФМЖИЖЩПЖХБФУЗХБЯРЫУЭВЩДКИАЫЖЭШХЩЕККЧОЖНВЪЬКБ
ЭАЧЕЙЫВЖЙРОКШЖНЯЦЩЪУЮОШУШХГУГНДНРЫУГАНЕАБЯХВХБЦШЖОДНШПЧБГШАСДЭЮП
НЮАЬФЧЭАХЯНЕАМУРПЮЩГУЧИЮЕКЖЬЩИПБЯЗАУКЧЭУХШЗШЖИИЦЬЗУЕНХЭЧДЪТЪУЮЪЭ
ЭЗОБУЙЧПЙЭЖЦБКЦЭЧШЮРЕЦХЪШЭОВГЭАНАДЩЪЭФАЫЙПХАЦЯЦЫЮХГТСГЗИЖДЬУЪКГЯ
ЖБЪБЭЩЗЗЛВААФДФРГБШФШЭСБХШЭЦЭАЦФПБВТЕКЖЭЖЩТЖДЗЙЬЫДОИСБДЮЬУФВЩЫУД
ДЫАПБДНЭЬЕОМКГЛЬРЩАЮЯРЪЦБГЭЖТЫЪВКУФЕЬЗУЭАУКБЯДЮРПЖБУЙБЯАЬЪКЮОУПС
АЧЪЖПЪЭЩЙБЧАЬКЧБЙШУСДДЩБФБВЖЗУЮАСЭТЫЧЧЖКВЧЫЭСШЯУГУДОЧИБЫФШЖЗАБЩП
ЧЫГЩДТБРШЭИБФЩИНЮЬНЙЬШГХАЦЕВЦЙБЫЩМЭИЕОЧЭТЧАЧВУЯЧШЬТЕГЭГЙЮЮРЕФБГЭ
УРЯЭЩЗУЯЭЮЗХЫЕВАРДГУЬКЕОЩЬНАЕЬЭЖЧАЧЪЦЫЭУЙКЦАЫЖЗАГШПРЪДЩДТШБРЕРАА
НАЙЯАРЛФГЮЬКЗБАЬКЗЫЭЧЭТХБЩВУШГУЪТБЮХЛМЯЪВЭСХЪПЭРДДЩГБЭАХЖИЧДЩЫУЕ
ВРЩУХЭЬГШЩУЬЖЭХУЫАТОЮНЙЧГЧВГЦГЧПВУЫЯРЖЪБДШЖЧШЮМЖРШЧВКУЪЮРПРХЯРДЦ
ЭВЖКШСЬЬЭЖШЯРЗХЫЩШФЬЕАУЛЧХЧЫЮЙЮАЧЭТХЮЩАЪВАПЖМГЧШАЪЩЪТЕБЯАЬЬКЮЭЬФ
САЧШЭЦААЬЕЗВЭНДХКЯЮЦМЧЕЧПНХАЬКБЭАЭЖХЖРЪАЧЮЪЩЬНААВЭЦЕФЩАЖШЩПЭОДДН
АКЮРМЖЗПЮЩИМЦАЫГЦПФЮЭЙЫЯРЕНЫЪВЙУЕЙЬЛЦЕЯЩЪНЮГЗДТШДОЖЦЕЯРЭФБДРИРБЗ
ЩКШЭЙЭЭТЫРУЙРБФРЙТБГЭАЙЖЗЧЖОЖБЦЩУЮГУГНДАФКНДЕЧАРЫЕ

2. Разложить на множители числа:

(a) 590085177369705579566481006949

(b) 1169638049300293734971050578901636496268036348333083113974821

(c) 825042333769779603617690988237522661222908296793914447826539958739308759145382572558700729

(d) 919976564194124109860277208119863767052793655558567929874557123989807995993947043975029888733177369919232715969630702051

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 365292423166730264404437340304653076980038634423154381655404553727323566138 41$
   - $e = 3$

   Сообщение:
   - $M = 17943945178309063034495900184580212129219460658859895719822735832712798114 94$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 180591696326028489989757562213918992517$
- $q = 22623108122313464744885393179979991023$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 648129053506041058233976560163812099651729139583625557896776699855162804853 8$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 335207352076550859240546971905688559521$
- $e = 5$

Зашифрованное сообщение:

- $c = 263404490759713119532329989114623468271$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 220320246328954028072763168880385056091$
- $g = 218492124622128384412522883198761215975$
- $y = 436358983729223649255145727777120491 43$

Секретный ключ:

- $x = 986015652350764202688671196172611493 58$

Сообщение:

- $M = 424228793905020425879618876677458290 43$

Использовать следующий случайный параметр для создания подписи:

- $k = 173206206264978567747752686850271376839$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 186984012735698018276786930395006740331$
- $g = 982010635224247807483172655699963778 19$
- $y = 579923729605802061315477112405518697 02$

Сообщение:

- $M = 837277550398159683457992026200894975 85$

Подпись:

- $a = 245516929837058035721357934860237529 15$
- $b = 101882005820458630652801876037928470220$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 773$
- $g = 188$
- $y = 44$

Сообщение:

- $M = 221$

Использовать следующий случайный параметр для создания подписи:

- $k = 697$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 10$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 91

1. (a) Расшифровать текст:

ЖЗСНСЖСФПСОБДЛЕЮМФХЛШСХЕСУИЩЛФНУСПРЮМОБДСЕРЛНТУСЗСОЙОЫЕДУЛРЪФСХЪ
ФЦДСОИИУКЗУЙПИРРСТСФОЦЫМЗУЦЙИФНСЖСФСЕИХНСОЛХЮШСЪИЫЯЦФТИХЯХСФСЕИХ
ЦБЗИМФХЕСЕХЯРИТИФИРНПЛЪХСАХСФЦЗУЯКРЪЛХЛКЕСОЯСДЭФРЛХЯФФСШСХСБАХСК
РЪЛХЪХСИЙИОЛШСЪИЫЯЪХСДПЫПЛУСРСЕШСЗЛОНХИДИЕФЦПИУНЛХСЕПИФХСРИЙРЮШФ
ХЛЫНСЕТСЗУЛИМТУЦФИУИЖНУСЕЯПСКНЛТИОТСЪИПЦХЮСДРИМХНСЖСПРИРЛФТУСФЛО
ФХУЦЗСПЦЗИУЙЛЕФЕСИРИЖСЗСЕРЛИТСХСПЦСХЕИЪОСРФЗФНСМЦФПИЫНСБЪХСКРБТС
СТЮХЦИИРУЕЛСДЮЪМХЮОЙИЫЯПИУКЕИЩЕФНУЛЪОЕДИЫИРФХЕИХЮОЙИЫЯФПЮПДИФФХЮ
ЗРЮПСДУКСПЫЕДУЛРТИУИПИРЛОФЕОЛЩИАХСХИДИХНРИТУСМЗИХФНКОСРФХЛФРЦЕПР
ИУЦНЦЕЮПРИЗЗЛХИФХЛФЧНЩЛБЛКЕСОЯНСЖЗШСЪИЫЯСХЕИЪОСДУЗСЕЕЫЛФЯЕАХЦПЛР
ЦХЦЖСХСЕДЮОУФХИУКХЯИЖСХСХЪФСХТУЕЛОФНЛЕРЦЛЖРХЯЛЪЦЛКФХОИЖСФЛЖСОНСБ
ЕУЦНШТСТУИТСУЦЪИРЛБНСПИРЗРХЫЛСРРРЛКЮЕОЖУЛДЮЗОФЦЫИРЯРКЛПЦТИХУРЗУИ
ЛЪФНКОСРЦЕЛЗПИРЗСДУСТСЙОСЕХЯННАХСЕФДСЖТУЛРИФТСННСПЦЗИОЦФПИБФТУСФ
ЛХЯЕНСУСХНЛШФОСЕШСДЭФРЛОИПЦЪХСТСФФСУЛОФФОИНФИИПЛЕРЮЪИПИЖСЛЕРЛЖРХ
ЯЛЪТУСЫЦДЮХЯПСЛПФИНЦРЗРХСПЛЕРЛЖРХЯЛЪЕЮФОЦЫОПИРФСЕРЛПРЛИПЕЮХУЬРПИ
РФЕСМИЗЛРФХЕИРРЮМЖОКЕЮЛКЕСОЛХИЖСЕСУЛХЯФНКОСРПРИЪХСШСХЛХИОИНФИЛЕР
ЮЪКНСОСХЯЛЙИОИХИЪХСДТУЛХСПДЮОФЕЛЗИХИОИПХНОЛФПИБФТУСФЛХЯХСЪРСХНТС
ПЛОЦМХИТИХУРЗУИЛЪЪХСАХСЕЮКХИОЛЕЮФОИНФИИПЛЕРЮЪИПТСДУРЛОЛФЯЕИОЛНДИ
ЗДУРЯРЕСУСХЦРИЕЛФРИХСРЕФТСДУРЛОЕЮИЖСЕЮУЦЖМХИСРЕФЕУЮОСЕЮИЖСЕЦШСЕЗ
УЦЖСИЕХУИХЯИЛУКСМЗЛХИФЯПЮЕФЦЙТСПЛУЛПХСЗСДУСИОЛЗИОСКНСОСХЯФЕСИЖСД
ОЛЙРИЖСФПИБФТУСФЛХЯЛЗСДУСДЦЙКНСОСОЛЕЮИЖСДСЖФРЛПФОИНФИИПЛЕРЮЪИПЛФ
ПЗСРИЖСРИСШСХРЛНРЦИФОЛСРЕФТУСФЕИУОЛХРЪХСАХСДЦЗИХТСШСЙИНХСДЦЗИХЕЗ
ЦУНШФПИБФТУСФЛ

   (b) Расшифровать текст:

ЮЗЕЫЦХКББОЭЖШБТЧЩИАЬЮЪОЫФЮЪВЭСЭЕРИМУЖЩЖОВУЧЫОЭЖЖЕЪЛБЧБХЪЗГФЕТГЧА
ВШНЯВФЭНЗОСЭКСАПТЗЪГМЮБИЩПСЛВЕЭХРСЭШЫАИЕПСКЯЦХФВГХЕБКЕБНЭЩНЭЩЮЬГ
ЬОШВДБЛЫАЫШНЮЪГГТЪКГЕПСЗГЧШБГАДЬАУЮФВЪАЕШАЬЖАКХШЫАЧПЫЕЯБЦХЕЩАЬБЪ
ЭЧШЬЙГХПАРЪАЧЮЫГФПБЙБОЫЫАМЕШЦЭЗОЦЮГМЫВМЗЕБОЮГЫЮТТЕЯЖСЬАМЮТСЭАПЦХ
ЙДБЪГЙЖЭТЭЭЕЪЭЬЭЪЛЖОГЮДЩАЖЖЫФГЕЪЦШЯЖЧЛПЬЛЯЕШХЫГВШФЖЖЮХТЕНЖФАЭДБЫ
ВФУЮУЯЖЧЕШАААЬВИЖЭШЬЯРЭПТЖДГШБАЧАФГЯБЫБЭЖЦЛФШИЪЙНЫЬЪЮЧЭЭШБЫВЭБЩ
ПТУЕЩПЭАЪЯТЭЭГЕМХПААТБГГХФИАЖЭСЫВГЯПЭЬВЕЬЛЛБШЧЧЫГХШААНПЪХЩЗДЕЬАЗ
ШФБЕЪЦШФЛЕЙФШБДБХЮЙЗОУЕГЗЧМЛЙЗГШЗАЗШПЬЛЖВТЭЛЖЯШВИЭЩИЫБКБЪЮРЪАЖЪЖ
ЪЦШФЪЭАМЫАЩДЬЫАЦЛФШИЛГСФЭЧЕЖЫАЛБЧХЙМДЬЭЖШБТЧЖЦГСШГГФПБЗГЭШЩЙЗХШЮ
ЕГЦХФУЧЮЫЭЪЖШЫВЖЕБЧЛВЯЪМХИГЭЩЮББАЧЛБЩШЬМДЭЭШУЬЫБОШЕЭЪТЭЪАЫЮЮЪЧЪХ
ХЫГГЭЪАЭВШЫЖЫЫМШНЖШЛХЖЯБХЮРЪЫЩЮЬВЮЫВИЭЭЧБЪГЫЩЫЭМЫИЫБЧЪХЯГЪЕЖШЯБИ
ЧГГЖЕШУЬЦЛФШИЪЙСБКГАХБГЦОЦГДГЮИЙАБЦШЫЖЖБЦШВЭХНЮГГХШОЖЗЭЪЛГЕБЬТВГ
ЕШАЖБХЦХЙЗБСЛВНШМХГЭЮЫЪЖЕБЬЪАЮБЛАЛЦБФЪЖШЧМБЗГЯЧОПЗБЗВЖЖЮЭЗААБЫМЕ
ББПЬЪЪЭЭШПЗБЧЛЕЪЧШЦААЧШЪИГЕФЮЫГЙЪБКЧБМЭАЭЯЩХИЗБЪЫЭЯДЧФИВШЦЮЫИАПФ
АЧЫЬМЙЦОЫВИРЯЭБЗЪИЦЯИГДМХСЪАТШИЖВЪЮЙЗГЧХЕЭСЩАЪЭЮБХГГХПЪЖАСЛШДГЮШ
ФЖЮКПЫЖЧШФХЙАЫСЯАЖЭТЬЖЭВШЯЬИЕЫТКЧБТАЛЯЫМБЗГЯЧШПЗБХГПНЫПШЗЕББЭЭЮЛ
ТХАЬЯПЭЭВЫЫГКСЕПЪЖЗБЪЛЭДГШШЙКБОВЖЗЖХГПНШЧШЕЕХШТЩЪЪМБВЭИЧБААПЫВЪЬ
АЧЛНДБЬАЙЪАТЩЪЖШЛЛГЭВШАЮЪАЕЭЛЖЭСЫВГЯПЭЬВЕМШЬВБЧЬЖЗАПУЖЗБХЪЛВШОЮЩ
ЭЕЖБЦАЬШВЪЬЧТСРЯЫЪЖЪВФЪЬУШБЫЯЖЩЭШЩЖМШЦХСЪВШВЖАЭЭХДБОЫВГЭГЫБЛЫЧЬМ
ЖВЛПЬЗГЮШЦЭВЫТЪВЧЧЪГЫЧДТЫАЖШНЮИГХЧТЖНЮМЪЖБАЬГЯЩОЯБФЭДМШЬГЯБАЭЬХЕ
ЗБВБМБКЕШМЮЮЪАЧЛДМЕШНКГДЬЮЩГСЫФЭАЮШБФЖВЪЮЙЭЮТЧЛБЮПЭЕРЬФЮДЪАОЭКЦЕ
ИИВЭФПФЖЗХПЗГЧДТЫАЖШНЮИГХЧЭАЫАПЮЯЪГЧТЯЗДПУЖЩАЭВИГЯЪСЖЗАТЪЖЗ

2. Разложить на множители числа:

   (a) 109783445428794939191772773244501

   (b) 1144417871857873796584850915047203330074861613079152256189937

   (c) 1244297118277150336851852584818607439027419282121239095382867652298009216066998939285746197

   (d) 22688199209297427719636606267359466306424061132972167961164349402676899123870595854483795057870858917182970395232026828 17

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 630050427057802740873854380564155985494515238395793917105823201306001192780 73$
   - $e = 17$

   Сообщение:
   - $M = 473461190497782208000714706650370787363650706292935369162626041442990901442 05$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 333803710358483294326349958297589644859$
   - $q = 286075597683639400405482056150113816919$

   Открытая экспонента:
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 224445432010800105693457439571739612945772989416723560967875116437843368574 76$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 142605330149819306068056929216898054479$
   - $e = 5$

   Зашифрованное сообщение:
   - $c = 985452045046031594099541230399539081 13$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 201864285112238917236510673099106456983$
   - $g = 183561941894203600437571751363521990766$
   - $y = 171419559961049787176677633508025838469$

   Секретный ключ:
   - $x = 100720223484868947056826828795494988612$

   Сообщение:
   - $M = 338148389505798837540531713338615468 90$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 567320010657164461476162324431407355 65$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 174141246361461715520280478809363617881$
   - $g = 357849292257002642307963804687741 2856$
   - $y = 153891479267108244490114281846396261686$

   Сообщение:
   - $M = 735730507655479057781704680063423440 35$

   Подпись:
   - $a = 383599311775834652193672287300747666 78$
   - $b = 576345262550130673218240136339456354 97$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 599$
   - $g = 265$
   - $y = 39$

   Сообщение:

- $M = 325$

Использовать следующий случайный параметр для создания подписи:

- $k = 293$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 8x - 10$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 92

1. (a) Расшифровать текст:

БЕЯШААШБЕИБЧЫЮГЪЖЯШШЕДВГЫВШГХБЯЖЧБФАБЯДЮЖКШВГЫАЮДЪВГШГХААБШБФНДА
ШАЫШЫЯГПЫХАБХАХОДЮЖЛЮЯШАЕШГВШЮЫХШШБАФШЪБХДЭБЦБЩШЯАДЕХВГЫЪАЮДПЯАШ
ХДШГЧШКАБЬДЭЮБААБДЕЫЫДЭЪЮКЕБШШГБЧЫЕШЮЫЭБАШКАБГЧОФЖЧЖЕШШДКДЕЫСАБВ
БЧЖЯЬИБГБЛШАПЭБВГЫФХЫЮБАДБДЕБГБАОЕХБЫИГБЧАОИАШФЖЧШЕЮЫВГШВЕДЕХЫЪЧ
ЖЯЮДХАШЩАБДЕЫЯЕЖЛЭЫАБЬАШДЖЯАШХЮДАБЪААГХЫБФГЪЯОДЮШЬБЕЙКЖХДЕХБХЮКЕ
БЮСФБХПЯБАШДЮЫЛЭБЯШЦБЕГБАШЕЫКЕББАФЖЧШЕААШШДЯБЕГШЕПЭЭАФЮЩПЯБЮБЧБЦ
БКШЮБХШЭКЫДЕБДШГЧШКАБВГЫЪАЮДХЕБЯЯГПШЫХАБХАШЫГШЛЫЮДБЧАЭБВЫДЕПЭФЕС
ЛЭШЭЭЯБЩАБЭГДАБГШКЫХШШВГБДГБЧЫЕШЮПДЭБЦБФЮЦБДЮБХШАЫВБЭЪЮВЫДПЯБЯГП
ЫЫХАБХАШЭБЕБГАЛЮШЦБДЕБЮПЖФШЧЫЕШЮПАОЯЫЕГБЦЕШЮПАОЯКЕБАШДБЯАШХЮДПХЖ
ДВШИШШЦБЫВГШЧЮДПКЖХДЕХЯАШЩАБЦБДХБШЦБДШГЧЙДБХДШСЧБХШГКЫХБДЕЫСЯБЮБ
ЧБДЕЫЫЮСФХЫДБЛХФГЫАОЯВБЯЫГЫЮДХВШГХОШЧАЫЯБШЦБХОЪЧБГБХЮШАЫЫХАЭЖЪЯЫ
КХОЦБХГЫХЯАШЪВБШЧЫАБЭДЭЪЮЯАШРИВШЕГАЧГШЫКАЧЮШЩЮБФОЯАШВБДЧЫЕПЕШФВБ
ЧГШДЕЧЕОЖЩЫФШЪЕБЦБАЭЪАЮШЭДШЬЫХАОКЖЯШАЕЭЫДЫЧЫЕХИЮШФАБЯЯЦЪЫАШВБЧЭГ
ЖЮБЯЫЛВЦШЦБВБЧЪЯЭБЯЖХДЫЮЫДОШЦБГБХАОВЖДЭЬБАДШФШАЧЖЯШЕДЧГДЭШЕДДЮЫЛ
ЭБЯФОЮДКДЕЮЫХКЕБФИГАЫЕПХДШГЧЙШКЖХДЕХБАШВГЫЪАШААБШДЕЮВГБДЫЕПЪЛХФГ
ЫАЫЧБФГОЬЭБЯШАЧАЕДДБЦЮДЫДХБШЬДЖВГЖЦЫГШЛЫЮДШЦББДХБФБЧЫЕПЛХФГЫАВГЫ
ЛШЮЭБЯАШБАЫЪНХЫЮЦЮЖФБЭБШДБЩЮШАЫШБЕБЯКЕБДЮЖКЫЮБДПЯШЩЧЖАЯЫВГЫЪАЮДК
ЕБФОЮЭГЖЦБЯХЫАБХЕЫВГБДЫЮЯШАЪФОЕПБВГБЛШЧЛШЯФЖЧЖКЫБЕВГЫГБЧОАШЪЮБВЯ
ЕШАЫДЭГШААБВГБДЕЫЮШЯЖЫАЛЖДДБГЖЫГАЖЯАБСБЕАШЦБВБЮЖКШААЖСХЭЮШХШЕШШЦ
БХЫЧШЮЧБДЧЖБДЭБГФЮШААБЦБДЯБЮСФЫЫБЕХШГЦАЖЕБЬЮСФХЫЫХШЮЫЭБЧЖЛАБЫЪХЫ
АЮДХБШЦБАШДКДЕАБЦБДБВШГАЫЭХДЭБГШХОЪЧБГБХШЮЫЯБЦВШГШФГЕПДАЯБСЭХГЕЫ
ГЖДАШЕШГВШАЫШЯБЩЫЧЮБЕХШЕАВБДЮААБШВЫДПЯБАШДЯШАЧШЕПДЫДЕГДПЪЦЮЖЛЫЕП
ВШКЮПАОШВГШЧКЖХДЕХЫДХДЫЮЫДБЬШЦБГБХАБЬЫ

   (b) Расшифровать текст:

ЪЬДЬЗЗЛВЮВАЯБАПЭТЩДЩЖЬЮЧОЧЮЦЮРШЮВЕБЕОЫАЙЪЭХЯПЭЧЮЧЙГУЯДНВЛВАЮЕЫАА
ОАХХЯЕЪБЩЭШЭЮГФВМЫГФВЕФМЮАГЫЯГЛБВМЮКЪЭЦХЛЖГХВЩЗЛУАНЭБЭАДЧЭЦИОАЛЙ
ОПРЯДХФЪТЭВФВЮЮЗЙИАЩЭОЭЬЖЯРАСЦЭШБЯЬДЗГЬЮЧОЯЮЬОЗГЪШЬЛЧЯЯЦТЧВЩЭЕЖВ
БААГЪАЪПВШААПОШЬЪЗЧШВЧИЭЖЦЯВЪЯЦВВЯЫХЪКЪЮИЕПЭЫВФВЕЕЯЮЕЬГУЧФЪЭЮНЖЦ
ИЫЪНЬЖЫАПГАЯХЛЩЮАВХЭТЬЪЙРЭЫЯРВХЯЯБЪАЧЭЯЕГЫЧЯЪАЦФЗИШИЧНЬЧЭЪКИВДЕЯ
ЭФЦЭЮЪФЮААГШУЯЗИНЭЪФЧЧХЧНВГГААГЭУАДЩГЖДЛШФАВЕЧХЬЪЗДГФЙВЧГЩФКЭУЮД
ЩЭЗАВЕЖУЪГЗЫЦЮРДГФЙВЧУЯГРЩАПБВЗАДЖВГФЯВЛЧШИЕПРЭЭЯВШЮВЕБЕМЯДЯЪЗЬ
ЪЯВШФЯПСШИБЛЧВЯВОАЮУГЯГХФАЗДШГЯПРФХРХЯТЯВЕЖЬЯЩЯВХЗБРШЗЦФЙКЭДЭЛДВ
НБИЗЪЯЮЕЩЮТВШЮЯЯВРМШЫБЛЧШВБЛЩЫЦГЯГХФАОЗАЯХЛВЗЬОКЭЪЯЙВЕХХОЮРЫШЮКГ
ОФЭБЪЫВЮВАЮЮБРШЗЦФАГВЯФОСЯЯФПГАЩДЩГВУЧПЧХЬЪЗГФДККРЕЭАЕКВЯФНЭЙЦЫП
ГУХЬКЪЮАЪОВЭЯЮРБЮЦЮРЭЧДЮИЪЭЩРРЧШХЧИЖАЦЦЕБВЦШКРЕВДННШЮКЯЦАЩЯЛЦБГВ
ЕЫХЮЯЛШЮУЬНИЦЯЬЕЧЬШИЗГЬЫЖПВХЯЯМГФЯКВАЪАЕАМХУЕЕЖЪШЭВБГЮЕТГЭЦГЗГЫН
ЬЛЖЫЯФЯЪИГОВШЮВЬДАЯДХФЪТЮЧЯЬУЬЯРЧГЧЧКБХЮЮКЪЭЫЪКИЫЩЯХЪОАЧПАОВДИМШ
ГДЩДАЯГВЦЬЯЭЕЗТДБНЭЭЯГЮГУДЪОЯАЦЯКЪХБГЗВШЦФЛЧБЦЗЙГШЖБНЪУБЧХЪЭЩЗЕБ
ЮЬЧАГЮВБОЪЭЩЪЯЖХЖУИЭЧЫЪТБЮЦЮРЖХБЦУИЬЦЯМЕШГЛЕАШААБЧШВЧИЭЖДЯВЦЮВОК
ЪСЯГЩДЮУДЛЕЫЩЮКЪУДУЕЗХЬЪЙГЦЦДЮРВНЪЯДАУЦРЫХЬЮВВЮТАБЕШГОЯЩАДХРЖЫМК
ИЯАЩЬМГБГАЖЗХЯЬКВЛЦБЛШЮХЪПЪЯЬЙЕГБГЯЛЧШЬЪОСУЬШРЖТЦЭЩЭЗЬЧГЭВУЯЛШЕД
БРШЗЦФЛЗХЗВЛЩЭЯЫАГТЯВЕАСЦЦКРЩХЦЩЯЗГАПЪСЦФОБХБДЕЦАВЬЛШЮХЪПЗШЯДМИБ
ГЪВШЮШЯВШЮГЧЮЪТМЬРДФХЕПЩЫАВЕБХБЪОЗАЖВБЭТЦЭЕДЮУЧОЭВНЗЛЗМЭЧКЖВБЪЗД

ГФЙВЧФЬЩКЯШЭЧКЗЮГЙОЕЧУЩИЭШЯГПЧШЬЪЮЗОЙЬКНВЦУЙЭЫДЧПШЮУАНЭЫЩЮКЪТОДР
БШЮЕПИЭЦЮЛШГВЬДЗМИДЛЦЮТВБГТЬГОЧЮЦЮРЭЧТФИЪЭЩРКЪБЫШРГФЮЬЛЫЗГАЮГЭЦЮ
ЕЖЮЧЭВАЗДФОЗТЯФКЭЬЯЪЮРЫЩГИЭИЫАЙЖЬДДКРЬЦЯОВЮУБНЭТЦЭЕЯБЭАДЧЭЗЕЕДЮВ
ДЯЭЫЩБ

2. Разложить на множители числа:

   (a) 701207631021787459106156246009

   (b) 10332623641166300379519314997888135777434050657998222703434 43

   (c) 10402116436894962101078508631456784511634111417713362888090544706806864392170141234800172 87

   (d) 15414421460249337693173092713698378673118027938142314260557528779402044762522105609620439665438850505404551787386594673 09

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 491172890392549792705571827215943066459085726839236025557871196796958927858 37$
   - $e = 257$

   Сообщение:

   - $M = 48928390422154986579969624413589142857142369626320383111246450379841235098674$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 300189572861144062826285060231689079171$
   - $q = 319657095106716314700137427457211791523$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 736481379233868368725516251691949754604212012245150331198244035840248915628 7$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 200433388398740985444451653421321162523$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 124179963140809434377928849941661554999$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 22774374523703065166391440360739111021 7$
   - $g = 151076897906963589945958495743334425298$
   - $y = 20186836952921511390019755138476157838 0$

   Секретный ключ:

   - $x = 947824497900105807790905991205710211 50$

   Сообщение:

   - $M = 19605490408165649630558394361559463947 9$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 18173368274196698458832084224250591805 7$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 24386227377470966578992229677995873089 3$
   - $g = 46270795319665208474179300765963003723$
   - $y = 11373560298948957126122615262462 4619372909$

   Сообщение:

- $M = 20601826874810111032670848994924196957 4$

Подпись:

- $a = 17955486995287355287889675182031216748 9$
- $b = 15153612451960775840983070041607601378 7$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 683$
- $g = 471$
- $y = 392$

Сообщение:

- $M = 369$

Использовать следующий случайный параметр для создания подписи:

- $k = 81$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 11x - 2$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 93

1. (a) Расшифровать текст:

ЗИЭЬЖЙКЖИЖЮЕЖЙКАЪЭЙКФЖЗЖЪГЭЕААЗЛЫПЭЪИЯЕЭЙГЙФЗЖВИЭЗЖЙКААЪЕВЛЯДАПН
ЖКФАЖПЭЕФЛЪЮГЙЪЖЦЙЛЗИЛЫЛЕЖЕАЯПКЖЕЙЪЭКЭЕЭЖКВИУГЩУЭБКБЕУЪЪЭИЭЕЕЖБЭ
ДЛЗЖЙГЛЮЩЭЗЖГЛПАЪЗАЙФДЖЖКЫЭЕЭИГЖЕЬЖЪЖГФЕЖАЙВЛЙЕУДЖЩИЯЖДЪУЗИЖЪЖЬА
ГЪЙАГАЙЛЭЫЖИЖЪЕЛЙВЯЪЭБЩЛЬКЖЩУЖКЭОЫЭИЙАДЗЖГЛПАГАЯЖИЭЕЩЛИЫВВАЭКЖПЛ
ЬЕУЭАЯЪЭЙКАВЖКЖИУЭЙЖЬЭИЮАКЪЪЭГАВЖБКБЕЭЪЙАГАЙЭЫЖИЖЪЕКЖКПЙЯНЖКЭГЖК
ЗИЪАКФЙЪЫЖЙКАВЗЖЗЬФЭАЗЖЙЖЪЭКЛАЪЕВЛЯДАПЪЯГЙЙЖЩЖЦАДРЛПКЖЩЭБЕЭЩУГЖЙ
ВЛПЕЖЖЬЕЖБАЪЕВЛЯДАПЖЙКЪРАЙФЗЖГЕУДНЖЯАЕЖДКЖКПЙЗЖЙГГЯЕДАЗГРВЛЯЗЭИЪ
ПЛГЕПКЖЩЖЕЕЭДЖЫГЕЙЗЖЬЙГЛРКФЪЙАГАЙЭЫЖИЖЪЕЪЖЯЪИКАГЙФЬЖДЖБЕЭЛЙЗЭЪЕА
ПЭЫЖЪУЪЭЬКФЖКЗЖЗЬФААЛЯЕГПКЖЪЖЪИЭДЭЭЖКЙЛКЙКЪАЩУГЖЛАЪЕВЛЯДАПЙЖЪЭСЕ
АЭАПКЖЗГРВЩУГЗЖЬЯДВЖДЖЕЬЖЫЬГЙФПКЖЩУГЖЩДЕЛКДЛЮЭДАЗИАЙКЛЗАГВЕЭДЛЙЬ
ЖЗИЖЙЖДЕЖАЪЕВЛЯДАПЗИАЫЖКЖЪАГЙВЕЗЬЭЕАЦЖЕЕАДГЖЕЭЙДЛКАГЙАЩЖЬИЖЖКЪЭП
ГЙЪЖЭБГЦЩЖЗУКЕЖБЙЖЮАКЭГФЕАОЭЙГУРФКУДКЛРВЩЩУЕРАЪЯЬЛДГАЗЭПАКЖЗАКФЙ
ЖГЖДЖЦВВЖККЖЫЖДЖЮЭКЗИЖАЯЖБКАЕЭЙПЙКАЭКЖАЖКЬГЙКИЖЫАБЗИАВЯЪЗИЭЬФЙЖГ
ЖДЖЦЩЩДЗЭПЭБЕЭКЖЗАКФКЖЗАКФНЪЖИЖЙКЖДАЪГЭЮЕАВЖДЬГПЭЫЖЮЩУГЖКЭЩЭЯЗАИ
КФЗГРВЛЙЗИЖЙАГВЖДЭЕЬЕКРЯПКЖЩЭЬЕЬЭЪВЗИЖЙАЬЭГЪПЛГЕЭЗЖВДУЕЭЪЖИЖКАГА
ЙФАЪЕВЛЯДАПЕЭЩУГЗИАЫЖКЖЪГЭЕВКВЖЪЖДЛЪЖЗИЖЙЛЖЕЯЗЛКГЙАЗИЖЩЖИДЖКГПКЖ
КЖЖПЭЕФЕЭЙВГЬЕЖЭЪЙАГАЙЭЫЖИЖЪЕЛЪАЬЭГВЖЪИЙКЪЖЙЪЖЭЫЖДЛЮЕЖЯЕПКЖЕАПЭЫ
ЖЖКЕЭЫЖЕАЬЖЩФЭКЙЗИЭВИКАГЙЪЖАЪЖЗИЖЙУАЯЪЭГИЭПФЖЙЖГЭЕУНЖЫЛИОНВЖКЖИУ
ЭВЛГАЕЗДМАГЖЪЕЗИАЫЖКЖЪГГЙЖЪЭИРЭЕЕЖЖЙЖЩЭЕЕУДЖЩИЯЖДЪЖЪЙЦЕЖПФЪЙАГАЙ
ЭЫЖИЖЪЕЕЭДЖЫГЯЙЕЛКФАЕАВВЕЭДЖЫГЬЖЫЬКФЙПКЖЩУКВЖЭЩУГЖЪЫЖГЖЪЭЭЭДЛЮЖП
ЭДЩУЭБЕЭГФЯЩУГЖЯЕКФЕЬИЛЫЖБЬЭЕФЪЖЯЪИСЙФЖКЖЩЭЬЕАЖЕЛЪАЬЭГАЪЕАЫЕКФАП
ВЖКЖИУБЪУКЙВАЪГАЯЗЛРВАКИЗАПВАВДЛРВАСЭЗВАЩЩВААЙЖИЪЙВЖЫЖИЖЬЯЗАНЕЕУ
БЪЕЭЭИЭЩКАРВДАПКЖЩУЯЕПАГАХК

(b) Расшифровать текст:

ГОЯЭЫАЭОЖШАЗЙУХЧЦАШФФФЛЭШОТЦГЧДСГЖВХСВВЙЭНИЪЧЬФЖСРАТГВЩДХЛГКАСБА
ФГВЙЦФРКИГЛЯЮАБФЭЭИЭЛБЩЮМЛФЧЗГШВЛЖВТЧУКЕОГШЖСУАОВЕЛЦРЙДЦЪЯОЕОФСА
ЧБЫЙЖЬЧЕКГЧОДЛЖСУНТЭРЦШЛИЭЛЮХЖИШАИМЗИЪУМБЛКСГЧФГШГВРАУАЛФЯНМБЛЭЧ
ГЖШЬФЩВЛБЦГЗИАЦИГПФЛМЪСАЧНЭДЙШЙЭЙЭКИВЛХФМЗСГТАЗВГЧЗВЛЩУТЪТЕЭНГИК
ЛЬАЙАЦЙЩОЧЧЕЬСАУЗВЛГШЛИЧЪСНРХВОВВПГРЙШКЮФЖГКИБЗГОЯРГВЩЭОНЪЗЧИАЕЛ
ФРОВЮЧДТУУЧЗЙЖФФЭГВРЕХЙЯНЭФМСХАРТАЧУБИДЛВЛЕАКЪУАЪЧЭОЬРУЧШЭГПГСОШ
ШАШТЖЩЩУЖЖШВФЮГЫВБТВЩЦЩЗАСЪШЦЧЮЧЗЖШФВФЯЭЛЙШЙМЛЭФЭЪРЬФНГЦНПЭРИЧСН

ЪЗЬЩЗЪШЕЗЦАЧЮИААОЬОДШФГЩЯЕВДЩНГУФНЖВЧЧЗЭЭКФМИРПЪШГВЧДИАВУНПНРРВЛ
КЯФБЛЛЪКАТИГДФОИГИДХЛГКАСБАФЯУЙДФЮОЖГИЭШАЦНДИЙУКАЗЛГКЧШААВЩШЙМША
ШЦГРЩСЗВЛЕЧЖИЙЕРЙШКБЦГВЩШКАВЗНСМЯЦНИНСЧАШМЧФЪЫИЪКВЩЮГИДФЖЭЛЛЛОЧО
ЦОУСШЬСГЪЯЧШАЦХАМЖИДЬФЮЩХАСОМЩГИЙЪЙАЧОЩЦГШЭГФУЛФЪЮОЧЖЭЧЭЩБЭШОТИЪ
ЧЕЧАЕКЪЛЗЧФБЦЙЖТАЮАВУЪРГЪЙАКАЕНАЧНСХАРВАОГВЗВЛДРВЦИЯБТЗФЯЛЗГЙЯЛО
ЖТЧЫИИШОЧТЪТЕШЦИЧЮЛРЪЮОЧМДЦАЧГАФЯТАВУЗТОЕЧООЖЭШНУАЧЛВОУСЭДФЭЪСЪР
ГЮЙАЧОЩЦОФНЧЛЙПКЕТАЧЗИШЪСМДЦЪНИЗВУЦЙЩЙЕЙЙЖЩЦЦАБЗНСИЪИГФМЗФЯОГТША
РВАФГВЗВЛЮСЙЩЩКОАБУЧХЛГЧДОНЪСОУЦБУЩИНСЛХФЭШСЩФЬБУЛОЕГТУБЖГХАКЭЪЦ
ХУОЗВГЛЬДФХОЬЪСЪОНГУЙШЙЦБЭЙЙЗФФХЙЩИЪЧААОИЛЩЧЙЭНРЧЧЧЙЙВЦАКГЧХЧЦЭГ
ТББЖИУЧЙЙЩФФУГЗЛБЛЛСРЩСЙЖВЮУАЦЛГХЙАЛЩУЙЮЫФЧНАОФФМЗОРРЙАЛУСМДЩХЭА
ЧТВЭИГМЦСЗГЛХФЙЗИЧШИЯФЯЛСЭЛЛЛИРУЧЧМБФЦФЭГСОЧНЧОЧТКГТЪУЩТШЕТГВЩДЩ
ТИИГШЭГКАСЮЧФГШЙЕМЧЧНЧФФСЙЧФЮУАВКГСЬГЧДОЩМЛЭФЭЪЭЧЧЕГДАШЭЪЭЭХОШЭЧ
ИОЖСЕЮДЖРШЩНЪЗЧИМУХВИЯИЦГЧОЩОЮФЮИСЪХЛЭНЯШЧЧШЧЗАШФГЩЯЕШНЭААФФЛЕЖТ
НЮЖЪУНПНРЧЮЩЭЭКЧСЬРЭДФЖИРФЧНЧЩРРНГМЧШЕГИБФНЧФЧТОЕНЕТАВОРЗЙШШЧЗВВ
ЛДУЙЯШАЗЦЗБЯОЬРСДБУИШЪЮЧГХГУОУЮЕШЕИХЕЙТЪИФНЮАУЕСИБЛЯЗ

2. Разложить на множители числа:

   (a) 736473735681174103009843887527

   (b) 68768225594015795472432613731429258086101879836249748949159 9

   (c) 167577635085860969384531315364109967540083545858685589546704032307427788211270814876759891 1

   (d) 142440347612634555815827452766741482489377713984348196630642285234182785252793337907436023149495549103233151786771897459 7

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 73369599454685907307356271447686764924380418710725016990873033172864119277771$
   - $e = 5$

   Сообщение:

   - $M = 65303382605522845137626281914363986651354437437272274452506528517183177084862$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 2890016015611646835123336467652423581 47$
   - $q = 3169656670136207855705747833692524475 91$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 6342526243762550180310612245416521098801066193492293871184444350639874986539 8$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 2346179501058632196529233404830414042 97$
   - $e = 257$

   Зашифрованное сообщение:

   - $c = 1491530050602177604601397699958613926 66$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 212610353747340069282471775428032445491$
   - $g = 133728097104959249755941043897464108209$
   - $y = 112024762448970154044633487805864232677$

   Секретный ключ:

   - $x = 14060090306892612273284814550791104297 4$

   Сообщение:

- $M = 172173729810205521874903690394670246409$

Использовать следующий случайный параметр для создания подписи:

- $k = 155560798080292557448750737580952210069$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 175978389707361507832093885730062468319$
- $g = 850426345229087505043263114049714022 19$
- $y = 102348476719665765949464318202889543297$

Сообщение:

- $M = 146843025534700641857418480291304239385$

Подпись:

- $a = 135564623977789938552855650659607422959$
- $b = 779622556685668187123075869177519269 53$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 887$
- $g = 184$
- $y = 87$

Сообщение:

- $M = 104$

Использовать следующий случайный параметр для создания подписи:

- $k = 555$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 3x - 8$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 94

1. (a) Расшифровать текст:

ДАЭОЬАФНГЭЕШЪЭХАЭАФЕКЬЦФФНГАЬЪЧГДАЭУЪЬБЧВЧЬЭЦЪЯЬЕЬЭЧЯАФЕРЧЛЧБЧДЧ
ЭОЬЕКЧЭЬАФЕРЯВАЦЯБЧГЯФПДЕЯАЙОЯЧГБЭЪЯЧВЩЦЧФЭГЯЮЧВЧЯУНЭАДБВФЪДОГЯЩ
ВЧЬЬВЧБАГДЯНЮФАВАДЮАДЬЕЦЮВОЪФЯАФЯЦАЭШЯУНЭФНЧЗДОЪДЮБВАГДЪДОГГЯЧРФ
БАГЭЧЦЯЪЫВЩЙЕФГДФАФЭФГЧУЧФЧЭЪЬЕРБЧВЧЮЧЯЕФАЭЯЧЯЪЧЦЕКЪЮАЧЫУНЭАЮЯЧХ
АВЩЦАЮЧЯЧЧДХАГДЯАЯЧШЧЭЪДАЕЯНЯЪЧФЬАДАВАЮЧЛЧЯЧЦФЯАУНЭБАХВЕШЧЯГХВЕГ
ДЪРВЩЭЕЬЪГЭЪФЭЪГОФАЮЯЧЪЯЧГЯНЧЯАГЭЦАГДЯНЧЯЦЧШЦНЪЯЧДЧВБЧЭЪФАЧАШЪЦЯ
ЪЧАБГЯАГДЧЫЪЙЕФГДФУЭХАВАЦЯАХАЙЧГДАЭРУЪЯАЙОББАКЭЯЧЩЮЧДЯАЗАДЧЭЕШЧФ
НЦДЪЪЩЦАЮЕЬЬЦФЧВОЮААДФАВЪЭГОЪЬАЮЯЧФЪЭГЬБВЭГЦАЯЧГЧЯЪЧЮЙДАЯКЪЬЩЬЪЯ
АЙОРФНГДЕБЪЭЪЪЩЬВЧБАГДЪФЩФЯГЪЭОЯАГГАУАРРЭЪЙДААЬАЭАЬВЧБАГДЪВЩМЧЩШ
РДЯЧФЧЦАЮНЧЭРЦЬЮНГЭОЙДАЮВОЪФЯАФЯЯЧЕГБЧЧДФНЧЗДОЕШГЯЕЭЮЧЯБАГБЧКЯАЦ
ЭЬБВЭЕЯЧГЬАЭОЬАЯГДФЭЧЯЪЫЪДАДЙГУВАГЪЭГЬЬАЮЧЯЦЯДЕЕШВГГФЧДЭАЭЧДЧЭБА
ЕЭЪИЧЬЬЕГЭНКЭЙДАЩАФЕДЮЧЯАГДЯАФЪЭГЬЕЦФНГЬЩЭЪФЯЪХЯДОЪЙЦАХАЯЮЧЯЪФЯЬ
ЕЩЮЪЙЯФЭЕЪБАГЭЭЮЧЯЩФЮЪБЕХЙБВЪКЧЭЕЧЗЭЭЪЮВОЪФЯАФЯГБВАГЪЭГГЧВЦЧЙЯНЮ
ДВЧБЧДАЮЯЧЕГБЧЭАДФЧЙЭЪФЯЪХЯДОЪЙЦАВАХФАВЧЯУЕВХАДВЧЩЯЬВЧБАГДОАЬВЕШ
ЧЯБЭАЗАБЧДВЯЦВЧЪЙЮНБАКЭЪЯФЭФАЩФНКЧЯЪЧАУВЩАФЯЯАЧБВЪВАЦАЫЪЕЬВЧБЭЧЯ
ЯАЧЙГДАЬАЭАЮДЮЕШЧДАЭБЪЭЪГОФГЧШЪДЧЭЪЬВЧБАГДЪХВЯЪЩАЯГДАЭФВЕШОЧБЕКЬ
ЕДЕЦБЧВЧДЛЪЭЪЯЬЯЕЯЧЬАЮЧЯЦЯДВГЗШЪФЭБЧВЧЦГФАЪЮЮЭАЙЪГЭЧЯЯНЮГДВАЧЮУЭ
ЪЩАГДОАБГЯАГДЪАЦЕКЧФЭЭГДВАХАФАЬЯУАЦВАГДЪРЯЧАУНЬЯАФЧЯЯАЫБАГДЧБЪЯЧ
ФЦЭОЯЧЮВГГДАЯЪЪАДЬВЧБАГДЪВЩМЧЩШЭЪЙЧЭАФЧЬЦФЦИДОФЧВЗЮЪАЯЪЬЩЭАГЬЩЬЪ
ЯАЮЧШЦЕЪЮЪЯЗАЦЪЭЪГОЪУКЬЪВИНЬАДАВНЗЭЧХЬАЮАШЯАУНЭАВГБАЩЯДОБАЪЗВНГО
ЪЮКБЬЮЪБАЬАЭЙЯЮЬАЮЧЯЦЯДАУАКЧЭГФАЧФАЫГЬАХА

(b) Расшифровать текст:

ЬПЯАЯШШЮДЦШУЫЙЮРШДИЮБЫДЗКШУТИЮБЫДЖЧЫЧМБВЮОГМГЪЗДВАЫРДЫАЫРАЖШЮВЭИ
БЮФЬБЕПЧНЛБФЩЪЮЕДЗЫЭАБПЪЮХЖЮАЗСБШШЮКЮЭИЗЧБЗЫДБЦФЖКЭБПАЙШВФЗЛЫАЛЪ
ДШЭФЮРЕБИЫЙБЕУДЮЦБХЖЮХБЧЛЗЧЫШЫДПДШШЗАШНВЮЧЮОИЫОДСИХХБПЗГБЧСДКХБЗ
ДЯЧШУЮЪШЧУСОШШМЮЛШЮЛЯЬШАЛЖДВБРНДЦБКДЫЖСЧШБЧБТГЮЧБИЫЙКЫИДКЕЫХДКЯБ
ШЖБЯВФЗЕБЕЦЮЕДЭНБЗАБЗУЛБЯТСЮМШЩЗИШШТЕЗЕБСАЗХЕВЕЙБЛЩАЗЯАЛЕЗЩЮФШЛП
АЭОГЖКДЗЮЦБКГМЯШУЧМЧШШШЗШАУСВДБИЫЛЕОТДЯШЛВГЕЧЕВШЮГАБЫКХШКЫЖЫБЗЫА
ЧШСТЖЫЭЛЕМЦКЛШЮЫБЗЫЬБХФЯКЭШШЫИШГВЕЗЭЯЛЗЛПВФЪЬБЕКДОАЫХДСШЮУАЫГЕОЖ
МЯАЛДЛХШКЫЖАЖДЩЭШДИЫДПЫЭЙЯШИФЭВАЫЭББДАЛИЮГВЛГБШЯЧИДБЩОЪЛПАНГРШАУ
ДЬБХЦЫЕШАОНБЕЕЛБХЮШЙАЗДШЗЫИГШКЗЛХЫШНЛБАЛЕЙШЯОГМЮХОИХДАЧДЫШЕКДДЩШ
УЗЛХБИШСЫЬОВЮЕПШАЗШХСЮЖЫШУЗМЧПЗЙЕБСИГААКЛГЖОЬЭЗМЩШЗСДЖЦЛГЮГЮНЗЛЮ
ЖУЫЬБББКГЗЦБОЭЬБГФЪКЭЫЫНБАБИГБЭБИЕЗЯАОИКЧЫЦЫГЕБЦИЕБЩУЮЛБЮЧИЗЦБОЖМ
ЯАФЩЗДЕЦЮРЭХЙБАШЕФШЗЯЭЪИЖШБУЗЛЮГЧЗИГЛОШЛПЯЛГЗДЖКТЪШЫИГГЖЪТЮРЭБШД
ЙБЦФГАОХСАМЯБТЮРДЕФЕЙШГБШДЯБДЖЮКПКДИБЮУЮЛШЮВГФЯЫИДИГБЧВБЫАЦШЗЖКО
ИЮЮПУСЕЫЪТЫРАЫТЮГБЕФЖФШШЧББЫАЛДЪЮЫЭББХАЛВРШЮФШЮЭДИЫЭЖМЛЩЗХХФЫЖАБ
ТЮКЭЖЧЗЛХШШДИБЭЦЯЖШЬТЫЙШБЗГЙЖЩОШДЫДТЫЛЮЫИДКЕПОЕЙЫГФЪЖОЬЩВЕШЩКЙЛШ
ЯЧДЪГЮОЗХЫВЦДРЫШХЖБЦЮЮЫЖАОЛВЮЩЧЩЮЕЫЭЦДЕШДТДЬБЦЛГЮГЮУЫЪОЮФГББЧУДЬ
БХФЫЖАБЙДРШЮФШЮЭЭФЩЭХДЛЙКШЮОЗХЫХЧЫЕГЪУЫКЮЫХДРЛЭЛНЧЦШУЫЙЮЫНБЗЩЫСШ
ЮДПТЗЖБЫХЖЗДЕЦГЖБХЭЫЕДБЧИЗЮБКЫДБЕЛЕЮГПЙДКВБКЕЙБЧФБЯЮБУГЭЮШМЮЛГШЮ
ЮЛПЭРГЕЧШПЗЛХБИИХВГФИБХЖТИЮЩАОАЗХАЧИМВЕЛБХАБОББББФФЖЗАЫШЫДПАФАЯЧО
ПЮАБАБЛКВБЧДЪБХОВЮШЕЧШЗСХБЩЗЧЖОГЮХОЙДЭЖЧЛЯКЕХОЫЖДЕЩЕЛШЮВГЗШВЦЫЭД
ЕИБЮЕФФБЮШАКЫЯЧОУЗГБГЛЯСШШОЗЛГШЗБЮАЫЛГЮВГОИЮЮЧЛЯКЕХОЫЗФБЦДЖЫЕЛБХ
АБЛЧЗЮШЛШЮГАФЮЪШЪФЕКАБОИГАКУЫЕДБЗЮЙЕПЙДДБДХДАЭБУГЗЯЖХДЙЧЭЩИЗШДШТ
ЖКЫУЗЕЮЧЮЮОВБЭЮЖЖЦХЖИБГЯЮГВГФЪЗЮЩСДЖБФЦПКПЭФВЖШЫНШЗЮПШЫЗФНЧГБЕПУ
ВЫЛШТГЮАЫЛ

2. Разложить на множители числа:

(a) 513692589499795096578424723007

(b) 629572321790106676691701195492694072565565671862778443636363

(c) 176931076260883811329092583993777994090733892427931486077905065735453962691539699250234671 9

(d) 240884061095456874937291441127796172053190098561304556223276814161275513167271526387493874287025773460788518734778033326 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 387358202480212070120409712049474436962468811412341784957026202206333090287 41$
- $e = 3$

Сообщение:

- $M = 429816022623333611872212499023257714960222496739968811041705661654975183614 6$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 323642997190186824149276368704141209957$
- $q = 219461077682381584891490618818787372311$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 681875407400298699779171353465247429970777552438956721427672358938058922641 63$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 209708185162257032603877547425338559419$
- $e = 17$

Зашифрованное сообщение:

- $c = 103964612852108606466469410185577039000$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 27564775044782353666570336299361808131 7$
   - $g = 14316505090641848950827615012884797957 2$
   - $y = 75368109404136916370171736946235078231$

   Секретный ключ:
   - $x = 12498552511254110936603612062531500179 0$

   Сообщение:
   - $M = 26747050154367955387340322716989737446$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 46938813186119999169902079160207152329$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 23503143421890756677139293338700487694 7$
   - $g = 51082711204154779417227806756847203161$
   - $y = 16208281437020114091250643959451920623 5$

   Сообщение:
   - $M = 33529360634069847948182060309188031003$

   Подпись:
   - $a = 11214988786315554049037239808838976277 6$
   - $b = 19758727895113734658241625963923642471 7$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 853$
   - $g = 319$
   - $y = 92$

   Сообщение:
   - $M = 541$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 425$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 5x - 10$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 95

1. (a) Расшифровать текст:

КЙИКЭБАЙВЖКУЙБОНАГНОКЙБООЖДКЭИБМЗКЙПНЗЧФЗЖОКЩОКПОБЭКСБОНОМПСЮКМП
ЮЛКНЛЗБИЙЙДТИКЯКНПАМШГСЮКМЗЗБВДОЮКОПВАМПЯЙБАБЗИКЗКАОЮКЛЗБИЙЙДТИК
ЗКАЯКНПАМШЛКЖВДЖИЙБНОМПСНЮКЪЛЗБИЙЙДТППИБЙНБМАТБОЖДЕКЖЙПЗКАЙБУБЯК
ЭЧЗКАБЗОШДГЮКЗШЯКНПАМШОКЗШЖКАБЮЖОКЙБНИКВБОЮНООШДЛМДАОДЖОЮКБЕИДЗК
НОДЙДУБЯКНОМПСДНИЛКЕАПЛКЯЗВПДЮБАШЛКФБЗКЖЙЙЧЕГЛБМБЯКМКАЖПЖЖОЧАПИБ
ФШЮБАШКОАБМЙПЗГЙЮБНЮГЯЗЙПЗНОМБЭДЙЧИДНЮКДИДЯЗГИДДЙДУБЯКЭКЯЮЧЙБНЮБ
МДФШЗДДЭОШЖИКЕОЖПВДЛМДЯКОКЮДЗДНШЖИПУБЙДУБНЖКЕНИБМОДЖНУНОДЪКЙИКЯК
ЗПЭПФЖЙБПГЙЗБЯКЯКНЛКАДЮЗАЧЖКАКВАЗДНШИЧЛМГАЙДЖЙБУБЯКНЖГОШЭБАЙЧЕДЮ
ЙЖПГИДУЖОКЭЧЛКАПИЗЮНДЗДНОКБЯКМКЮЙДЮЙОКДЯЙОШДУБЯКОКГУОКЖЖЩОКЮНЛКХ
АДЗДЖЖКЮФЮЭМДЙЗБЖНБЕДЮЙЧУЮБАШКНОМДЯНЮЖМПВКЖДОБЛБМШПЙНОПОВБНЙДИДЛ

ДМПБОЛМКЮКМБЙЙБУБЯКНЖГОШЖЖНЖГЗЛМКЭКЗШЙПЪЛЗБИЙЙДТПОЖКЙЮБМДФШЗДОЖЮ
ГЯЗЙПЗЙИБЙЖЖЭЧЙКВКИЙНЖЮКГШКАЙЖКЙБЮЧАЗНЛНДЭКБИПДГОКЮЩОПИДЙПОПМГАЗ
ДНШЛШЙЧБЖМДЖДЯКНОБЕДЯКЗКНКОТЯБМНДИЯКНОДОМБЭКЮЗДЮДЙСКГДЙЖЗДЖЗНКВД
ОБЗШЙДТПЛКЛАШМНСЗКЛКОЗНШНОПЛЕОБНБЭБАКИКЕЛБОМЙАМБДУНЖГЗКЙОБЛБМШЙБ
АКЮНПГЗКАББЮЛКЛКЕЖДАБОЭБАЛКЛАБОБНШЛКАЛШЙПЪМПЖПЛМКХЕОБЛБОМЙАМБДУУ
ОКЭПАБООКЭПАБОЮКНШЭКЯЙБКНОЮДОЛКЛАШПФЗЙБНЖКЗШЖКПНЛКЖКБЙЙЧЕКОЛМЮДЗ
НЖНБЭБЙЖЮМОДМПЛМКСКАИДИКЛЗКХАДПЮДАБЗЙБНЖКЗШЖКЭФЖДМТБЮЖКОКМЧБОБНЙ
ДЗДНШКЖКЗКЮДНБЗДТЧДНОНЖДЮЗДНЛКЯДНЛКЮБФБЙЙЧСНОМПАКИПАБМВЗЛКМЧЮЙБЯ
КАКЮЙДУПЮНОЮПЭБНЛКЗБГЙКНОШГНОПЛЗБЙДЛКЖМБЛКНОДЭБЯЗДМГЭКЕЙДЖДЯМЭКР
ДТБМНЖДБАКИЮБГАБМГАЮЗДНШЖМДЖДЛШЙНОЮПЪХДСИОБВЙДЖКЮЛМДФБЗАКИКЕНЮБЗ
ШДУЮНОМБОДЗИБЙПЛКМКЯНЗЮЭКЯПЮНЖМДУЗКЙПЮДАИБЙЭЧЗКАПИЗУОКГЗКАБДКЛОШ
ОБЭЛКАСЮОДЗДЙПЭ

(b) Расшифровать текст:
ХИШЖДХСЦЕТЙМУФЙЮФЪЖЪЪЕРНСХУЫЦЛТЮЫВПЩХШЛЯЛЧЦДПЩЛУЭНЪХМАОПОЛЖСХЛЩВ
ЙЬНРКЖТМСЕЖПУНЩПТМНЙСМЛЩКГСХШДЙЩГНЭНВЦШАЖЬТРВДХЧЦЬТСПФЪПЧХЪДЛЧЪУ
ФОВМХЙРЧХЧЛТЩПУАНВЙГЭЦТПРЯПЧМХЩФЧКХПЙФТЦЙНМЧТКЭШЦЫКЭУХСРЖТУРДПИМ
ШЬТСХСЙМХИЦЬЬЦЧРЙУФПБЗФКЮНЪТСХЛЖРЧУМЖСХКПЕЖШМХЩЬТШХЭДХУХЖРХЙЩЭКШ
ЩНЗЙЙПМЕЬИВУАЛХФЩВЙМШУЭЕВМОЭЕФМКЕПХИХЖГТМФУЖМЬУВСЪЦХЖКЧВЩФЯШЙНГЭ
ПЮНЬГУХЛЙММЛЦЪУГОФЕПЕППЬМППТИЙЮТФЕЖЦХФАОЪЩХЖРХЩРРЖШЪМИЭЧЛРЩПКЦЦК
ЙЯМЧИПСТЪВМЮХХВНХФНЛТЦМКЭУОЩКЖЙУЛЦГДХФЦЫЙУИНЙПУСЫЬТЦМААЩГЛЦЩСХИГ
ЕРПЧЪЖРХЛЦЩФЬЩЦЫППКУЬЙЦМЪИОЛЧНАШИЩЖРЛЦМЪИОЛЧНАШФМЧЖДЪИРЫПШЦЦЬЙЙТ
МУЛХЦШЖРЛМЪЩСШСЦЭЕПЩКЙЛХЧНЯТЙМШВМПИНИЕШСРЭПКФРДЬЦХМТЖЬТРВПЙЧЛДЖШ
ЩНЙУЙМХЕЬУЪТИЖЦТНЕЙУШУЖВХЛГЙГМТДАШХЩФЭОФМЦКТЩЙУЕЖЦЧНИЬЙНУЖВФВЭЙГ
ХПЭДПТМХАКФЛНГТХИВЭЦЩГЩГПИХМЛВТКЦЗПТЪЯЕПССКЬСЪКЫЪЙЛМУЬТЪУШВЖЦЧФЖ
РМЧНЬТХИЦБШМТЦЪЖСЦЪФНЪНРВПЙЙЦЖСЪННЕОВЬМЛВПФФАЮЩХЙУМЦМШЭЕХЙЦБЛЧЪУ
ЗФКЮНЬТСХЛЖРЧПЩКОПАХЙПСТРВМПФНЯОЦЧЦГЦХЩНГНХТЯЗСХМЭКЭУПФЖЙЬФЦЖОПУ
НЕУХЩЯЙПСЧЫЮЙТПРЖЕПФРЯОПЬЩНГЩПУГПЯЛДДПЕОЫЯЕЪЙГНГЩПУЙВТЕРЛЕЧПУДФН
ПТЗПКХУЖГМЯЧВТЦШУЭДХХМЕЛХХХЯЩЩТЩАГВЦЫЙУПТРЯСЪСЫЯЕЪЦШЖШПМЩДФЩПУАТ
ГПЦКВМНУАГХШЧЖМГОЦЪМШДЪЖКУПХЛУХЕЧИЙЯЦЦИЙТТЦРЕГПЧЖТССУКЖУФЦКРЧПЙГ
ЙНЕБЭКШФЦПЙУХЛГЙОИКАУГУНЕПЩЙЩВПРХЧЙОХШЪАЛСЙМИФКХЛГОЪЙААТГЪКАЕМТЯ
КПШЙНГЭПЮЩЖНФХЖЕЖИВУЖВМЛХУКШЩШАЛФШКЖЖРЬШЖНХРУЖЩЛПХЭНХКЫЙЛСЩДЖУЧО
ЙЖКФПТЖГЮЩЦЩЬТХМЭМЩГЧЖЕХНМЪЖКХХЭТСХУФЛХУРЕФЩПЫЬПШЩЦЪЖЧШДЪУХУЯКПХ
ФПЬЖЧНХЗПЙХШЖУПТУЖЩЛГРЖУЦЧКАМШМЛЖГВЧЫПУГЦЦЬЫМООВПЙЧЛЛФШТГРМПОМГЙ
ЯЪФВСПСРАДХТЦЙНХМЛЖТЙМУФЙЮЦЦЭЦТШТЖСММРЪТСХШЭПЮЪЪАМШШХЖГУМОЬФСЧЫГ
ЭФВФАНЪНРВНПХЩКОХЙРЪЩПУРДЖФФНЙЛХТДВПУПХЛУЩХФЛООЛЩЪЖТГРПОЬХМАМШУН
ЮЕЪПФАПФПЩКЪПТРЙУЧПТЙЖКХТГШПП

2. Разложить на множители числа:

(a) 45183072164125944267633109544 9

(b) 960207966862871496460059173185950695137885057089542861423557

(c) 10382616734356567919841396516123939678495695834288322494889164155377563578625991079713836 93

(d) 963032715674730089234144527754376288412742392374399370724245878792743129893796405118877472626645120562471820572055581323

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 59035223330885563455222214430057597307000756208482506614731573796151557310431$
- $e = 5$

Сообщение:

- $M = 54293835564968229626578341613669729498515651499294350177140392549525185081601$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 30249278479045164669485558195651573056 7$
- $q = 31404069116903174960940818020552577178 7$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 4401402618165587293405956332311973432779492778545161070442689062381882101184 9$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 181067292819399028878671300408440346617$
- $e = 17$

Зашифрованное сообщение:

- $c = 244194888349036879932102612344747640 20$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 202759294924158698699406509971610319419$
- $g = 191924138979283686657320134021204987164$
- $y = 434287036769895997699116428650184796 32$

Секретный ключ:

- $x = 111777349595988622171953457097003054623$

Сообщение:

- $M = 24691283684006644258262161936823849724$

Использовать следующий случайный параметр для создания подписи:

- $k = 151370663779328207150600671544661436849$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 224371342961470625808693508517023128289$
- $g = 630209375664843636291089091401790 87763$
- $y = 266104119885097945100315212384916290 91$

Сообщение:

- $M = 116963380407530458804602826978845129262$

Подпись:

- $a = 167983349468073998443966519503216535256$
- $b = 129278529178288108331300522899199764 02$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 947$
- $g = 737$
- $y = 660$

Сообщение:

- $M = 715$

Использовать следующий случайный параметр для создания подписи:

- $k = 5$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 9x - 5$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 96

1. (a) Расшифровать текст:

КЬНОЫШЬМАОЛЪЧБОФЪУЩДФЕЯОХЬШЧНЛОФСФЧБНЕЧЦШЩЧЛЧЩЦЧЛЪУЧАСФЛЪОНФЧЦОН
ЧПНЛБСЪЕУРУЧЛУЧЫЧШДОЮЧЫОФСКДФЧШЧНЪНСЫЕОМЧЛЖЫЧЛЩОХСРЫЧФШДЦШЧНЛСПЬ
ЛДЪЫЬШСФХЧТЪЛОФЕСАШЧНЮЧНСЫУШЬМАОЛЬСШЧНОЫОХЬФСЪЫКЬХМСЦОХЧМШЩСНЬХЫ
ЕАЫЧСРЫЧМЧЛДНОЫЖЫЧАЫЧЪШЩЧЪСФЛПЦЧШЬМАОЛШЩЧАСЫТЫУСРЛЧФСБЕЬЛСНОЫЕЧЫ
ЛОАФЪЛОФЕСАШЬМАОЛШЩСЦФКЬХМЬСНЧФМЧЩЪЪХЫЩСЛФЪЛСНЧХРЦАСЫОФЕЦДХАЫЧЫД
ЫУХЬНЩОЦЧШСБОБЕЪУРФЧЦЦУЧЦОЯЦБСЪЛОЫФДОЧАСЦОХЧМЬЫЫЬЫЦСАОМЧЩРЧКЩЫЕМ
НОХЧТЧКОЩЪОУЩОЫЩЕХЧФЧНЧТХФЧТЛУШЩФЕЪУЧХХЬЦНСЩОШЩЧЛЧЩЦЧШЧНКОПФУШЬМ
АОЛЬАСЫТЛЪФЬЮЪУРФЪХЧРЛЦОЯЧЫНЛОХЬКЬХМЬАЩОРЛДАТЦЧФЗКЧШДЫЪЫЛЧЛФЬРЦЫ
ЕЧАОХННЕУХЧТЛРНЬХФШСЪЫЕШЬМАОЛЬЧКОЩЪОУЩОЫЩЕМЩЧХЧМФЪЦЧЪЫФШЧЪУФНХАС
ЫЫЕЪФОНЬЗВООНЛЮФЫХСЫУФОЛДТСБОФУЧЛДТШЧФЧЪЫДТЦБОЪЫЕЩЬКФОТЖЫЧАЫЧРЦА
СЫЪУРФЦЮХЬЩЪЕШЬМАОЛШЩСУПСАСЫЫЕНФООЧЫЛОАФЪШЧУЧТЦЧЪЛОФЕСАЧКОЩЪОУЩО
ЫЩЕШЩЧНЧФПФХЬЦНСЩСРЫЧЦУЧМЧРОФОЦЧМЧЬЬУЦЦЪОХЕЩЬКФОТБЫЦДКОФДОЬЬУЧЦЦ
ДОЦШЫЕЩЬКФОТНЛОЦНЯЫЕЩЬКЮШЧФЧЫЦЦДЮМЧФЦНЪУСЮЪХЦПОЫХСЦНОЪЫЕЩЬКФОТШЧ
МЩОКОЯЪАТЦЧЗШЧЪЬНЧЗЦНЛЩЬКФЪШЧФЫСЦЧЗАЫЧРЛЩЦЕОШЩОЩЛФШЬМАОЛУУЧОХЦОН
ОФЧНЧШЧМЩОКЯЧЛСНЧБЫЦЧЛЪХЦПОЫХСЪЛОФЕСАУЩУЦЬФСЪЫФЧКГЪЦЫЕЪЖЫЧКЫЗБУС
РЛЧФСБЕЛСНОЫЕЩООЪЫЩКЩЪУЧХЬНЧКЩЬЩЪУЩНОЦЦЧХЬРФЧНОХСУУСХСРФЧНОХСЪШЩ
ЧЪСФМЩЧРЦЧШЬМАОЛЛСЦЧЛЫЧКХЧФЛСФЪЧЫЛОАФЪЛОФЕСАРФЧНОСЦОРФЧНОСЫЛЧСЩО
КЫЫУСШЧБЩСФСНШЧЩЪЫЪУФСЦОМЦОЛСЪЕУЧЦЕСЧАОЫДЩОЮЦЧМЮНЪШЧЫДУОЫЪШЩСУПС
ЬПНЧАСЫЫЕНЧАСЫДЛТЪУРФШЬМАОЛЪОУЩОЫЩЕШЩЧНЧФПФЧНОФЧЪСЫЯОЛЧОНЩЬМЧОЫЭ
ЫЦЧОЦЮФЧШАЫЧТКЬХМОАОЫДЩОЩЬКФБЬКФСЪЕУЩДЫФДХЩЫСЦЧХЩЬКФОТОВОРТАСТЫЬ
ФЬШАСУШЧПФЧЛЦЦДТЫЛЧОТХСФЧЪЫСЦШЧЪЫЧФЧХНЛЧЩОЩЬКФОТЖЫЧАЫЧОВОЛЪУЩСАФ
ШЬМАОЛЪЛОЩУЦЬЛЧМЦОЦЦД

(b) Расшифровать текст:

СЩЕРЫЫУЕЬПХТЖЩЬЙЩАЬЩБШМУЯСЩЙМПНРВЯШМЦМЫЯЗРПУЩАЧАЦТУЧАЬМГАМАКПЮВХ
ЫГЭЙЦБЗЬАЬЮКШЯБЮИРМЯЮЛРЛЦЦФЩВМХКРАЬЧЦЩОЬШКШОЩЬЗЮЯЦАУВГАЙХРОЪЦННЕ
АЬЗЪМЩЬТХИАЙЙЮКУЖБЪОБЯЦХЖЧШУЫМЩКСЩБЩЦЖЖПЬЪТЩЬЭЬЧОРКЯЪНПАЩННМЯАБЫ
ЕПЬОШЖШЭУХЕЩЯБЧЛУХЖНЛЯЪПХРЙТШЧГЖКЦХЕЩУСЮСЭЮЗУЙЯЩНМЩАЙЦЯОЦТКЫЖШЬС
ЬТУТУЫТУТУЫМРЦЬРКШШЛРЛУАЦНЦЦЪНРЛЮЩСУАУТБСГБЭХНЙМЯБЩЛЦУИЩЯЦРРУВЬЯ
КЦГЬЮШСЖУЪУРЯЙЩУЬХЯАРУАЬТОЬОЬШЧЩЙЦУЮРЯБТКЭИШЭУФВБЫСЩПШРШЭЩЭЬРОГЖ
КНПРЦЫСЩПШРШЬКЬХЗШГДЫКЬИЬЩБХМХТШЧЙЯЦЦХЕЩРФЩЙСЬРЩППЬИНГЯАБЮЙЦДСЩР
УЯТНМЩЦСШГЪЩУЫГПАСЩЖБЪТУХМАУШЖРЬХЖКЫУЙЩЙФЫУПГЮФЧЗСГЬЗЩПАЮУЪОЦЭКЫ
АЬЧТРСТЕКЩЛЦЯЗЩЬЖУГНЩШБФЭКЬУГОМЩЬЗЩЬАЬЧЩПШХРЪССЕКНСЫУРЮХЖУРУРУПК
ЩРЯАЧЗМАЫНАПЪЬСЮЕПЩИЩАЮУСРЛЫЬЙЪОЦПКОЛБАБХКЦЩУЬГЮТНЙБЬЯШПОЙЫНЪССЕ
КНБЬЮБХМБЯСРУЫБРЬЛУАУЭАУЕРЩЛЭЬМПЛЬЪТРИАКЦПЙЪУТШГПБЙРРЭЬСУЙЬРТУЯБ
ТШЪОЬТУЦДАКПХЛЕЩПХЕЫАБНМЯКНЮВУАЦООЦЖПЩРЮУФЗГРРКПЪЭЬЫПАРУНЙФУТПК
ЬЯПНММХТРЦКААВГЪЬТХМЫЕНЦГСЬЗЖЯЮЬЦУЙЦЦМЩИЫХХРЕЩЦЦЩДСЩНТОТЦРУГСЬФР
НЩЬСЪСЖШШУАЙЭРУЙЦЯРЮЦЧЯПТЙЭБИВГРЯПХЖЪАУПЖШЦСНВЬГТЩАУЫНРКЮЯЦХДБАК
МГЯШМХСШЬЧЩОБМЗЫГПЕКЬРРУСШГЮЯЦХЕЙРРЬРЮШРЧЩЕШУПЛФТАЩОУЩЦЪОЖЦЗЦСРЬ
ХЩЛЯШЛУАЬЮУШНАЦЫЩРЕУИЩДЦРКГЪАЙТМГЩЬСЬАУАКЭОЦЯЧЦГАРЦРБЫЗЬГАЬРЗИЬ
АХУВДАБЭОЦСУПМААУОМПАГГИЬАЗРХЩУСЮАЬЮУШХАЬЧЖНКУЭЗДЦРШЙИЮЬЗЗНЦАГЬЪ
ЪУХЭАУЕНШМЧЬХРЙЭЬЙЮКЩТЗФНЬЭХЩЯБУСУКЙЭНЭРКЯЧРКФУЪЩОЬЖУЪМЩУЧРЙЦЬХР
ЙТРУЫМЫРУЭЕРЦЙРЙЦЭРЮЬЩЬЭПЪЯЭШЬРЦЩНЬЪЦЯКЦЖРЬХЩЛЯАРХЙУРЧЗВЭЬЪНЙЦРЧ
ЗМЮУРХЙМЫШЦОХШРЙЛБЩЙЫССЬОЧУЫБРХОЙЩУЧЖЯШМЦАЬЮУШСЫУЧМОАРУЫМЫЕКЧРЮЦ
ЦЭЙУАФУРАКЦЪВЩКГЦСЕЖКЫЕЫЭНЭЪЯФННМЧШХЩАКМЧЧХАЬЖЩБТЯЧХИЬРПЦКЙДПЬИХ
ШМЭГЧЩНН

2. Разложить на множители числа:

(a) 6372345935237962372094776235 27

(b) 7756967998833459135625338385962661532659874545915999224880 99

(c) 1063116035576852438474599533482073827400908285018286876912236712740443620575857160255381981

(d) 1392110038638308139530339644368734798739655188907333201385221670002574091726302785956913278249602035980393918617339159947

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 940605603563483882045884356171532691562800883261543017494023142688705546038 01$
- $e = 257$

Сообщение:

- $M = 736608225621972774482764727302810018752283157972201406695246708502140475291 73$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 327255941880204454343971758919820712313$
- $q = 215184895635550398434447150444143537547$

Открытая экспонента:

- $e = 5$

Зашифрованное сообщение:

- $c = 564114280149054401041257008023494381199012275229114598229648746872521157340 19$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 192138527369249803206576895894568963851$
- $e = 5$

Зашифрованное сообщение:

- $c = 108151644134351961155018948015033703028$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 294953883590563579774073989702712274283$
- $g = 169035942134978962666915323792911563632$
- $y = 271321710935164083864037238192272418586$

Секретный ключ:

- $x = 177541830430331250703932379271949205223$

Сообщение:

- $M = 110577937952591427051928549929505650125$

Использовать следующий случайный параметр для создания подписи:

- $k = 251709241035728957277951126706101929777$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 186329754602842211098554526350853991963$
- $g = 151291731423983617885522486095916115479$
- $y = 164920950472797271092300901622562280669$

Сообщение:

- $M = 869784783469379581953365871563161804 85$

Подпись:

- $a = 137300156263790303001749738093089880393$
- $b = 104144746559835876868515957170470657768$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 643$
- $g = 452$
- $y = 635$

Сообщение:

- $M = 165$

Использовать следующий случайный параметр для создания подписи:

- $k = 169$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 10x - 10$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 97

1. (a) Расшифровать текст:

ЦМЖХЙТЩПМТЦИТФТЗТЖМЛСЯОТЦТФЖХРТРИЙПЙЕЯПЧКХСКМЦЙПМУФМЖЯОПМОИФРЛПЙ
ЦЖЬМРСМЩИЖТФЯИКЙУФМХЦЧУЯУЧЗЫЙЖЧКСЙУФМЖПЙОПМТЕЭЙЗТПВЕТУЯЦХЦЖЧРМФП
ХТХОЧОМЖФЙРЬПТУМХЙРМЛЕЙПТЗТФХОТНОФЙУТХЦМСЙУТПЧЫПЖХЙИТФТЗМЕЯПМТЦФ
ЙЛСЯФЛПЧОХРФАЙНМЖСТЖСТНХЦСТЖМПХАРСЙСЙХЦЙФУМРСЙМЛЖЙХЦСТХЦАТЙЙХЧИА
ЕЙРЙСРЧЫМПЙИМСХЦЖЙССТЙФЛЖПЙЫЙСМЙРТЙХТХЦТПТЖСЙЛИСМЫЙХЦЖЙУТРМПТХЦМ
УЧЗЫЙЖМРЙПИТЕФЧВПТЬИАХОТЦТФТНИЙПМПХХОЧИСТНУМЭЙВМСОТЦТФТНЙКЙИСЙЖС
ТЖЯЙЛКПЛЗТФТИУЙФЙХЦФЙПМЖЦАХХУЧЗЫЙЖХОМРМСЙЛИСМОРМЖБЦМЩУЙФЙХЦФЙПОЩ
УЙФЙЖЙХЕЯПТЕЯОСТЖЙССТСХЦТФТСЙЛПТИЙЙЖХЯЦЯЩУАСЯЩМИТЕФТОТССЯЩЦТЭЗТФ
ТИТЖОТССМЪСЙРТЗПМЩТИТПЙЦАМСТЗИЖЯЩТИМПЖУТПЙМСЬЗТПТИСУЙЩТЦСТЗПЧЕМС
ХСЙЗРЙЬПЙНИЙНХЦЖТЖЦАЧИЫСТУФТЦМЖЧФХХЙССЯЩСЙЛИСМОТЖФЦМППЙФМЦЭЙЦСТЗ
ФЙРЙПХЖЯХТЦЯЖПЖУТПЙЖЛПМСЙИЖМЗПХАУТУФМЫМСЙМЛСЧФЙСМПТЬИЙНЦОТЖЕЯПТЕ
ФЛСЬМЩЖТЙССЯЩИЙНХЦЖМНМЖТЦЫЦТТФЙСЕЧФЗХОМЙЫМСТЖСМОМСЛЯЖПМТХЦТФТКСТ
ХЦМВМЕПЗТФЛЧРМЙРТИСКИЯОТЗИЧИПТХАСРООЦТФХХЙЦАМУФТЗСЦАИТЖТПАСТЗЧХЦ
ЧВЦТПУЧСЙЩПСОЛОТЦХЦЖЬЙЗТТЦХЖТМЩЦТЖФМЭЙНЗТЦТЖЕЯПЧКЙЧИФМЦАЙЗТХЖТЙВ
ЦЧФЙЪОТВХЕПЙВООЖИФЧЗТСХСПЬУОЧМЛОФМЫПЛИФЖХЦЖЧНЦЙУЙЦФСИФЙМЫООЖХЕТЗ
РМПЧЙЦЖЛЗПСЧПМЧЛСПСЬЙЗТЧФИСМОСЙХОЛССТЙРЧТЕФИТЖПХЛИФЖХЦЖЧНРОХМРЯЫ
ХОЛПЙРЧИЖСТПММЛЕЙПТЗТФХОТНСЙИЖСТЕЦВЬОУЙЦФСИФЙМЫЦТПАОТЖЫЙФЖТФТЦМП
ХЧРЙСЙХЦАОЖРУМХАРЙЪТЗИЙКТСТЖХОФМЫПЖЙХАЦОМЖХУЯЩСЧЖХТРСТВТЦЖЙЫПРОХ
МРЯЫУТПТКМЖФЧОЧЛУЛЧЩЧТЕЙЭПХУПЬЙЧКООСМЕЧИАИЖРИТХЦЖМЦАЦЧЦТСУТИПРСЙ
ХПТКЙССЧВЕЧРКОЧМЦТЦЫХЧХООПФЛЖЙФСЧПЙЙМХЦФЙУЙЦТРУФТЫЙПХПЙИЧВЭМЙХЦФ
ТОМЕТЗЧЧЗТИСТЕЯПТПМЬМЦАРЙСЖИФЧЗТЦЪМРЦЙФМСЙМРЙВСЛЙРПЙСМФТИСМСМУТО
ФТЖМЦЙПЙНУФМЕЙЗВОЖРЛСЫЦТЖЯЖХЙЗИКЙППМРСЙИТЕФМЫЦТЖЯЖХОТРЧЫЙПТЖЙОЧЗ
ТЦТЖЯУТРТЫАРТП

   (b) Расшифровать текст:

ДЮГЧАНБЭЪБЕЗЙЯНПАЪЩНЬТЙУНЮАФЭОИЧЪЯЖЬВЭФЙТЮЪЮЙВВВЯДНФЭЧЯЕЗКЯЯЕЫЖЯ
ЬЪБЕЩНЬФЖШЭОЫАГАМЭЭАЛЕЦЬЦЕНЦЕЩИСЮЭХГНХЕЮЦЙВВЮАЧЭЕЯММШГЯДДХЪДУКЮЦ
ЯЕОВЖБЙЙХСЦОТАЖЭНКЬЛИГТХГНИОСЭВКОЪЖЩЖСЭЭУАРШГВЗОЬЛВАБХАУЙОСИЧЖЧВ
ЖУМЕБЖЭИООЙЬОЧШЪЙАЕБЩМЖОЯЛВНОХЙЮЙВШЬЦИИХДБЧИТЕЯЭНУГХАЛБЯХОМЗАУЙС
ВАПНОЭДЦИТЮЕХЙРЮЫДГКЧГЯМЬЭЭДМПХГЦФЕЮЗЯЗНШКНМИЯИЩЯТШЪВАБЬУЭЙЛЗГЩМ
ЕАЬЗИШШЙЬГШЪЖЭЬЫЫАДНОЬГЦИЫЭЭАЛИЬЭГИЫЬЖТЛЗЮДИМЧХИЦВДТЖИОТШГЩМЬЬУУ
ЬЛШЮЮАЙЪИЦКОБКЩНКЦЭАЙДТГВННЮБАОГЗЭУОЗФЭВЧМЛЗЦЛЕЬЭЮГЛШГЯУДХБАЙСЪЖ
БЙСВАВЕКЮЪЯДИЕЯАЛГЫААЙТЮИЯКЛШЪЯДУБГДБЛШЪЯМТШЩБЯТЮЫЯЕЗЪЗЯМТТГЦИНЮ
ЫЯКУУПЦЭЫЬЪЫЙМХЕХИТЛЛУГДХГИНОСГФЙДАЩЯЖТЫАУЙСВАЭФИЪЕВКРШЪЦВШХЫЯЗЕ
ЭЗБГНШДЬГКЪЗБГДТЖБИОУЖУЛЕЬЭЮФИЪДМЙТЯИУГЛШЙНЯЛХЭВНЛЮЙЭАРЪКНММЛЗБГ
БЫАЧГЛШЙНЕГЮИЯЯКГЫХАПЮЙЬЙВЬЩЯЛОФКЯЮОЪЖЭАНФЕГИХЮЬЩЖСБАЬЧНЛБЯНРФАХ
ОЩШБЮМОХЬЩИЕЭАЦЕСЬЖШЭНЖЛЭЦБЛГЩЙСВЕЯЭЛХЕМЕРГГНИЫЬАЮЭОЯИЯМКВЖЦЯЕВД
КГКЮКУАЧЫЫБЙМЮЫЬМНЮЫЯМУФИЦЭКГДВЙСТЖЦЩХЮЯПУКЮЦУЯРГЫГЙЛЯЫДМРЮЪЯЕРГ
ЮЩЖНБЙДБСЭЖПЬРЭФПЭЫЕЖХГБХЙЯЭКГДВЕЗЫДЮАУБЙГЦЙТНЭГСВИУЙТГЮЯНЕСЭТОД
ХКТИИБКУЙЕОНЯВЮИВЯЩБЛРЦЖИЧВЩЬИВВЩГТАЭТЙВЫПГЙБЮКУАЛШДЦИКШНЮТЛМЕЩЕ
УГЪЩЯОДАЗАРБЖЬЯТЛЗБАКАКЩЖИСИЮЧВЕДЩМТАЗЯЭЕЫДЦИКЬАЯЛУБЪЦЖЬШПЯНМХЕЮ
АОВЙГЭЛЯЖФЙВААУКРЮЙЦЬВЮКГАБХАФЙСГЬБАВЪЛЭГЗЮЫЮЯВЯЖЬЦМУЖВКОФАУЖДЛВ
ЯТЕЬХГЙВБЭЫЙНЗАГМКШЩЩНКИЫЯЗПЮЭЖЖЗЭДЩТЕАЭШКТМДЩИУВДМКРШРЬГКФЖЭГКГ
ИЫЙОБЪЦФЕЭЕЯЗУТНЭГСВИЯМТТАЬЗЕЭЗБГКАЛЬАИЯЖЙАЛЮЩЯЗНХЬЯЖОЦАГЧОЭКЯНЧ
БЮЦЭОАЖГГЛБЖТХВШЪЭИЕЗКЯАГЮЪММОЬЖТЖГЮИЯЯИОЕЦЕОУЬЭАНЯИЩИТМПГЙОЭЪЦЖ
ЕЫЖГЭЕБКЩЗЕЭЪЯМТАЖФРОЧЦЙЕУЪЙЦЬЕЯИЩЭЕБКЩТТЮХГЙЗЭП

2. Разложить на множители числа:

   (a) 869819814529701858144648385027

   (b) 76262099972627008026486317486645189188387415162445081434010 7

   (c) 702858724818618654382678242279489501137790195985701598063678869833480512149328629600502607

   (d) 135344492102048671560002124334454129450652958253504320279679896587470853268732934354955144285055750850456178487460989201 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 700218250969810641891175682770837476624529687928621065307699850290820887501 51$
   - $e = 5$

   Сообщение:

   - $M = 409136270644548704930650363096960478083582207762588681290181636291086466974 87$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 298843316965897955870291444788981013677$
   - $q = 186241822699266354160975134223543923053$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 465722285572129064959102664103374713258045885529153366272783113812458722192 3$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 264669641478314342566085531546537122009$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 209265735430292222698194144595902161159$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 305276074998949739535443300795880586111$
   - $g = 184182759724886924152349639383547235884$
   - $y = 297154833552510191126239818384524181078$

   Секретный ключ:

   - $x = 786165710594773488345785606606975397 41$

   Сообщение:

   - $M = 117422549152080290190778171823535775502$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 30146623426692886312223221955681428311 7$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 23787441255436014822000425909913118502 3$
   - $g = 12310427279831666443844833059321843708$
   - $y = 958286583241049758398529237273062326 62$

   Сообщение:

   - $M = 188131187225782699232226708318399576360$

   Подпись:

   - $a = 827689331704168290049082825982093048 93$
   - $b = 524479282079102029322379204127396568 60$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 733$
- $g = 676$
- $y = 674$

Сообщение:

- $M = 379$

Использовать следующий случайный параметр для создания подписи:

- $k = 413$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 15x - 10$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 98

1. (a) Расшифровать текст:

ТЭЗЫМЭШЪШЭХЯГУЩЦХФТЮАЭЪЧЭШЕЯЮЯХАТЮЬГЭУЮТЮАГЭХЗХУЮШЕЭШЦЫХВМЭШЦЫЮТ
ВМБЪЧЫБВАШЗЮЪТУЮЫГСЮЩЫХЭВХИТСАШЭБЪЧЭШВМЭХСХФЭХЕГФЮШУЮБЯЮФШЭЮДШЖХ
АФЮЯАЮБШВМЯЮАФЪЮЬЧЗХЬШЧТЮЫШЫЯЮЦЫЮТВМХБЫШЮЭВХСУЮБГФАХЬЭХЯАШЧЭХВВЪ
ЭХЗХУЮГВХСШГЯАТЛШБЪВМЪЮЫШЯАШЧЭХВЗВЮЦХЮЭФЮБХУЮФЭИЭХУЮФЭБШФХЫТЮАХЭ
СГАУХБВТЮШЬШБГЯЮБВВЬШЭХЯАШЪЦХИМЫШБТХБВШХУЮТЯАШЪЧЭГОФЧЯЫШВМВЬЮУЮЭ
МЪГЬЭХБФХВБЗВЮХУЮЬШЫЮБВМЯЮФЮБЫЭЪЭЬЮВЮАХЭСГАУБЪШЕЪЮЬЭФШАЮТЫЮУШЪБВ
АЮУЮЧЫЮФХЯЮЪЧЫБМЬЭХФЮТЮЫМЭЮГСХФШВХЫМЭЮОЬЮАЮЧЯАЮСХЦЫЯЮТБХЬГЬЮХЬГВ
ХЫГЯАШЬЛБЫШТЗМШЕАГЪЕЭЕЮФШЫБЯГУЗХТЧЬХВШЫЬЮХБЬГЙХЭШХБМТИХСЫУЮАЮФШХ
БЪЧЫЮЭЬЭХЯЮФЬШУШТДХЫМФЬАИЫЬЮЩЪЦХВБУЮТЮАШВФХЫЮЪЪВЛФГЬХИМЭБЬХИЪЯГУ
ЗХТТЮЧТАВШЫЬЭХСЮФАЮБВМБЯЮЪЮЩЭЮЮВТХЗЫЗВЮЭЕЮЦГБМТХУЮТЫБВШШЗВЮЮЭТЮЫ
ХЭЯЮБВГЯВМБЮЬЭЮОЪЪХЬГСГФХВГУЮФЭЮФЮСАЮБЪЧЫЯГУЗХТВХЯХАМБЪЦШТЪЪЮЬБЮ
ББВЮЭШШТИУЮАЮФБЫТСЮУГЮВТХЗЫТБХСЫУЮЯЮЫГЗЭЮСЫУЮЯЮЫГЗЭЮЯЮТВЮАШЫЯГУЗХ
ТЭАЮФЬАХВБУЮЫЮФГБЬЮЧТЭХЖУЮТЮАШЫЯАТФГЭЮЯЮФЮЫУГЯАШБУШБВЫГТХАВМЗВЮТ
БХНВЮЯГБВЛХБЫГЕШШЗВЮТЮАХЭСГАУХФЮТЮЫМЭЮТБЪШЕЧЯБЮТВЛТШФШИМЯЮФЕТВШЫ
ББАШЗЮЪЗВЮЮЭВХСТУЫЧЮСЬЭЛТХВТБХСХУЫХЖЛБЮУЫБЭЮЯЮЪЧЛТОВЗВЮТЮАХЭСГАУ
ХУЮЫЮФШЬЮАЗВЮВЬХФВЬХАВТХЗШЭГШВЮЧЗХБВМХУЮЬШЫЮБВМГТХАХВЗВЮТБХУЮТФЮ
ТЮЫМЪЮЫШВЛИТСАШЭЕЮЗХИМЯЮТХБШВМВЮГЦЭВЮЩЦХТШБХЫШЖХЯЮТХБМШНВЮУЮЬЮЫЮ
ФЖЗВЮСЭШЪЮЬГЭХСЛЫЮЧТШФЭЮБЫЮТЯАЮЪЫВЮУЮБВАШЪЬЧЫЮБМЯЮЪЮЫХСЫШЯГУЗХТЪ
БЗБВШОЕЫЮЯГИБВЫЯАЮВШТЮАХЗШВМБТЮХЬГВЮТАШЙГЯЮЫЭЮЭГЬЛЗБЪЧЫЮЭХЬГВХСХ
СЛТБХФГИШВМФАХЧВМЗВЮВЛЧСЮУВЛАМЯЮУЫФХВМВЪТЗХЬФГИФХАЦШВББЬТЬЮУШЫГБ
ЬЮВАШИМФАГУШЕУГСШИМАЧТХЬЫЮЪАЮТШЭВТЮХЩБЮТХБВШФВЛЗВЮЧГУЮФЭШЪТЮЧАЧШ
ЫСХЫЮСЮАЮФЮТГВХСВЮЮВЪГФЦ

(b) Расшифровать текст:

ГЛУКПУИУРКСЕЯШКРЕВЛШЛДДКФШЖИЕЗШЛАОППЛЭПУХЦИЕТНПТЫРНПДПУЧУЦБРКРЯТ
ЗКЪЬСТКЖЯДУЗРЩЕСЬХЯКПУЧЩЦКХЛХВУХРЩНТНЕЫКШГФЬУЛЖЦЫПШИЪЦВШЗФГУФЧЯЩ
ННПНЩХФУУДЧКТЛЪОЧТИФОФХЛЮТБТИЭОИПНЩМЛКСТРМУПУОМХКЩЛСУМХОФХСВЧНПЗ
УОХТЛЮИУЩЛЗЕХУЗЩНФУЬЧЕТЦПЯЗЗТЩЦМСКЙХУЧКПЫКЗЦИЦГУЧСУРНЮЛШЛУЙИЪСПН
ЦЭЕХЮЕЬЕТАНЫИСУДБЗУСАГОЧЦПМЙУЩЛЗЕХНЗУОХТЛЮДХШЙЦСПНТЩРШКХВБШТХЯВЮ
ННЭИФХЛЮИСКХЯТИРЕЮОИУКЬОЙКТЯДХПЛЙУЖШОЯШЙБЛАОРЧЛЮУЙКРЦГУЧЪЦГУФУЯИ
МУЫЬТПЦХБНТЙУДЖЖНРИЕСУРЯСТУЕЮЕЦРЛЮЕТНКЭЕТКЛЬИФУНБЙТКМЭЕХКРФНШЦРЯ
МНФУЦСЧШТЮОССОЯДШЭЛЩБАРЖЬУЖУНЯОЦПСББРКРВЛУЗПЩГЗХЗЦЙЦПСФОУЩЛЗЕХНФ
ЧРУСРИЛЦЗСЦОФХЕХННКУВСПМОЫКТЬОЯСБССЦЗТПСЭСЧЗСВПШИЪЦВАСЕВТКФЛУОЗХ
ИЭБШХРЫКФХЛУЗЧНЛТЕРУЖЯРЦПСЪКХКТЯСЧНСЮМКТЦШНРНТЯЩЙНОВКМРЪГОЧШОДПН
РСЙДБФУУДТКТЯСУЗИВТНРФАРНТХНОЧЦПЯЗЗТЩЮОЬЧСТЕРУЖЯРЦПЦПКХКТЯСЧБККИ
ЮРТБОЧНЕДЗРУЗЦДУФСВЛКЙРЦЙПХМЮОЦЧЛЮКУТИЗСУЦОЬСНТПЯЕИУЖЦНКХОЫОЧУУМ

ЙСУЖШСЗНЗЦТКРЯВТЗУЕГЬСУИДСКХЗЩЕЗУЕБЕСЖИХСЧЗИЮНУОСБЕТЖЦБГЦПСЪОЦЙЮ
ВТХУЖЩЙЦЧУЩКЗМОВОЦЧСЬОЧПУМТУКТЩСБССЩСЧРЪЩТЧБИФОЗЦОДХТМТБОЦЗЫЦГУФ
УЦВУЦШЯДНЧИЬЬЦЧЕЫОЦЧИЬЬТУТБПУХЬЩКИХЛЮЕЗПСТЫМСИЙНТУЖЯВТАРЦШТКПВМЧ
КРЩИНЗСЙЕЙЭИФОЗЦРЯШКТЛВЗРУЗЦЕСЦОДЖЖУБЮЕЙУКУОРКРЮЫКНЗЯЛИШТБИЦИЛАР
УЧЛУНАКСТЪЦТЛГЬНСИПЧКЦХНОТАМАРФУУКИПИУЩНКЗРЖОЙНОВНЦРЦЧБКЗСБЕТЖЦБ
ГКУХЮЧРУНГБХФУЯШРУЖЯГУЙЗЯФКЗУЬНАТИЙНКИСФОЙЗНЯТУХСЦЧНЦОЯОТНКФОХУЗ
ЯТРШЪЩЛЦНФГООФСБЫШЛИУКУСРХУСУБЮЕЗРОВСРАЫЮОУЧТЦРКЖИЧЧНПСУЧЧУСЮБАР
ЦАУИЬИУВЦРСТОЙКЛВННСЕЭЕЦЧИЦЗЙНОУБКРСФОХЦНДЮПХИАОЦЧЯУКУКМАРКЛЗЦНЪ
УЗЩЛЦУРЮСРШЙТЕЬЧСЫСКЧФХОКИСАОЗКЗЦННЧСЭОИШХДТУТТБЕХЗОВВУКЪГЕТНИЩС
ПМОЭНКЦЦБОЗУЪГОЧАХЦПКХЯВКЛКЫНСКЖИУОФХЕХННКШЯТКРДМЛУФУЯДУРЙГЬППРИ
ЛНУДЛСТНХНМУГФУЗБЦПБЬКОЛУНУЗРЯЙЧ

2. Разложить на множители числа:

   (a) 614786292995868181209275867177

   (b) 514248332584359472742370961682558860908268605541294595535167

   (c) 135914598984344880901026563176085127845781729525014469667146007076579615669875567574759230 7

   (d) 125311274961726887232835153324382315809186975161759243555141132678243192235643446787462907092742796139495751783620379166 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 71255279562169817319425830489000243005825097007205361294146830942851084703011$
   - $e = 5$

   Сообщение:

   - $M = 57579155962123715175092291915818432278870463754046892301137434441770447635087$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 32746041790116973271704405340671981155 7$
   - $q = 33477588500857293351062425815002628508 7$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 33821684126026691680288205014545659685386191009222566559324159543229752226626$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 11556332344253808264599410600054133002 3$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 50175014620553312990511344461524744204$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 22826419429305380642235961327463372113 1$
   - $g = 79250677345983023729785212513289361201$
   - $y = 11915184972239630216049469968106500130 8$

   Секретный ключ:

   - $x = 29706058303819407252744514938015892426$

   Сообщение:

   - $M = 18660744659751574177285266504996745420 0$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 14921838931788963295706635872265277109 9$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 325113426975525677804874822094300493897$
- $g = 131712014161576317289306293682306854957$
- $y = 17994170747514457187956484214872804715 2$

Сообщение:

- $M = 265419548638445032905889167304197738460$

Подпись:

- $a = 98217345457044693952743691734813281675$
- $b = 20192029816764121511726673969438078290 8$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 677$
- $g = 314$
- $y = 115$

Сообщение:

- $M = 401$

Использовать следующий случайный параметр для создания подписи:

- $k = 175$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 8$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 99

1. (a) Расшифровать текст:

ПЗМТОКМЙНКДМЗБЬСТЛЗМТСТОПДЖПДМЗДЖВКТЧЗКНБНЛМДБРДЦТБРСБМДМБЗРСЗЗВ
МДБРНЛДПЖДМЗДЛВКГДКМГБНПМЗМБКЭШДВНРБМНВФАДВКНВНЙЖЙОТВЦДБРЛВЦЗКРЛ
ЗКТЭСДАМРДИПЖРЙЖКНМЧБАПЗМТМНЖМИЦСНОПЗОДПБНИБЗМДСДАДОПЗОНЛМЗСРЗЬС
ОНСНЛНАПСЗКРНМЙЛПЫЗЗБМНБМДЗРЙЖКДИКРЙНБНБЪФНГЗЙПРМГДБЗХГПТЭСДАДБН
КЭВНРТГПЫЛПЫЗБМНБМАЪРСПНБЖВКМТКММДВНЗГНВГКРЫЦСНОДПДГМДЭТАЗИХДДПН
ГЗСДКДИНМЖЙПЪККЗХННАДЗЛЗПТЙЛЗЗТОКАДЖЦТБРСБЙЗМТКРЙМДИМНБЬСТЛЗМТСТ
НЦДМЫРЛДКНБЙНЛМСТБСДПКРЫЛНРСПЗММЖМЙНЛОКЧЗРСКТФЕЗБСЫЖРБНДЭАПЪЧМДЭ
ОТВЦДББЪЧДКЗЖРБДСКЗХЪЗЛЪСПНДРНЧКЗБВНРСЗМТЭЦСНБЧДАКВНПНГЗДРЙЖКРЛД
РЫОТВЦДББЪПТЦЗКЗЙПРМТЭГДБЗХТЙЙГТЛДЧЫМДОНРКСЫКЗЖОНОНЛГМДЖРСБЗСЫКЗ
ДВННАБДМЦСЫОКДЛММЗХТОНЕКТИАТГТОНРЕДМЪЛНСХНЛЧБАПЗМГПТЕЙНЭЖЙТСЗЛЖО
ЫДЛЗБНПНСЖОПДЛЦДВННОРКРСНЗРКТЦЗКНРЫЧБАПЗМТРКЪЧОПДГКНЕДМЗДОТВЦДББ
ЪЧДКЗЖРДАВНРТГПЫЖЙПЗЦКНМБЗРРСТОКДМЗЗБЗМНБСБЛРНКВКМНЗВПЗМДББРНАЛМ
ЪБДСЬСГДБТЧЙМДОКДЛММЗХЖГДЧМДВНОНОНМГНЦЫЗБМЛЗПНМНБЙНСНПЪИЙЖМДМОПЗ
БЖСЗЗЖГДЧМДИЙПДОНРСЗОТВЦДБТРСПДЛЗКМЛДМНВМДММЪДРБНЗВКЖЬСНЦСНДШДРО
ПНРЗКНМЛДМРМДГНТЛДМЗДЛЧБАПЗМРЙЖКСДАДОПБГТНСБДЦКРСБДПГНРСЗЭСЪЛМДЬ
СНВНМДРЙЖКЖЛДСЗКОТВЦДБТЙНДВНКЗХННЛПЦЗКНРЫРЛСЪПРРТГЗНСБДЦКДЛТЛНЕМ
НКЗАЪКНОПЗСБНЗФКЭГФНАЩБЗСЫЦСНГНЦЫЛЗПНМНБЕЗБГНМЗАЪДДЖВПЪЖКЗМЗЦСНД
ДАЪМДРОРКНЗСНОПБГРЙЖКРЛДРЫОТВЦДБЛНЗОЫМЗХЪМДОНШГЗКЗАЪАДГМТЭГДБТЧЙ
ТФНПНЧНРГДКЖЙТЛТЧЙОНОГЫЦСННАЛМТКЗФРКТЧИОПНГНКЕКБЗГДВНГНАПНДПРОНК
НЕДМЗДЙЙСДАМЖБСЫМДЖМЭГЗЖМСЫМДФНЦТМНАНВБЗГЗСЦСНЕЗЖМЗЭЛНДИПГАЪЖОКС
ЗСЫСДАДЖСНЦСНСЪГКЛДМРГДККСНКЫЙНМДСПДАТИСНВНЦСНОПНСЗБМН

(b) Расшифровать текст:

ЦХЦЧФКХФЮФУЫСБУРИЧДТНЩЛЦЗКУОБКХИКЯКГСШФУХЛСЪЦБРЧДКЛЯФЯФХСЮЭЙРЛУЯ
АОУКБШЦХБЗЗКООЬУРИХЯАЪНФЮТЧНТЧХРНЛЫШПКБФРЙСЦАИШРРАТКЩХАЙУЫЛЭПМТЛ
ВЧАПКФКХПФЯУЖЭИЪРЬХФГКОЪЧАЖТИПЦУРСМЪЧНСЧДЗНОЛЧУЙРЩЮАЦОВЕЗНЗЛДБНП
ХЧХЧУОИШРЛЬАСПООИШЧНЩГЧХЫСЧКЬХФАТЦХЦЕЙУПТАИРЗЛВЛЧЯЧЯТУЖЫЙКХИНЮНТ
ЦШЕЙЗИЦЪУЧЕФВНРЛЧОНУРИАЭРЕЩУУХРЩРИУФЩЦХАРОЪСФИЦДХНЩЧЪЙКОНГЗУЛТДШ
РИШАСТИЧЬУРЯРАФХЛКФУХРБЗУПУЩШРНИЛЪФУЪШЪЧКОВЯУФУФБШЦХОЭНСУВРНЗРФФ
ТШЖФГШЙУБЯРЦНФФУПРЛЫУЖУШЪРЦЯОЮХБЛИЯУЗРЩЩТРЕУЧОЧЦКЮШЦНФДУХСПДПУХР
ВУЗИУЯУНКАГТРФВАТТИЧЬУРЯРАСНРЩДЧУПЩЯМЙЖФГШЙУБЯФУЗФЩЗРИЛЪЦПКСГШРЮ
ЗЬУГУКЙЧУПФХРЦЗЛВЛЧЯИЮЦЗСЛГРУЕФЪНЦТФЭТНХВФЭШТЦАЦБДЩЦКРСИККПСУЙКТ
СЩУКЛЗЛЯЗТИИЪТТСЧДНЗЫЛХУЛИУЪЬЗСШБНЦЯТАПУХФВУКФТЬФУХЦЕЙНХЛГБУХИЧМ
ЧЛРУШЙЦЯЧСШФИЧПХЦТВБНЕУАЗТТЦЪТРТОГБССКВУЛЬЛРХШНФРНМТСЬЗШТСЬТУЖТЪ
СФИЦДХНЩБЬУЧСЦБУЙРСЧКНТФИРУЕСХУЦЦКВАТУНХУЗСЦЪРЦЯЧЯКГКУРЬЧСИНТКДФ
ХЧАФРЩРУРУАЗЙССХШФИЦЧЙЙСЭЧХББРБНЧРТЪХУРФФТКДЛГФУНФЫЧКФВАЖШЗЩЛКСД
ЛВШТФЛУШЦХЦАНЧЯИККЦСЧДУТЛЛАЖРФРФЖКЗУЕГЦЛЦАЧШЖФГШЙУБЯККСШБШЦХОЭСХ
ЯОФТУЕУЕКЪОИДУОЙЛБХНЗИАХТСПЬХКХЛЯТЗОЧОКЗРУЧЧКУХЧРНЕФАЛНЗИККЕФЩЗ
ХЬЛЯНУФББРКИИАФХСЧЮНТНФДУХЮЛЮХБЛИЯУЗРФДЗКЪСЬУКНРЯТЗОЧОКЗРЫАЧНДБЭ
ТКЗФФУРЯУЧКЖИЧБСЧФШФУСРФБХНТОГРУРФЧФХСИЪТЫЛСОТУМНГЧКРЭЪЗУФШЪННКИ
ЪТНОИЧРННФЦШЭРФФЧУХМЧЙКРВЮХБЛИЯУЗРУЧФУОДУУФЮШГЧЗСИФЗМЖСЯШЧЯУБКЧИ
ЦУШХЖФУХЧРФБУКШСФЙКУЛФТГКЧЦБТЦЧПХЬДДЦМТОГПНТЛДХТЗЦЧКЗЛЭХХНРЛФНМ
ФЛЮКОФШФКТРБЗФХИКЯНОЛНФКЦХУАЬЧСФЯЖАОФГЗУДФШЙКРФДМПОДЙКТЛИЬУТЩЛХУ
ЙТФЪСКРУАСШТФФКРИУЪГЬХФАТФУОГШЧФШФУЗОХВНПКУЪФШЖЭЧЗПСШАХАМЩЩТРИЙА
ЗЧССБКННОФТШОЛЮШИССАЗУБРАЧУУЭЧХККТЪТШХЩЮКХХИЪУПУФФЗРИУЯФУННЯЖАОУ
ВУЙЦИГПУУЛБУЧСТБКЧУ

2. Разложить на множители числа:

(a) 677322138179975735769812092649

(b) 723240890646708797446086316198473862465011271086347733874267

(c) 157934489156114604252895683056338911691755743813099997668542674149425385621143370149320515 9

(d) 194529338225257592346647411903511178048156095358837505176572877086582622669199084638823960060270479951973420358294427789 3

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 44964026580601401068011295044022572163247720899668461441514546937355490289137$
- $e = 17$

Сообщение:

- $M = 10145466576010694273243964734779113939641328943173645438870261842932481508689$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 25316515310217706182963745853032899969 1$
- $q = 32629908582383201254612756114070147401 3$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 865959158851830745992708839458933976071579713283659568762383744848540099617 7$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 13312379292831119350616233026108485172 1$
- $e = 3$

Зашифрованное сообщение:

- $c = 78496845580618994949574510817647734840$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 338501788809018270777315358571257161731$
   - $g = 610959969792740652392687876850984199 01$
   - $y = 201271133188718909093158926484388259044$

   Секретный ключ:
   - $x = 277434251247602847884851765511134584297$

   Сообщение:
   - $M = 256057338022622551028622970323082039612$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 120584072394345587569347921755325362 33$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 255236676668614592586161760985469159797$
   - $g = 139723931992912261783030456570088828575$
   - $y = 571930652867634294499045326783878222 01$

   Сообщение:
   - $M = 624899039785860613350026517074283509 61$

   Подпись:
   - $a = 528050797562458923384790568481807689 54$
   - $b = 321658884393534419104155361711545243 53$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 1021$
   - $g = 930$
   - $y = 91$

   Сообщение:
   - $M = 474$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 361$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 16x - 17$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 100

1. (a) Расшифровать текст:

ОЯПИЖЯСВСВМЛМПЖРЪРАМЖКОМВЖРГЙКХРМРИМЗЛГАГПРГЛГЛВМЯЛМЖНОЖВЛМБМЯЙБ
МВОЖЙПАГЙЪЖХЖЙГБПНРЪАМВЛМЗИМКЛРГПЕСОЖЛЩКОЕБМОХГЛЛЩЗЖАЕАМЙЛМАЛЛЩЗ
ОЕЯМЙРЙПЕСОЖЛПЛХЙПМКЛМЬОЕБМАОЖАЙМУМРЛМЛМКЙМНМКЙСПЙМАГБМПРЙЖОГДГЖ
ЯГППАЕЛГГЛИМЛГФАКГПРММРАГРЛИИМЗРМЕНОМПМЛЕУОНГЙЖНОЖПАЖПРЛСЙЕКМЙХЙ
ЖАПИМОГНМПЙГВМАЙГБМНОЖКГОСЛВОСБМЗВГЛЪСРОМКНОЖЦГЙИКОЪГЖАЛМАЛГПММЯ
ЧЖЙГЗПАМЖНОГВНМЙМДГЛЖМЛНОЖЕЛЙЖУЯЙБМОЕСКЖГЖРМРХППМКЛМЬПМБЙПЖЙПЪМР
ОВЕСОЖЛВМЙДГЛЯЩЙАЩПРСНЖРЪЖЕБМОМВАРМРДГВГЛЪЛГХГБМЯЩЙМКГВЙЖРЪРСРДГ
ОППРЙППКОЪГЗЖАЛМАЛМЗНМОСХЖАГГПАГЙЪЖХСЖВАГЗНЖПЪКМИКМЖКОМВЖРГЙККОЪ
ЖАЛМАЛЕНЙИЙНОМЧЗРГНГРОЛВОГЖХПИЕЙМЛРЖУЖКБМЙМПМКНОЖВГРПЙЖЛКСАЖВРЪП
ЖЙЖЛГРЯМБМВЖЛЫРМЕЛГРЛМАГИЛГЕЯСВСАПВМКМБЖЙЩРЩМВЖЛМПРЛГЦЪПАКМГКПГО
ВФГЛЖХГБМЛГКМБМРАГХРЪЙЬВЖЛПМИОСДЙЖЛГУМРГЙНОЖЛЖУНОГВАРЪПХСАПРАКИМ

РМОЩГКГЛАМЙЛМАЙЖЛИМЛГФМЛСГУЙАМЕАОРЖЙПИЕСОЖЛСБОСПРГЛЖКМЙХЙЖАМЛУМР
ГЙКГЛОЕАГПГЙЖРЪВСКЙПГЯОППГРЪКЩНОМАГЙЖВГЛЪЦСКЛМЖЯСЗЛМЖАГХГОМКАЩПР
СНЖЙЖАНМУМВЫРМЯЩЙМАИМЛФГТГАОЙЕЖКЕРОСВЛАЦАМГЛЛЩГОПНМОДГЛЖНОМУМВЖЙ
ЖЛЦЖБГЛГОЙЩБМРМАЖЙЖПЪИВОСДЛМКСПМВГЗПРАЖЬНСБХГААПГГЧГПРМЙНМВМОГЛЯ
СОБМККГДВСРГКМИМЙМГБММРОВЩПМГВЖЛЙЖПЪЖПМАПГУПРМОМЛНОЖЯЙЖДЙЖПЪИЕЙМ
ВГЗПИМКСБЛГЕВСЯСЛРСЬЧЖГВГОГАЛЖНОЖАЖВГЛЦЖУАМЗПИНОЖУМВЖЙЖАНМАЖЛМАГ
ЛЖГЦЗИЖОЕЯМЗЛЖИМААГЕВГЯГДЙЖМРЛПЖАПГНОГВАГЧЙМПИМОМГЖЯЙБМНМЙСХЛМГМ
ИМЛХЛЖГАПИМОГИЛЕЪБМЙЖФЩЛНМВИОГНМПРЖЬРРЖЧГАМЗОЕЯЖЙНСБХГАОППГЙГБМР
МЙНЩМПАМЯМВЖЙМОГЛЯСОБЖИЕЙМПЪЛЛГПЯСЛРСНМПЙГВЛЖЗЖОГЦЖРГЙЪЛЩЗСВОЕСО
ЖЛЯЩЙАРМАОГКМРОДГЛНОМРЖАСЦЗИЖКРГДЛЩУЯЦИЖОФГАИМРМОЩГОППГЙЖПЪНОГДВ
ГЛГДГЙЖКЩЖУСАЖВЙЖАГПЛМПВЖЙЛПАРРОПИМЗВГОГАСЦИГОГХИЖОЕЙЖЙЖПЪЖВМОМБ
ЖПРЙЖЛГНОМУМВЖКЩКЩСРГЦЙЖПЪАЛЦГКЯГЕВГЗПРАЖЖК

(b) Расшифровать текст:
ОАХРКДЭЗФПХЪЗДРТСФЭФМЮЪВЖРТЖЮРКЬИВКУГЛГФДШЮЮЩФЮГЩНУМКАДЗАСЧППЮКЙ
УФЫБФКУЯЗЬРЛЭЗЬРНЮИАНХФЖЪХУЫФКНКЬФЯЗРСФЙЛПЛВКХОШГВКМШРДРЯВЗЩПЩШЛ
ГМЙЫЗДЗШГЯЯЗФТЗЫНКЯЗЭМРТЖЪМСЮЭАУСХДЯЗДЮАЮРИЭЗАФДХРЭРПЭЮУХЖХЛБТЗЦ
ЭЧДЗЗЮВЪХЬМЮПРЦДГГКЫБФПГВИАЖДЮЙЕУМЪДЪМРЭЖНЗНОЭЪДЯВМЮКПГЛЕДХЧГАЗР
ВЫЧТУВБЧСТЮЙЕГНХЖЯРЗТКДЗПХИВРУГЖЕНУМКЧЖЕЮДАДУТЮЭЮКЗБЮРЛСЮЦПЭЩЭЦЮ
МЯЙАКЙЭЮГИНЮКДПЭЬЬАНРБЗЮПЖАЮЫСЗВЙАДКЗЫЦРФМЫГКНМЮФПГВЧКМФЛЕАЛСХЛВ
ПЖАЮЪЩОВМКМОАХЪДПЮЫЯГЗФАЭРЖХБФРЪЫБФУЗЫЗЪЙПХСОНКЯЮДТПФЙЧКЩЪЛАКЧЯЙ
ЪДЗЫСФГТШЖЭЗМБЮЫКДЭФЙПЗЫЮХМРХЮХРСЮЪЧТКГКЭЭЪЭЮЯДКБЛЯРЗШЕЮТЮШЫЯРДЭ
ЫГСНХКЯХНАМЬОКШЗГФНБХЯЗСЮЭФКИЭЗРСРБДЕЪЛБГЩНУТЮЭЮКЗМБРЪЫБЬРЕЮЖЪГХ
ФХФЗТМОАОМЯЮВЗДЮАЕПДБЛВЗЩГЬЕУТБГАОХЯЗЭМХШЫЧНКФЛОЙПВХБРНЪЗФПКЪМАГ
ПИЮЫРСБЖАУФШЭЬРЕЮЯЧСРБДДЮУГЭВЮДБЮЮНЮЗБКМКСМЯФХОЛЭРЪФБФУЗЧОФЩЗЭФЗ
ФКТЗДХИЭЭФРТХЭАПГАЭАГКАЧДУДНЛАДТХЕЩЖДХЙОАТЧЭЭРУМЖЧУМЮДОМРУЗЭРУЮЫ
ЮРНЗЭЭЙПЪЕДХЪЬЮЪОТМЮЪДПЮЫЯЗХФДЪФЮБЫЕЕРЫЗУПИШДГГНОББТКБДАПКЫКЬУФХ
ЖЧХУЬЗЫЖДХЙЪГФОСЬДЙЫИЪУФЮДЧФЭШЖАГРШОФЙДХДЬХТЪБЪУФЫИАЖНХЕЧПЙУЙЧОЗ
ЫАЮРМФЫЧТЮЮЛФРТШДГЮКУЗЭРДЧЮЮУМЮЬАСРЪАЭУЮГЭВКНЯЗЯЗЛБЪЭЗАШЗЯХСЫАХТ
ЖШЫФЧРФЫДХИХЕЪПХВМУФАИГФЭУВЙЧНКЫЫЦДЗАХЪЙСШКДРНХЛДРНЯЗГИЖТСЯУРВЪЧ
ИНБИВРМЫЛЪОКЯЮВЗФЙБЭЩЗАЮЩСРАЗХТПХЖАЕРШАБЗТФЫЧТЮТЖЕФТХЖЯЗАЯЮДНЗОЭ
ФРТСФЭСРЫЗЯДРЮЙЕИЗЭЖНЧНОЭЧЛОХЯЦХКЬБЕЙПЫСФГТШЖЯЗГЮВДЗУМКЬЙНЦЮЯЫКЭ
ЕЧУФМЖЦЗИФЫНГФОСЬХИХЪАНЗХЖЧУФАЮЭЛФХИАГЗАЮШЗОЯЗГНЗФЖЪЛЙАЭЮФХИГЮРН
ЗЕАНКЫКОГРУМЮТЮШЫЯРДЭКДРНЯЗЦНЗЭЮЧУПУЮЭЮУЪБЮУСЮГАЛУВЫЪЗОЮЯЪЖТХСЧП
КБМЦЮГЛЖКЗЛЧЭФЗТМЕЪТЙФЫЭКУММХТРЧФУТПМББТРЪДДКУВЗЭПУТЗЧООХКДЗЕЮЛА
ДУМБЩТХСБДЮСХЙФРЕЮКЮЗНМРЬДЖАМХЙНЮЭЧКЙЬЗЭЩНШМГНЭ

2. Разложить на множители числа:

(a) 575986920958806680368731949063

(b) 778680937520568617530884328924412679915227418248916625036283

(c) 10172792689416014001618573726443747152233486501515744350632147382250018490148558005675489 41

(d) 155933740623381329135971558746154851896162566328778778328921999339558676374709378944554150884472653032995829971718513005 9

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 603232130214060368023397334717940237787664796981218814987847190969022252699 09$
   - $e = 3$

   Сообщение:
   - $M = 384963062511096830845846126915222582046744209389735754069272801601833186640 44$

   В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 260151312594908681578485696724449046571$
   - $q = 255802670711856981448180373194994415209$

   Открытая экспонента:
   - $e = 3$

Зашифрованное сообщение:

- $c = 29507291815616862207157315859052701126640699396180687196238262829334081031731$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 22354959098695997294029494454876811777 3$
- $e = 17$

Зашифрованное сообщение:

- $c = 12472634032380896420187980529540644549 8$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 31829670578753899095242860796302505063 9$
- $g = 49688228872823849939947916088487235326$
- $y = 29004808743385873253206871982962479691$

Секретный ключ:

- $x = 22595082011654484823656661475340510047 7$

Сообщение:

- $M = 78569488992586402586251685625791755650$

Использовать следующий случайный параметр для создания подписи:

- $k = 26669132025811741322388786019642692110 7$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 27174236733705922669025365139622830755 9$
- $g = 42610833575065685511853256840126300230$
- $y = 12367673135763752004547040348990717088$

Сообщение:

- $M = 17582747569992085179783839070861744647 6$

Подпись:

- $a = 62736009070850377653456851391605727730$
- $b = 22145991711948829733298917649306566778 6$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 907$
- $g = 87$
- $y = 160$

Сообщение:

- $M = 89$

Использовать следующий случайный параметр для создания подписи:

- $k = 589$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 7x - 9$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 101

1. (a) Расшифровать текст:

ЦАЖТЦИПЙССЯНОФНХМЕМФМСЖЙЫСТЙУТХЙПЙСМЙХЙНСЙТКМИССЯНЧИФЙИЖСЙЧЕМПТЦ
ЪРТЙЗТТСПМЬМПХТЕЯОСТЖЙССТНХЖТЙНЦЖЙФИТХЦММЗТФЙХЦАЙЗТТЕЯОСТЖЙССТСЙ
РМЛПМЖПХАЖЗТФАОМЩКПТЕЩООУТЖЦТФПТСЖЯЩТИМЛХЙЕХЯСРТНЧЫХЦЖТЖПЖЛРЯХПЩ
УЧЗЫЙЖЕТКЙУФЖЙИСЯНИТЫЙЗТИТКМПЗТХЧИФЯСМЛЕЖПЙЦЙЗТТЦОЛСМТЦБЦТЗТФЛЖЙ
РСЙПЙЗЫЙСЙОЛСАХЦФЬСУФЭЧФРТНЧРЙФСПТЕСТРРЙХЦЙТЦХЦМЖЦТЫЦТУТЫМЦПХЖЦЯ
СЙВХЖТЙНХТЖЙХЦМТЦЙЪРТНУТХЦФИПЖРЙХЦЙХЖТПЯСХОМРМЩФЧЭЙЖЯРСТИЖТФСМСЧ
МЛРЙСМЦАХЖТЙНУФМХЗЙХТЙИМСМЦАХХФЛЕТНСМОРМХЧЕМНЪРМХЕЙЗПЯРМЩТПТУАРМ
ХЦЯИМХФРСЬЙРЧФТИЧМХУЧЗССЙЗТТЦЫСМЙРРЦЧЬОСЙХРЙПУФМСЙРУПОЦАМХЦФПХАЖ
ТЛЖФЦМЦАЙРЧЕТИФТХЦАЗТЖТФТСЙЖЙФСТХЦМРТПЖЯТЬЦОТХЦМПВИХОТЗТРСЙСМТЦЙ
ЪРТНЕЯПСЙЧЦЙЬЙСРФАМЖСТЖСРЧЫМПХАЕТПЙЙЖХЙЩЕЧИЧЫМЧЖЙФЙСЫЦТРТЗТУФЖИЦ
АХОТЗИЕЯЦТПАОТЛЩТЦЙПТСИТЗИЯЖПХАТЕМХЦМСЙМУТЫМЦПХЙЕЖМСТЖСМЪЙВРТЙЗТ
СЙХЫХЦМТСХОФЯЖПТЦЖХЙЩХЖТМХПЙЛЯМХЦФИСММРЙКИЧЦЙРСЙУФЙХЦССТИЧРПТХФЙ
ИХЦЖЩООЕЯРЙСХУХЦМТИСКИЯЖЙЫЙФТРЕЦВЬОХМИЙПСИМЖСЙУЙФЙЖЙФЦЯЖПМХЦЯУФМ
ИЖТФСТЗТОПЙСИФСТРЯХПМЙЗТЕЯПМИПЙОТМЫЦЙСМЙСЙУФТМЛЖТИМПТСИСМРТЕЯОСТ
ЖЙССТЗТХЖТЙЗТИЙНХЦЖМТССХЖМХЦЯЖПХЦФМССЯНРФЬРЦЧЬОРТПЫЖЛПЬЙФХЦСЧВШЧ
ШНОЧМХПЙЛЯМЛФЙИОТОУПМСЙЙФЕТЦЧЖИФЧЗРФАМЖСТЖСЦЧЦКЙХМИЙЖЬЛФЕТЦТНТЕЮ
ЖМПЫЦТСЙТЕЩТИМРТХЦАЙЙЛХЦЖПЙЦЙЩЦАЖУЙЦЙФЕЧФЗМЫЦТТСУФТХМЦИЦАЙНХУТХТ
ЕТЦУФЖМЦАХРЦЧЬОТЫЙСАТЗТФЫМПХАЛЫЙРЦЙЕЙЖУЙЦЙФЕЧФЗХОЛПТССЙЧКЦТРФАМЖ
СТЖСЩТЫЙЬАМЦЯСХУТОМСЧЦАРФАМЖСТЖСТЦЖЙЫПЫЦТЖХЕЧИЧЭХЧИАЕЙЙЛЖМХМЦТЦБ
ЦТЗТУЧЦЙЬЙХЦЖМЫЦТТСЙИЙЦМХОЦАУТОФТЖМЦЙПАХЦЖМУТРТЭМЧХМПАСЯЩПВИЙНОО
ИТЫАЫЙПТЖЙОУТХЦФИЖЬЙЗТЛХЖТВЖЙФСТХЦАТЦЙЪРТНУТЦЧУМПЗТПТЖЧЖХОТЙХПТЖ
ТСУТРМСВЭЙЙРСМРТЙУФЙХЦЧУПЙСМЙХЯСЕЯПТЙРЧЦЗТХЦСТМОЛПТХАОТПОМРЧУФЙО
ТРУТЙЛКНРЦЧЬОХО

(b) Расшифровать текст:

ЦЙЭАБЦАЮЧЙСРЦЦУОСЧЖОЧЗЭЪЗЧЖЭЦЭДПУЧЭЩЯШХЗДНЬЧЮОЦЯОЙСЕФЪЛЬЦФЦАЧОЯТ
ЙЧХБСЯФЖЬЧЪОЗЭЪЗКТАЫДЗЕКФНЫФАЫШУУЯОЖЩХЬЧИЬУЭФПЦЙЯОАУТЦЪЮЧМЬОВЦТА
ЫДШТЪЬУФТЬЫКФЫЩСКЫОЭЫКЩЯДЧСФУЭЯБФЯЫЪПЫОЫУОЧРВПБЦЙРДЗЧСЮЧБМТСДМПЙ
ЬСЪСЖЯМКХЕВЫЧФОЧЫБМТСЧМШТЯЬНЪОЧФЪКМЪЮЗОЕЬЬОЕПЧБЙОЙЬЧЖУЖЧЦКШТУЛЗЧ
ХЛЬЙЪЦЭФШУТЦЧЭОИЭХДЫТЮЧМЗРЭАЖОУЯСУОРВАДЫЙЪЧЭДОЬЧЮОСЬЧДЧЕЬЧНСПЧЫК
ХТШККШФФЧУОСЛЪЖЧФЭШМСЖКУЖЩЧАЪЖЧНЬЪОЧНЩОДНКФЪОФУЯОАШТЖСОЫАФОЮССЫЪ
ЮЧЙТЧКЫЙЖОНЫЖЩУЙОЖЮЩДХЙЯККФЙФШКФЙЦЦПЗИЪПБФЧУУИДЦЭЫУЪУЭФАСПЧССЧЦЮ
ЧЖЧСБЩЖЫЧЭКГЦТЬКЧФЧЖСОЕРФЦЛЧШЯЦТЬЛАУДШТЬОИОЪЩСДЛХФХЙЬОЫЦКЧСЮЩБНУ
ЭАБФСАУКЩТСДПАМБЕНЧЦЫОЙУТФУЖКТЪЫОЕУЭЩПЪХЩСДШТБЧИУКУДЕСЛЬЪГЦМЫФНЬ
КФЪЮЧМЫНБФТЫХЧПМЪСАЬЬСНПБЧУЩПМТТЧИОСБЧМССФПБФПЬЧЮЪОЭЩБЪЧУЕЭЦХЯРЗ
ЬЫЧФДЛТБШКУОЭХПЪПВАЪШФЖУЛФЫЩЫКФХБСМКИФЛЖСОЯСЮУТЯЧЮЦМЕУПФАЩУЖЫТАЧ
ЯФХЧФДЪАСЧАЦТСЩБХОЧЦПЫААХОЬЬЩОЮЦТТСЮССАЕЮШФФЪОЬУЬЧЕЪПРЧНЫМЧЪЛФЫФ
ХВФЧАЕЙХЧАЕБЧЕЭФШЪЦЧЛФОЗЭССЦЙЭШЧЫСЭЪОЕРБЬФУЬВЫДЫАМЫДХСФФЪКМЪСЛЧК
ЪЧЮФХЛКОЗЬЩОПЦЙТЧМЪУЯЛЭДПЩЧМЧЦЩЧЙЫТБАНШТБЩБКТСФЖЦПЛЗРЩСЕЬГНТЬЧВС
ПЧАОЧРВЪШОИСФИЦЙАЛКТЧЯЧЖКЦНБЖШТЗОЗЛРЭЗЖЧРЬЫПЛББЧЮЩЙЫККШФФЪЛФСЩЩК
ЛЦЧЪЙЧРЬОЮССЬЧНЫМРДЗРСБНБФТЫЦАЧЕЬЧГЦЦЛАОЧИЪХБЦЖКШДЪСРДЗСЛЫЧНУЖКМ
БЧЗЯЭДАЙАУЖЩЦЭЦЮСХФФЙЪЦФЦБКЙЦЧЮЬОЭМКЬУЭЫМОЕЪОЙСМУЛЙЧХЭКЗРСЬХБЦЬЧ
ЩДЦТНСАЧЕЯЧОЧВРЬИММЯОФСПАЪАОПБЕДРСФОГХЙШСЛЧПЛРПЪААЦКХЕЭШМОУЯСЙФХ
ЦЩЭЧЦВКОЗЬЩЛКБЙЪЛОЧХЫЧБЛФФХЖУУЯСЗПМСФИЧЫЪЕЙДНДЛКЪЦЩХЧЪЧУЧЭЩТШЦАО
КУДПЛМУХКСЧЮЩВЦЙЬСЮМЙЭММЭМЧКОЗЬЩНБЩСВФИОСЦЬСЧУЭЫКХУЭНЭОКЪУЭЧУЯОМ
РЕВНДФЙТЧКАЙЬЕЙОТАЫКЩТХЦКСХБФКЪЯЮЫШЬОЭЩДРСЫСЭЧУЯОЮЪРБОЙСМДЧООПРД
ЗЧУЯСЮЪЦБЕДЦЙЫЧЯЦЙААНЫСКТРЩСЕЬГКЯЪХБЩЦСЧЛЕСАОИЕЕФНКНМЬЧОЛЙБКОЗЬЩ
РЮЧФЭЫЛЩМЮЧАЦПФМКЪ

2. Разложить на множители числа:

(a) 693936231696656463775264205917

(b) 10753855523469610083058686294714518864915098665061652710159 01

(c) 774706663487737552882443264843212085216589418624861073372134322777813614395468769576398043

(d) 176839964793334547333524193778740759924943698085161075512774289660015502901791192700994750043924984726625442073854601720 7

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 690572135245141522915262221423584677596982358641417545098616331891714507322 91$
- $e = 3$

Сообщение:

- $M = 507419505139006694997614241026294562550324254775039523303659722825433413904 88$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 331550906915820575089539253310297539141$
- $q = 27837752549506127071465209597458961170 9$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 770096370413477119898009908523935946616102370200287608393492637205500037764 47$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 11870192973307202051882537284704857407$
- $e = 17$

Зашифрованное сообщение:

- $c = 444594392925168956878444313748662156 06$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 29617666603847201162979989540625972929$
- $g = 23664081814937411501327106573888104062 9$
- $y = 10225872415553178889117632147649499227 9$

Секретный ключ:

- $x = 29034052783858652342585537044507296541 6$

Сообщение:

- $M = 23655592973037338345876967714967987339 9$

Использовать следующий случайный параметр для создания подписи:

- $k = 27079853288077761272008278042543210332 9$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 335394824823469414753430485277135693153$
- $g = 15216841994363980923319383291490769155 2$
- $y = 16342972140334041750040395721228704265$

Сообщение:

- $M = 352711009892330495033447010849768179 45$

Подпись:

- $a = 10690328939834477840916656877820936413 1$
- $b = 28317106614307282936348623850700082226 0$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 607$
- $g = 428$
- $y = 241$

Сообщение:

- $M = 361$

Использовать следующий случайный параметр для создания подписи:

- $k = 433$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 2$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 102

1. (a) Расшифровать текст:

СУЖРЖСЭТЛЗЙГЛЛПНТПТУПОЙЙГЩДПСПЕТМГВПДФПУГЖШМГТЖВМДПРПМФШОПЙУЕТОП
ТЛГСФЛПРЙТЙТМЖЕПГМПТНГНПДЙМФТНПУСЙЩЭЕСФДЙЦДФВЙЩЭПХЙЧЖСЛОНГПМЖЯРС
ЙЖЦМУЬФЗЙГЖЩУЭЖДПСИГЖНМПЛСПГЙОУГПЖКТПГЖТУЙЙУЕТОПТЛГСФЛПРЙТЙТМЖЕП
ГМПГЬЩЖМГНЖТУЖТОЙНЙТГЖМЭЙШТУПМФГПСПУЕЖСЗОЩЙЦМПЩЕЖКРПСТРПСЗЖОЙЯЦМ
ПРФЩЙЛСФМЭОЬКПУГЖМНЖОГРСЙЛИОФЯЙИВФДЕЖНЖОПТУГЙМЙТТГЖМЭЙШЖНГИРЖСУЙ
ЕЕЭЛВЬМГУЛПНЙИФНМЖОЙЙЙУЕТОПТЛЛЮУПНФНЖТУФПУОПТЙУТРСПРФЪЖООДМГПУВС
ПЩЖООРФЩЛЙОЬНЙТПЦСОЙГЩТУПМЭЛПГШЖСОПГПНГУПДСХЖРСЙМПЗЖОЙЖРСПРФЪЖОО
ДМГНЬРСЙВМЙЗМЙТЭЛВЖСЖДНГПМДЙРПМЛОЩГТУФРЙМГЕЖСЖГОЯЙПТУОПГЙМТГОЖКО
ПШЖГУЭТУСПТУПВЫГЙМНОЖШУПОУПКТУПСПОЖГТЖЕЖСЖГОЙГИВФОУПГМЙТЭЩКЛЙРФД
ШЖГТЛЙЖВСПЕУГЖИЕЖЮУПЙИГЖТУЙЖНЖОТЙМЭОПГТУСЖГПЗЙМПНЬЕПМЗОЬВЬМЙРЖСЖ
РСГЙУЭТОЕСФДПКЕЖОЭФУСПНОЖУЖСРЖОЙЖПГМЕЖМПНОПКЕЖСЖГОПУЧНПЖДПОЦПЕЙМ
ТЭГГЖСТУЦРПУФТУПСПОФСЖЛЙТРСПТЙМОЖТЬЪЖУТМЙРЖСЖГПИШЙЛГТЖЛСЖТУЭОЖВЬ
МЙСЬВПМПГЬМПЕПЛВЬМПНОПДПРСЙЩЖМЛДСЙОЖГФЙПВЫГЙМЖНФПТГПЖНОНЖСЖОЙЙВЖ
СЖДЙТЭТЛИМПОНОЖПЕОПНФЖЦУЭПРТОПЕПЗЕЙТЭФУСНЬРЖСЖРСГЙНТРЖСГЬЖЙРСЙГЖ
ЕЖНГДПТУЙЛУГПЙНСПЕЙУЖМНШЖМПГЖЛДФТСПГОГТЛЙКТМФШКОТУПМОТГПЖНМПЕЛВЬ
МДПУПГТЖМГОЖЖТЕГФНДСЖВЧНЙПОЙПУШМЙМЙЙФЕСЙМЙГГЖТМОЖВПВЬМПТОПМФОТЙМ
РПДПЕВЬМУЙЦГПМДОЖТМТЭСПГОПЙТРПЛПКОПМПЕЛРМГОПЛШТЭВЬТУСПТЛПМЭИЙМРП
УЖНОЬНГПМОНРПДСФИЙМТГНЖШУЬГППВСЗЖОЙРСПЩМППЛПМПРПМФШТНЬФЗЖЕПТУЙДМ
ЙТЖСЖЕЙОЬСЖЛЙГЕСФДДСЖВЧЬОШМЙЩЖРУУЭТНЖЗЕФТПВПЯШУПУЛПЖТРСПТЙМПШОФГ
ЩЙТЭОЖИОЖНВПДГЖТУЭПУГЖШМЙДСЖВЧЬТНПУСГПЕОФТУПСПОФДМИНПЙРСЙОМЙУПЗЖ
ОРСГМЖОЙЖЙФГЙЕЖМГТФНСЛЖШУПУПРМЬГЩЖЖГОЙИРПГПМДЖОЖИОЛПНЬКРСЖЕНЖУРС
ЙВМЙЗМТГЖМЖМДСЖВЧ

(b) Расшифровать текст:

ЗЯРФГЮЕРЭЙЩЮМАДАШЖЭВЩЮДИПДПОЫТЩЧЖЮГВЮЮАЯЮЭСДЫЪЖУТЮЧЮЙЩЯЕВРЪЭЛЕРЗ
ЫЪЖФДЮЬЭМЙШБСФНГВЧКИАРШФЮЩЧГЗИИЖБГЙГЩЛКИНХШЖГЯЧБУШЦЯПКНХЯШОЙВЯБД
ДУГГЗЪНХШЙЫФВДРЩЬЕЫПЫБЕВРБФЖППЮЯШАРФЫВВЗЯЫВСРГЭЯБСДЭЯЖХЗАВЭРЮЬЕИ
РИУЕШЗПЦЬЪТЫХЮХРЖИЯВТДВЩФМНФВЮРШЯТДФДБЗФНЫЪЯШЕАЯЯЫЖЫЬВВТЮТЯЫИБВЮ
ЯЗЗГЗЯРЫФВАЙГИЩАКШЯЮГХЩЭЩАСЖЯЕЕКЖЬЬДЮЕЦЛЮЮГМЩВХЗГПАКЕЦДШУЫИЩАПСЦ
ЙБНВЭЬЫРШБЧЯКШВЩВРАБПЕРЧМЯБУГЦЧБОЗЯЯАШЫВШЫНДВРЭКЧЩЖЭЗЛЬГБХЭЫВЬЖД
БВЦЗЮЬЬЕРНЮЩШСДВЯШЖЙАДБНДЧЩАПДЭЗЭТЫВЖППЗЫЬЯКЗЮАЫДЪБЗЦОПЩЮДФБАВДО
ИБЬХФТУЕЕРЖЯБЖКГЫВАЗМВБХЪЕЫЗБГДБВЕКБВЮБОГЦЬДМЭЬХГКГЮЩВТЮЫЪШЪТЬЬХ
РЖЯЖЫФТВСЕРЭИЩЯДЖЦААЗГХЩЩПДУЩЕЗЖВЯШЕААВЧЭВЦЖДДЮЙРЭМДЮЕЯЗИЦЖВРЖЯМ
ЖЩИЯЪЪГЫХЦЫЖЮЙРЕОНГВЯЫЮЫЗЭЙБЫЕЖФДЭБХРЗГВЭПЮИЩЦРГЦЦЫИЙЫДБОЫТЩЮРЯВ
ЖШСЮХЕАРЩЯБШГШЯБХРГОЖБРЧЬЛЭРЙУЬЧЗБУЕЯРВХЩЮЗГЫДСПЫТХШНДЦВФННЫВЭРИ
ЯДБЗЕБЬАНЧМЯБУЕЦДХЙДГШЮЗГЮПЬЧДЬАЫМВКЬЭКЭЛЕАКБЭБШЩИЯВФННЫВВТЫХЦШЫ
БЯХЖТГВЯОЧБЯЖЯРОЮЬИОИЦЯИКЭЮЯКФДЗЩЮЭЫЯХБЙСТПХНЮЩАЫЙГЦЕШПСВЦШНТЩЛД
РЩЬЕАРЗЯААЗГЩЩЯОПЩЮДРШЦЖБДБУВГРИЩЖПУГЯЦШФЫБГБМЭЬЕЯПЫЮЩДКБЦБВРГХЩ
ЮУЪЯХГФТВЫФНЩЯЦГЗВЦБАРЪЯЕЮЗЪДТМЗЯВЖАШЮЩЬХЗБЦЯШЧИНЕЭРЖЦЩЯЫЮЫГБУАЫ
ЯАРШВЩВРЩЬШОДБЮЦБУИЯЮЮРОХЬФЗЬЬЬЧТЙЧББДЫГЩГОЫЧШЖФЫЭЛДРИИЕЖУИЮВХКБ
ВЕЫНТЮЩШРЧЬЛЭРДТДЕКБЯЕПДЧЦЯЖАИДЛЖМДГВГФЬЦЯБСДХПЯНЗНДБУБЩГБУИЦГШП
ГЯВФНЫФЯАЗЧЯГБЪЫЬАШНАЩЭДПЫФЬХЖЖДЧВРШЬЬЮЧБЯГПОЮУЩЕЗЖШЦОНЗХЩЮНЗНАЕ
ЗБНЦБЖГЯАЦПДУЩАКЫГЩЯПДЦБШГДВАШЪБЯЕПУДВБШИГМАЯРЖЦАХУЫЩЕКЗЭЬВАХЧБЬ
АЙАБЬКНВКЬЭГЫХХЖТГУПЦНГДЯЫЙАЩХЫФАЩЦДЗЧМЯБОЖЫЬХКЛЯДПДЫГЩГДСЬЕЕМДЪ
ЕХКЖЦГБЛШМДЪКИЦЯППДВЖЫАНГВЭЙБВВЧХОЦЦЮЗГЮПЯУГЦЧЪУСАЯЯЗГЩЕХЗБНЬКНД
ЙШЫЪБЩМЦРВЩЕЭРЖЯЕЕНЮИЖБИ

2. Разложить на множители числа:

   (a) 767990000815140728656986719279

   (b) 153098703012951209525936147710345099962053110648155101492059 9

   (c) 151977418774474083533468730700058930532413483760040323349266209176747451419141629902692730 9

   (d) 111257280135942112189071736813529843735126976599062835239620618227069867139834678319066563044982410153202566326941371188 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 4955658538467850572876228855514410329664254974923261655684308582058333310161 1$
   - $e = 5$

   Сообщение:

   - $M = 1875751558965725210690532534068619015180504455203140981377794244005618385583 0$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 220071047033173284594129966477804501167$
   - $q = 337945012413973847569905573080531685557$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 155258016693419657379429676217787911573122962003477306556414412933582119135 77$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 124847641929468335030017277656434747587$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 575367243143321242759179168636571241 3$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 248079566217424172556553360186451258249$
   - $g = 203162840192140376024457211833215049328$
   - $y = 80640311623443038514180445176103199428$

   Секретный ключ:

   - $x = 238824312150995776853812373390468678732$

   Сообщение:

   - $M = 143915366470260517744248847324938456561$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 852975179177223089342265438818574216 61$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 184971929464721691101501866103958731063$
   - $g = 130070014755180551337882452590626406202$
   - $y = 536916699605886708520355733963738521 93$

   Сообщение:

   - $M = 191443120659965126735818958653112684 86$

   Подпись:

   - $a = 928202492972308390970114437278137256 66$
   - $b = 891419310128151306718871695564321132 24$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 929$
- $g = 364$
- $y = 495$

Сообщение:

- $M = 892$

Использовать следующий случайный параметр для создания подписи:

- $k = 511$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 5x - 5$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 103

1. (a) Расшифровать текст:

ДЗЖКСАГВЪЖИЖКДЕЖЪЬИЛЫЖЕАЕЙЖЙКЪАГАААИЯЩЭЮГАЙФЪЪЖИЖКЪТЭНГЫИАЕЭЪАЯЕА
ДОЭГУБХЙВЬИЖЕЙЙЩГДАЕЫЖГЖЩЛЕКЖЪСАВАЛКЭВГАЪЖЪЙЭЙКЖИЖЕУЫЛЙИУАНЗИЭЙГ
ЭЬЖЪГАИЛЩАГААНЪКГАЪЗГЭЕЫИАЕЭЪЙЖЙВЖПАГЙГЖРЬАЗЖВГЖЕАГЙЩКЦРВЭАДКЛРВ
ЭАВИЭЗВЖЗЖЮГДЕЭИЛВЛВЙККАЮЭЗЖЬЖЙЗЭГЙВЯГЖЕЕДЪЖКАКЪЖЕЭЪЭЙКДИФАЪЕЖЪЕ
ЗЖВИЙЕЭГЗЖЛРАЩКЦРВВЕЭДЛЗЖЬЖРЭГАЩГЫЖЬИАГЭЫЖЙЪАЬЖДЙЗЖВЖБЕУДНЖКАКИЖ
ЕЛКУДДКЛРВЖЩЕАДГЭЫЖЕЯУЪЕЫЭГЖДАЯЩЪАКЭГЭДДАГЖЙКАЗИЖЙАДВЕДЙВЯГЭДЛЩК
ЦРВАЗЖЪЭГЭЫЖВЕДЪЬЖДЗИЖНЖЬДАДЖРЪЩИАЕЫИАЕЭЪЖЙКЕЖЪАГЙХКЖВКЖЙЗИЖЙАГЖ
ЕЫГЬЕИЕЭЕЖЫЖХКЖЙДЗИЭЬЪЖЬАКЭГФЕПГФЕАВРБВАЖКЪЭПГДЖБЖКЭОЙЕЭВЖКЖИЖБЫ
ЖИЬЖЙКФЦЖЩГАПЦСЭБЙКИЖЫЖЪЖАЕЩЖЫЗЖДЖЫЬИНГЖБИЛВЭДЖЭБЕВЯКФДЖГЖЬЖЫЖЯГ
ЖЬЭАЖКЖДЙКАКФЭДЛЯВИЖЪФДЖЭЫЖЙУЕХКЖРЪЩИАЕЙВЯГЫИАЕЭЪЛРЪЩИАЕЖПЭЕФИЬЫ
ЛЙИУЪЖЯФДАКЭЭЫЖЬЙВЯКФЕРЭДЛГЭВИЦПКЖЩЖЕЗЭИЭЪЯГЭДЛИЕЛАЩЭИЭЫЭЫЖВВЯЭЕ
АОЛЖВРЪЩИАЕЕЬЖЩЕЖЕЭЗИЭДЭЕЕЖЗИЭЬЙКЪАКФЪЙЭВИЭКЕЛЦВЯЕЙВЛЦВЖДАЙЙАЦЖЕ
ЖЬАЕАЯЫГЪЕУНЗИЭЙКЛЗЕАВЖЪАЗЖВЯЕАЭЫЖЬЖГЮЕУЩУКФЪЮЕУРЪЩИАЕЖКВИУГКЖДЕ
УБЪЯЫГЬЕГАОЭЭЫЖЕАПЭЫЖЕЭАЯЖЩИЮГЖЙФВИЖДЭМАЯАПЭЙВЖБДЛВАЫЛЙИУЖКЕЭЙГА
ЭЫЖЕЗГСЭДУЪЖРГАЪВЖДЕКУЙКИЭЗЭКЖДЙДЖКИЭГЪЖВИЛЫЙЭЩЗИАЗЖДАЕЙЪЖАДГЬЭЕ
ПЭЙВАЭЫЖЬУЕАПКЖЪЬЖДЭЕЭАЯДЭЕАГЖЙФЪЙЭЩУГЖЕЗИЭЮЕЭДДЭЙКЭРЪЩИАЕЕЭЬЖЯЪ
ЖГАГЭЫЖИЯЫИЩАКФЙЖНИЕЪЙДЖДЙЪЖЭДЛЕАЮЭЕААЕЭЪЖГФЕЖЭЖКЪИСЭЕАЭЖКЩЭЙПЭЙ
КЕЖЫЖВЖИУЙКЖГЦЩАЙГЛЫАЪАГАЙФЪЗЭИЭЬЕЦЦЖЕАЕЭЛПЙКЪЖЪГАЪЩЛЕКЭАЖКПАЙКЖ
ЫЖЙЭИЬОИЬЖЪГАЙФЕРЭДЛАЯЩЪГЭЕАЦЙЪЭГФАПКЖИЮЭЙКЪЖЪГЕЬЖЩЕЖЯЕКФПКЖЪЖЪИ
ЭДКИЭЪЖЫАЗИЖАЯЪЭЬЭЕЕЖБЕЗЬЭЕАЭДИЯЩЖБЕАВЖЪЖЕЗЖЩЭЮГЪВЖЕЦРЕЦЫЬЭЙКЖГР
ЪЩИАЕГЖРЬФЖЙЭЬГГЭЭЪУЪЭГКАНЖЕФВЖАЩГЫЖЬИЙЛДКЖНЭЕЭЯДЭКЕУДЖЩИЯЖДЗЖЙВ
ВГВЗЭИЭЪЖЯЛЖЕЪЙКИЭКАГЗЖГВЖКЬУНЪРАБЛЮЭЗЖЙЦЙКЖИЖЕЛЪЖГЫАЫИАЕЭЪЛЯЕЪЖ
КЕЭЫЖЖЩЕРЭБЖЗЙЕЖЙКАЪЭ

(b) Расшифровать текст:

ОЖНГЩИЕИЯЙПЗЯУЯГЗЮСОВЪЫМЭИГПЭЯГЯТШНЛБЛАЙЛГЕФЙЯЕСУЙЖМИБНЛГЖЮТГАСТ
АИЗПВЦЯИЗХУЪВФЫОДЦИЭМРГЬХДЛИЪШУЪЖЗШМФЭТЫГЛЪЕЮЛГВДГЛБЪЗХЖРСХХЬГВИ
ЗАБГУБМГВЛХЭОЪЗЭЙКГОЮЯМБЦЗАЙГЕХЕСЖИУЙВВПШЖМЖХШКОГФШЗМЗССАВЗЯГЗГВ
ЪБЙРМФГИГАИУТГДСФОКАТАЙПЪДЪТГБЦЯЙПАЦЦГЙГПЭАРГЪВЙГОИТОРЕССАКЗИАГЯ
РОГБГШЕАЯЖЭФХЛДВХЮЗИИЗННМБИЭВАЪОЮЭНГОЪГАШОГРСУНААНГФВЧЛШУЭГФИНШЛ
БЭКЪДПЛНШРПЗИЯАЗГХЮЬГЩОГИВЕИЪЛЙГЕШТАЗУЮАКЖИУЙПЗУЛЗВПБВИРГПБНОГЖЭ
АКЪЩЪШИГРЮЗЖЛУБНАГЕЫВГШСБНМАСЬГВИПОТРГФВЛУЧЛФАРСЛЭЙБЩОШУЛЪЖЮЮМЖХ
ЧМАГИОРМАСБНМУХАКГЬСОЬЩАСВТПЗЛЯЛЖМЛЭЙЬДСБКГНРЮЮМИЗЫАЛЭПЮАБГЕУЛЛЭ
КЮИЛЩУГЮМЮЗХИЪДУЮМРЭОБМБЪРХЛЙГПШЙРДУТГЙЖНЬАПЗЦЬЙГШСЭВЛМИЭГБАЕЪЛГ
ДСБНЪБЮТПМЕХХСЖЭЙШЭГБШЫАЯЪЗШЗЖЧСФОНСИЬЕИАБВЦГЧУУГНЕЛФОРЯРЬИНЭУЮЮ
ЖЬЗФГКШСБНКДЛАОЦЯЦЧЛВЭПЪЛРЪЪМЩНИЫЪОПГОФНПЯТХМЛЖХАГЛВЮХЖЬЩЛЬЙЗЦХО
УИВИФЙОГФЫЧЯЪОЮЮМЕФЪЕОЪТЮМРСРЕЙВЭОБЧАЖСАЙИЧИАМРКСВЙОЪРСООШЗЮЛМШЫ

ЫКМЯУГНМБЦСАОЪЖГГИЕИЪАЧЪРХВКЪУЧЖЖЪИБЭЖВЩЮЭЩЪЕЮЖЛРЖАОПЗРЮТГЕРХЖЖЧ
СФИМГДАВЛРШСАОЪЖЕКМЯУЛНЩКДХЖЩБФЭАБГПЧИЖБЛЯЛМЖХШЛЙЭФМЕЖЕЖШВПЯЛХМР
ЪТШКМШУГВЖАФТЛЕБЮИЖГВЛСЙЙСЫХЩХЖХШЩНЪЪЫЧЛРИУЛЛЭКЮИЛЫЛЧИЪБОЮГКЪОФЖ
КЪРЯЛЖЧОХЕРЪОМИМЖХШМРЕОБЭМГДАВЖЗЯБАЯЪНЯГРВПШЛМВСТЗМЪЖЮЬСЩЦЙАБГРЗ
ЖЪВЛЪГНЕИФМРЧОЫАБГФВЛМШЛЬМГЕЗШНЩБФВЛЖЯСЬИГЪРОФЖБРШТГШСЪЛМБИБЭМЪМ
БЖСЫДЛГБГХЮЭЩБКТМИИБСАЕЩИЫГФИФЦНЪБИЭКМЩУХМРВШЫАЯЭРТЙВИПХБВИХХЗЛМ
ОЮМКЪУЪНЪЖПЛАУАЛФЙАГОМИМЖНЮЛМЩОХТГАЛФЙИЕИЯЙПЗЛБКОГФШ

2. Разложить на множители числа:

   (a) 913741589426479008943062426437

   (b) 10169328510738584578552117153769155411591727804813856493221 47

   (c) 11961566312688977617587065535323087824530189423460255249611721108762952404566210870023119 21

   (d) 18267799464843011673680570554414789775867830106991842041927077435609023457547664306275659708173756409569004552933732992 09

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 65350166880359350711845208026938816126192664246292535411549292827808296200111$
   - $e = 3$

   Сообщение:

   - $M = 10760048941818950600649405577400438336903404392687038475158357778043074344884$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 185109344333826420449393127993715952069$
   - $q = 198266209642090595904357522746589937993$

   Открытая экспонента:

   - $e = 5$

   Зашифрованное сообщение:

   - $c = 943540334081149534293462419196972617624432297095071993079814460682314910 6081$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 163019697804944371882156467110414630821$
   - $e = 3$

   Зашифрованное сообщение:

   - $c = 116112136920173947053983956357328471 47$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 24641475349764301573678801133645561824 1$
   - $g = 24291378379373179492590364878525371845 9$
   - $y = 13928762216691476744492682377178198276 7$

   Секретный ключ:

   - $x = 27305587173127849572408168488494531691$

   Сообщение:

   - $M = 24741576180558430589269018028412529036$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 11582362376044305105805117516278623039 9$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 30360491013301552507920955491890444562 1$

- $g = 254323130841996898007090860027546084849$
- $y = 28584724888444230942442536950984332792 8$

Сообщение:

- $M = 10384534165069548870535211763720440862$

Подпись:

- $a = 55762874099449857192022834669363482782$
- $b = 27677249010110070675821223728133745418 4$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 1009$
- $g = 206$
- $y = 199$

Сообщение:

- $M = 944$

Использовать следующий случайный параметр для создания подписи:

- $k = 647$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 16x - 13$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 104

1. (a) Расшифровать текст:

ПЗБИРЗОНЛМЗОНРКНБЗХТАДПДВЗОКСЫДРМНБТЦДРСЫРЛНКНГТЛСТЧЙБРКДЖФМЙЖЪБ
КЛМДАДПДЦЫЛНДЖГНПНБЫДРБДКЫЗЦТРЛНСПДСЫЖГЗССДИМГДКЗМЛДМЖИЦЗИСТКТОР
БДПФТКЗРЫЭЧТАТРДКБЙЗАЗСЙТРРБДКЫЗЦДЛЗНСОПБЗКРБГНПНВТНАКЗБРЫРКДЖЛЗ
БСТЕДМНЦЫОПЗДФКБРЗЛАЗПРЙВГДГНКЕДМАЪКОПНАЪСЫРТСЙЗГКЖЙТОЙЗМТЕМЪФБД
ШДИЦСНЗАЪКНОНПТЦДМНРБДКЫЗЦТНРСМНБЗКРБСПЙСЗПДРБДКЫЗЦРТСПНСОПБЗКРО
НКБЙЛРНРЙТЦВКГДСЫЗЖНЙММВПЖМЪИОДПДТКНЙОНЧДКАПНГЗСЫОНБРДЛЙНЛМСЛБНЧ
ДГБАЗККЗПГМТЭТБЗГДКБЪРНЙНВНАПЗМКДССПЗГХСЗОСЗРГКЗММЪЛЗЦДПМЪЛЗТРЛЗ
БФКСДРЙЗДЛБПТЙДЗРСПТАЙНИБЖТАФНМЗВПКРЛПЙДПНЛЙНСНПЪИОПЗБЪЗВПЪЧДБЪО
ЗБКПЭЛЙТБНГЙЗОПЗОПНЗВПЪЧДГНКЕДМАЪККДЖСЫОНГАЗККЗПГМЦДСБДПЗМЙФРСКР
ЛНСПДСЫМЗФЗВПТЦДЛГНКДДНМОПНГНКЕКРЫСДЛОПНВТКЙЗМЦДСБДПЗМЙФРСМНБЗКЗ
РЫЦШДОНЙМЙНМДХЛПЙДПНРСКРОНГАЗККЗПГНЛАПЗМОПНЗЖМДРМГМЗЛМДРЙНКЫЙНРЗ
КЫМЪФБЪПЕДМЗИББЗГДМГВПНАМНВНРКНБЗОПДГКНЕЗКЛМДРЪВПСЫОПСЗЭНСЙЖКРОН
МДТЛДМЗЭЬСНОНЙЖКНРЫДЛТМДБЗГЗЛНЛТРСПММЪЛНМОНВКГДКМЛДМЙЙАЪРРНЕКДМЗ
ДЛНГМЙНЛЪПЖВНБНПЗКЗРЫТЖМКЦСНДВНЖНБТСЗБМНЛЗБМНБЗЦДЛЖТПЗМЪЛЦСННМПН
СЛЗРСПВТРПРЙНВНОНКЙТЗМФНГЗСРБРЗЛАЗПРЙДОПЗОПЗДЛДПДЙПТСРСНЗСБСПЙСЗ
ПДЖТПЗМОПЗВКРЗКЛДМНСНАДГСЫРМЗЛБЛДРСДЦДЛАНВОНРККОНРНКГСРЙЗРНФНСНЭ
РНВКРЗКРЛЪРДКЗЖРСНКЖТПЗМОЗКЛМНВНЗОНСЦЗБКЗЛДМВНБНПЦСНМГНАМНОПЗБЪЙ
СЫЙНРКТЕАДНМПРРЙЖЪБКЛМДПЛДИРЙЗДМДЙГНСЪНСЙНСНПЪФРНРЛДФТЦТСЫМДБККР
ЗЛЪБРСКЗЗЖНРСНКРНБДПЧДММЪЛЗОПЗСДКЛЗСТСБЪЖБКРНМБЪТЦЗСЫЛДМЗВПСЫМАЗ
ККЗПГДЬСНВНБНПЗКНММДНАФНГЗЛНГКМЧДВНАПСРКТЕЗБНВНБОНФНГДМОПЗЛДПОПЗ
ГДЧЫБЛДРСДЦЙНЦДЛОПЗЙЕДЧЫЖМСЫРБДГЫМДБРДЕДАЗСЫЕЗГНБОНМДБНКДОНИГДЧЫ
БСПЙСЗПЗРСМДЧЫЗВПСЫМАЗККЗПГДГКСНВНМГНАМНТЛДСЫЗВПСЫРНБДПЧДММНАЪКТ
АДЕГДМЗРАНКЫЧЗЛОПЗКДЕМЗДЛОПЗМКРЖТЦДМ

(b) Расшифровать текст:

ЦСЬДНОЫЩШУВЬЭЧЦМЧЬАЦЧЦШДОЧЪЦЙГЫОЦЮЭУШРЖРШСЬШЧЧЗЪЫЬОЦХЙЪЧЦРЗРОУГШ
МЩСШЙХЧЫЩЖЖТЧПЮШЛЧНЗРТУЫЫЪЧЪЭЮЧЧМЩМРЦСЭТЪЩЧУЭНОНРГУЪЫУЛЩЫЛЩЖБШЧЬ
БРХФРГЗУЧОДЪЩОПЮЬФЧНЮНДЦЮБУРУЫВШЪЛЩФЭОЫЫЪХЬСЪЖЩАОЦЫЧЬЪЦЫПЬЗДЮРЪЫ

УОХСХЖЗЦЕФЙЧЩЛЦЮЮЬЫЩРЧЦЫВЮЗЗШЩРАЫЪЦЮФТКДЭТУЮХГЙУРКРЩЧДБЦФНЧФЗГЩЪ
ЫЗЕЩФЬВЮЭЕЦЩЩЦРАЭДЧШФРГУФСНЗРХСШЙЭЦЧЪЖРНЧЧГЩТЧШЮПЬЮНДЧЦОЬВЮЫСЦЮЬ
ЧУЫЙГСФУВЩТШЩАЩТЫЖЙТЦЛЧДУЦШЬИУЪПЦТЬХБШЪЩХЦЩЯТЩХРГНЪОФБЙЫЧФНЬЫСУН
ЭЧШЦЫШОЦЭДМЧТХАЭДЖЭДШЮЧПЮГЕЪЪЖЩЪСЦОНКЩУГЩПСПЕЩЮЛЦСХУНШЮЧЦОШЫЪЩОЧ
ЫШЦЧЬБРНЬРВЩТЦЩАНОФУАЩТХЩЫФНЧЬЪРБЛМЖУЦЧМСХЦЧНЫШЦЧЬГУЪЮЩЪУЫОЦТШДТ
ЫЫГСЫРБЗЦЧЩЧЕЛСЦНЭЧШРЗШХЧШЫАЧЩЩОЪЧАРВЮЫУЬЕЫЧЪУБРМЧЬАЫДЛЬШЩЗНЩЗПЬ
ШЩИЩХЬЩИНОАЦДШАЫЩИХСОЬИУЮСПДЬЫЧФГЖЬАУИРФХЩЫОЧЛЬЮЦЕУУЖУФДВИЫОНЗАЩ
ЛЪХДОЧСЩНРЦЕШЕЩХСШФЭХЦРЫОЧФЙЧЩЛЦЖЫХЬШЦЫЭЯДЭЙЭЧЦНЭЦЧЫЧЫШЫОЭЖПУЬУГ
ВФЦРВУФЧЬЫЫНЧЫЭМСЩЭТХПНЖЯЬЫСАЮХПНЩЫЬФЧНДУРНРШЬЕЦПДЧЦЧФЗЧДХХДЦУСЧ
ДМЩРЩВШОЛЖИРЩШРБНДЩНБУРЩЮАРМЧЧДЙЫОЭЖПУЬУЗХРФВИЩЬПЩИЫЧНЮГРШЧХЬЮОХ
ЮЗНЧСАЗЩАСШЫШСТГШМЩСШЕЩЪХРБЬСЦПУЭЧТЮЩЫЧРЩФЪЧЪЧДЭЩСЧЗХРФЩГЬНОЫЬУБ
ЕЦЮЭДЪНДРЪФЩШЩЪЫУЛЩЫЛЩЖБХЦЮЬРЦЪЦЙГЫОЦТХУСНГЮУЬТВУАЬОЖЯСЦВЮХЛЧПАУ
ШОЫЫПЧКРЪЩХУЭДИЫХГЕРЩОПАЩЫЧЫДФСРЕЗШОБЗЗНЦОСГЩТЪЭЖЬЫСУШЦЗКЩШШЧТШЕ
ЬЫСЮЬШОХЫТЦЕСНГЩЛЦШЫЭЛЧРЪРФЧЩИНОАЦГАХЬЫЗЗУЫЩЧЖЦСМСЦЖЫЧОШОЫЫМЬЗШ
ЮЭЛЧРЩШХЦРГУЦСЭШЩСЮПД

2. Разложить на множители числа:

   (a) 4978002121075156330659946956 79

   (b) 8778624624494736402937004370606246624438694174834253779991 99

   (c) 8357644998508267873234249007522762912426113371047925197414528775036855702235592991202649 99

   (d) 7384241946429634659814093257878246224337331442666497990235149248149253413885684050465749205549386579788307956150485788 17

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 737989870507409408351854125964372360305444871934218572452047713441300007031 81$
   - $e = 5$

   Сообщение:

   - $M = 256516314192531749560443836759128681772069307168108941180376227863629613060 8$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 178573614471237545690108700036449966891$
   - $q = 310087340907698150343557456407316513489$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 54885402598906520862570339006823488477575820003597290765604835803861582473913$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 22365631882374631468921936315797440961 1$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 17389815158105390809133010430187635440$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 27811466955822950447505253553272586961 1$
   - $g = 21037905142096587790413414814506082293 8$
   - $y = 11309727078967754096650799025457885667 4$

   Секретный ключ:

   - $x = 61288395809070333074235018215380418448$

   Сообщение:

- $M = 27114422313916563679257918079850245968 0$

Использовать следующий случайный параметр для создания подписи:

- $k = 25527816499794454062052281662272538 0519$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 25612435695044071841021663858912031 9029$
- $g = 17900266465422401602127055706120789 2500$
- $y = 12173906445305287333019983327981357867$

Сообщение:

- $M = 14049644487991802472423783051472392 3719$

Подпись:

- $a = 47410903579630321739873955551919954931$
- $b = 18413646221822742698162147000844899489$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 647$
- $g = 413$
- $y = 523$

Сообщение:

- $M = 283$

Использовать следующий случайный параметр для создания подписи:

- $k = 213$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 14x - 13$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 105

1. (a) Расшифровать текст:

ЙИЗАИКЙЮЖЯЦЭЭИАЯЙОЗАИГГЙЬЙЛЙНГЖМЕЗНОУЕАЮЙЭЙЛАДТНЙШНЙВИТГНШНЙИАЬН
ЩУЕГЕЕЕЙДЗИАМННГКЛЙМГНЧЬЖЮЙМЖЙЭАИГОЗОБГЕЭМАЛЭИЙКАНЛОУЙНЭАТЖЗИАЗН
ОУЕШНЙНЭЙДКЙМБАИЦДЙНАСКЙСЖОДОИАЮЙЛОТЕОГКОМНЧЙИНАЬЬЖЮЙМЖЙЭГНИАМЙЮ
ЖУЖМНЙЮЯЗОБГЕЭМЕЙТГЖМКЙМНАЖГЭЦРЭНГЖНЙКЙЛГВВМКГИЦГМНЖЗРНЧЭЙЭМАМНЙ
ЛЙИЦРЙНАЖЬАБНЧГИАЗЙЮЕЙЗИНИКЙЖИГЖМЧЗАЛНЭЦЗГНАЖЗГМКЙНЦЕЖМЙНАЖГМЕЙЖ
ЧВГЖЭЕЛЙЭЭЦРЖОБРМНЛУИЦДЗОБГЕЖМЕЙЭЙЗАИЕЖГЕЖЮЙЭЙЛИАЬЙДМЧКЙЯЙДЯГКЙЯ
ЗЙАЬЖЮЙМЖЙЭАИГАОБМГИАЯЙОЗАИГАЙЭЖЯАЖГЗИЙЩГЭШНОЗГИОНОКЛЙМИОЖМЖЙУЯГ
МНЙЖГМЭАЖЧГТЯАЛЮЖЗАИВЛОЕОЮЙЭЙЛЭЦРЙЯГМОЯЛЧКЛГАРЖГЕОЯКЛГАРЖГМКЛЙМГ
ЖКЛЙНГЛЮЖВИКЙМНЙЖЦДЯЭЙЛЮЙМКЙЯЧКЙЗЙЮИНЕИОЖГМЧКЛЗЙИВЬЙЛЭЦРЙЯГМОЯЛЧ
МЕЙЛААЯЙЬЙЮЛАДМЭЦУАЖГВЕГЬГНЕГЬОЛИАФАКЛЙЯЙЖБЖМРЙНМЗАИЧУАЩМГЖЙЩЬЦЖ
ЙНЕНАЗИЙТНЙРЙНЧЮЖВЭЦЕЙЖГРЙВГИЭМНЛАНГЖИМОЭЙЛЙНЯАЛБПЙИЛЧКЙЯКЙЖЙЩГЭ
ЭАЖЗАИЭЮЙЛИГСОНАМИОЩИЙЯЙЭЙЖЧИЙТГМНОЩЖОТГИЙМЭАФЖААИМНАИАЭГМАЖЭГИН
ЙЭЕГЭЦМЙЕЕВСЕУКЕРЙВГИЛЙЯЙЗГСЕГДЕВЕЕВЖМЗОБГЕЖАНУАМНГЯАМНГАФАМЭАБГ
ДГЬЙЯЛЦДМЭАЖЧГТЭИАМВЗИЙЩКЙЮЛАЬАСКЙНЛАЬЙЭЖЙЮИТНЙЬЮЙНЙЭГНЧТДЕЙНЙЛЦ
ДИГЕЙЮЯНЕИАЕВЖМЗИАИОБАИРЙВГИКЙУАЖРЖЙКЙННЧЮЯАБАЭЙБНЦДМКЛЙМГЖОМЭАЖ
ЧГТВЯАМЧЭУАЬЖЮЙЛЙЯГАЙНЭАТЖЗИАЮЙЖЙММЭАЛРОЭВЮЖИОЖИКЙЖНГГОЭГЯАЖТАЛИ
ОЩЬЙЛЙЯОГЯЭМЭАЛЕЩФГАЮЖВТНЙЬЛНКЛЙВЬЕЕИАКЛЙВЬИОНЧЭЙЯИЙЗРОЯАИЧЕЙЗЛЗ
ЕАЬЦЖНОЖОКЯТНЙЮЛАРНГНЧВЖЙБГЖЭАТЙЛОСЖЙЭЖЧИГЕЗЙЛЙВКЙЕВЖМИАЭАЖГЕЭШН
ОЗГИОНОРЙВГИЭЙУАЖМЕГКФГЗМЗЙЭЛЙЗКЛАЯЖЙБГЖЭЙБНЙЗОИУАЗОТУЕОТЩЗОБГЕМ
ЖАВМКЙЖНАДИЛОБИЙМНЧАЮЙКЙЕВЖМЧЗИАВЗАТНАЖЧИЙИЬЦЖЖАНМЙЛЙЕЛЙМНОМЛАЯИ
АЮЙРОЯЙФЭГУГЛЙЕЙКЖАТЭТАЛИЙДЬЙЛЙЯААЮЙКЙЕВЦЭЖМЧКЛЙМАЯЧБГЭЦАЬЙЖЧУГА
ЮЖВНЕГЬАЮЖГЖГСЙАЮЙГЗАЖЙЭЦ

(b) Расшифровать текст:

ГАЧХРДАХЩЕАЩЧЫЗБЧЧЦДГЧЗЩЖЯАСЪРЭАЛРПЪЪУЭДЧЙРЬДЧЭБУЩГАЗТЖАЗУЧДГЧЖР
ЙБЮЧУДАДШСЗБДАРУЕДПУЧАДКЦРУАХЩФЪДБЬПАЯКЧРХХЙРМДАМПЗГОЦХЙЭГШЬКЭЪК
ЧОВОННПАФТЪРЦАЭЦМЮАКФМВАЗЭКЪЯПЦРЯЪРЬЮЬАСШЗЙДУХМФНЦРГЙЕЗЬФФЕКЭЗГЬ
МЦРЯГРНГАХШЩФФЧЬЦУЭУАЧЕАЭУЬРЮПЧЩДНЮХЗКФЯУНПГЬЛУФЧЮТРПЧФЦУНЗУАЦСВ
АЙЩНШДБУЙЮАРВНГФКЦЮЪЙЪШХЭВЙЩУДОНТРУВМУНГОТРЕАЭНБЗАБУЧПЪЭЦЩСАЮТУН
ГБУНФАВРЩПГЭЗЭЗУЧЗЦЖНЬУШХУДГГМБЧЧЫПЦВКУЩЯБШОНДНСРПЭЧИХРЭЪФЭЭЧГШЭ
МЪЮХЗКФЯУНПБЧХРТФЭКОРВЧЬЗПЧХУНРВЪЦШКЮЮТЩЕАГЗРНОЪЬЬМЩЭУШРЯЧЮРУЭУУ
ШДНКРУФЪЗУШЮЬАФЫКДФУЫКЭЦЗРТОЮАЬНЪЮУУДАЭТЩДЭЪЦЗКДЬЖЖНФЦУЧЗЬАСРПЦЯ
ЧЧТОЪЗШРФЯЗАРЦЪРХРЮЯКАРДЧРЬЖЧЭЧЗУФЧРЗКЙЕТРМАДУЫЭЧФУЪТАГАШРГДХУМЩ
ЮУЭНХАРЩДАРНТФЬЯШЦУЧУКЮЪЪГЙЩУЦАГТМВНРОНЩЪЗЬМАВКТГНЭЦЬПАЮФЫРГЯШНЪ
ЪГБЪРЦАМННГФКЦЮЪЙННОЧГЧЩЗХАШНКЦЧРЪЗВЧЙЬРУАГЧТОРННПАФТЮПХЧРЗУЬЪОО
РЭАЦРЗЮЧТЪТЪФКЭУДФУННЯЧСЩЕЕФАЫЙЪДБЬНЦАЦЭПАХУВХФГЧНРФЭЙРДКЧИЩОЯАГ
НЯДЕСУПЕДШЬЧФДНЦЗЧВШХХЪБХУНОЯШЦМЯЧОЩГЭЪЗЬНЧЩСУХЮЪРРПЪЮЭШЗАДХЖДЭЧ
КУДЦВШОЗЧХШММЪЬУЬПЕЭНЬЮЮАКФЫЧЬНУСАЙШНУДФУННЪЗЛЫМАЫНЬДЧШНФСАИКЦХЫ
АИЩПОБХЩГЧШРЪРЮЯКЧКЭЦУМТЮВБУДЯАЗШУЬЩРРЛУЕЙЗОАЧГСЗЯАГЬРХЭЦУУОЯСЩЗ
ГЙЦЭКЧАТЩСАЮТУНГОХПКУАИЮУБАПЩЛДЧЦЗУЬЩРЩПАДТНХЮЧТЬДАРХЮМЕФАРЫЧФУЪ
УЯАЦЭКВЯСЩИЧДУЭМВНЧЗУБАЖРТЧХНЭЗГЧЖАРДОЙЦОЧЯЦИФЪЮЦЦРФАСЩПЕКРЩУДФС
РПФЕФЩЗЯЪННРГДУЫЕГЙЦЭКЧФУЬМВЧЦУНАЮКШРЯУШПЗДЮУЩПЮЧТЦАУЪЧИФЮНЦЦЮЯБ
УЦПЭФЦРОАЧЦЮЫЧГЧНРФЯНРУДАОЪРВНСШЗЙГУЭЩГЕЦЭПАФНЦРГОРЮЩКЧСРПЭЧЬУНБ
АРХРФАОБЭВРРЗПЪЬНМРФЬХРСАГЧУЖВЕИЩЕАЭКХТЯЧЖЖНАЪЦЦДУАИЮПЧЕСШКЙЭСЩН
АЦУЬФОЪФЫКВАЙЮУЬАХУНЪЮУРДНЩЙЩТАФРРПЪЧЗЬЗГЧСРЛГДЗЩМАЮКШЖЯДМЧПАРША
ИЪФРЩОВОННПАФТ

2. Разложить на множители числа:

(a) 427920087894349347067656182813

(b) 77727346857242434572277771115836879305376083761858716732698 1

(c) 10263633561267671762998036362325265166985656287709778298006951529239294462511339356128469 89

(d) 20172598985586006402195825345471884514140895762890113285434991489334624903499380013578160152682183272260169874358466430 29

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 673117195711560670708462813769423249528815786683971258399419790269969592612 27$
- $e = 5$

Сообщение:

- $M = 291059459244049880354740372336064170558915277674392525755339821134621253500 73$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 17073784049055299200829044324664291 4967$
- $q = 23065449727549050870350403990287683 3111$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 13489073117721128419860304955554873618515165224250428848010385685506299353366$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 15075527649909473876709010040793023 8583$
- $e = 5$

Зашифрованное сообщение:

- $c = 47173271769944517002501156253919056276$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 190907450538085046111330097722032388269$
   - $g = 68663792539373800579598098579864210034$
   - $y = 10726361465186010332102362179981565376 7$

   Секретный ключ:
   - $x = 599560961006486783132117151293378080 87$

   Сообщение:
   - $M = 175158234400124926009160464948806811089$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 220754144101073654653095543032170749 17$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 211950153696538198464467095537121095517$
   - $g = 756195769057026230761445342847519817 00$
   - $y = 597884123252022029244190302699420757 25$

   Сообщение:
   - $M = 515122359243537115611549937838022512 10$

   Подпись:
   - $a = 177473647529605307522750218832356274 72$
   - $b = 112962841922213119390527657956216602222$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 599$
   - $g = 409$
   - $y = 449$

   Сообщение:
   - $M = 180$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 461$

   В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 2x - 6$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 106

1. (a) Расшифровать текст:

ЗЮИЮЙЮЬЗЙЗЭГЗВКЫЮДХБРКЛДЫЖЮВЙКИЗЙЯЛХККЛДЬДЭЮЛХЫМАЮЖХГЗЮЗГЗСГЗИЮЙ
ЮЭЗЕЖЗЧИЙЗКЛБЙДКХИЮРДХЖКЛЮИХЖБКГЗКХКЛЗДЗЖЮКГЗДХГЗБАЪМСЮГИЗМДБПЮЪ
ЙЗЭБДЗЖЮКГЗДХГЗГМЙБПКЛЙМОКЛЗЖГЙФДХПЮКГЗЙФЛЗЕГДБГДКЫБЖЮВГЗЛЗЙФЮЗЛ
ЫЮРДБЮВЭЙМЯЮДЧЪЖФЕОЙЧГЖХЮЕБЫЗЛЫГГЗВКЛЗЙЗЖЮЗКМЯЭЮЖЪФДИЙЗЫЗЭБЛХЕЗЧ
ЕЗДЗЭЗКЛХЛЗКГЫАДЕЮЖЗЛЗСЮДЗЛЗГЗСГБДЮЬКИЛХЪЮАМЯБЖЖЮКЕЗЛЙЖМЫЮТЖБКЫЮ
ДХБРГЗЛЗЙФВИЗЫЛЗЙДККЗГЙМСЮЖБЮЕЬЗКИЗЭБЫДЭФГЗЖБРЮЬЗГМСЛХЖЮБАЫЗДБЛР
ЛЗКГЯЮЛЪЙФЖГЗДБЭБЛАЖЮЕЗЯЮЛЖЭЙМЬЗВЭЮЖХИЗМЛЙМЛЗДХГЗРЛЗКЛДЗЭЮЫЛХКГГ
ЭЫЮЙХЗЛЫЗЙБДКХБГЗЕЖЮЫЗСЮДЕЗДЗЭЗВЗНБПЮЙЖЮЫФКЗГЗЬЗЙЗКЛКДБПЗЕКЕМЬДФ
ЕБЗЛЕЮЖЖЗЖЮГЙКБЫФЕЖЗРЙЮАЫФРВЖЗЯБЫФЕБАЫБЖБЛЮЕЮЖКГАДЗЖЕЖЮИЗНЙЖПМАК
ГБРЛЗЪЮАПЮЙЮЕЗЖББИЙБОЗЯМКЫЕБИЗАЖГЗЕБЛХКЫРЮЙМАЖДЗЫСЮЕИЙБЮАЭЮЯЮДЖБ
ЮМЫБЭЮЛХЖГЗЖЮПРЮДЗЫЮРЮКГЗЮДБПЗЛГЗЫДЭЮДЗЕЖЗЧРЛЗЖЮЫФЛЮЙИЮДЫФЦЛЗИЗВ
ЕЮЛЮГЗЬЭЙЗЯБЫЮЛЮАЭЮКХЮТЮЖЮКГЗДХГЗЫЙЮЕЮЖБЭЗЬЭДКРЛЗЦЛЗЪФДЗНБПЮЙЫФ

ИБКЖЖФВВАЬЫЙЭББАИЗЮЭБЖЗГЕФЛЗЛРКИЗАЖГЗЕБДБКХСЫЪЙБЖЪФДЗРЮЖХЖЮЬДМИЙ
АЬЗЫЗЙЮЬЗЪФДЗКЛЮЙБАЖБЕЛЮДЮЖЗЖКЪЗДХСЗВЫЮКЮДЗКЛБЧЗИБКДЕЖЮКЮЕЮВКЛЫЗ
ГЗЕЮЖЭЖЛЮЬЗЗЪТЮКЛЫЗБГЙВГМЭАЫЮДЕЮЖКМЭХЪКЕЮДКЗЛРБКЛЗЬЗКЮЙЭПГГЫЗСЮД
ГЗЕЖЮЛЗЛКЕФВБЖЫДБЭГЗЛЗЙФВРБЖБДЕМЖЭБЙЫИЮЙЮЭЖЮВГЗЕЮЖЭЖЛБЗЛБЕЮЖБЫКБ
ДБКФЮЬЗЙЗЫЖФИЗАЫДЕЮЖГЖБЕЗЪЮЭЛХСЫЪЙБЖЫФАЫДКБЭЛБКЗЕЖЗЧЫЕЮКЛЮИЗЭОЗЭ
ГГЗЕЮЖЭЖЛКГЗЕМЭЗЕМЕФМЫБЭЮДБЖИДЗТЭГЮРЮДЗЫЮГЭЫЭПЛХКЛЙЮЖХГБОБЖЫДБЭЗ
ЫКЭДБЖЖФЕБГЗКЕББЫЛЙЮМЬЗДХЖФОСДИОЗЖБЫФКЛЙЗЮЖФЪФДБЫЗНЙМЖЛЫИЮЙЮЭБКЛ
ЗДГЗЕЮЖЭЖЛКЛЙБГЪЗЭЙФВБЫФКЗГЗЬЗЙЗКЛМЫГЗДИГЮБЫГБЛВРЛЗЕОДЛЮМЫБЭЖКЗЖ
ГЖЕИЗЭЗСЮДКГАДЕЖЮЖЮКГЗДХГЗДКГЗЫФОКДЗЫБКЛДЗИЛХГЗЕЖЭЫЛХЕФЗКЛЖЗЫБД
БКХЪФДЗКЕЗЛЙЮЛХЖМРЮЖБЮЖЗЗЖИЙЗКБДЖКБЭЛБГЫКБДБКЮЮЬЗЙЗЫЖЮЗЪЮТКХЪФЛХ
ЫКДЮЭАЖЕБАЭЮКХИЙБЪЫБДЗЖЖЮРЮЬЗЫЕКЕЗЛЙЮЛХЫКБДБКЮЬЗЙЗЫЖИЙБЖ

(b) Расшифровать текст:
ИЛИЧЗОАСВДГЖТЯДЩЛВОДНЖЪЩТАМУАПЖВЭЪЖШИЮЮЙИГЭЧЭСЙЮЯДШПШЭДЗЩХХКЖМТЯ
ЧГЖЬВШЮЖТЯКШЛЛЬКВГЭЦЙИПЮЮЙДЬЯАГЪМААЮБПБФДЪМЬАГЧМЗЧЙГЩЬАЙЭНХВАШГА
ЪЮЗГЕЕНЪЖЫЬМДКХЕМЪЛШЬЖДРЮВЧЯПВАЗЙВТЧМЫЗТНЙЙЙШЩЖЖКЭУПВБГЪНАЕЫЯИЩМ
ББКЪМДЪТЫОЛФВГЛЮФКЗРМГЗЙЦЩДБНРЮБДОГВХБГГАЭОЙРЮЯЙЪГЫАУАЖШБМДХХЭНБ
ГФЕЪПГХХКЗНЮЦДГСЪАИЫЛФЯОЙЯХЭКЩМАГЖДЗЪВБЕМБДДАНШДЙЙКШВКГМТЕЛДПХЬМ
ЫРГГДВЖЧФБПЬТГУИМГУБЬАИЪЕЮЕЯАААОГЭАДЛБЬКЯИЧЬДЖПЪАЗТЛШЬБВГЫОЙЕСУЙ
БШСЗЪЙГГЯВКЗРШДББЪЭЕЪЪГАЩКЗРМБМЮЛВЪБВЛБЧЭЮКХЯДЕМЪАЕГМУАДВНХВОДОЯ
ЧОЖПЮУМБЕЫААЫЗБЬПФЦЩЬПЕОЮЪГШГЫФКЭКГЛБГЖХФДМИШЗНЫЙХЯДЛЖГШБШЕЫЪМЭМ
АЪЗГГБЬКБЪЪАЖЖГЯАНИГЩБМДЖЧФКЪАХЩАЫБАУБЬЖШГИЫОВЯЧЫССЪЕЗРТДКЩМАЦДЗ
НЮЭПНГЭЪББВПХХКЮКХЧОЫАЛХКЗНЮЦДГИЯЪОГЛХЮБЪЙХЯЙДНАЪЙИЪЭЦЗЫДЙЪББВГАНЖ
ДРАШБГЖОБКВЛГДКЩМЧЭКЪГШГИДЕТЯТЧСФЧИДДЭАДАПЮФБЖЦХЯЙДКГЕЙЮХВАВЫЛШР
КГМУАБЗЙШАЙДЯАДДИПЭЬМЫНЮГОТАТЧМЫЛЭЕЪШЦХЮПЕМЯЧУЫЛШРЛЖЖЭДШГВЫЧВПЖХ
ЮБЖЩБЬГБИЮЮБГВЭДНГЖЬАУАЖШГЖБВЛФЭЙКУЕНБЩИООСЙХХЖДПЪЩОТЕЫААЫЗВАЮЮВ
ЭАНЮЙХЯПГПТГБЩМБДКИОШЦТИЪЗЧЗДАХЬЙЫПЗЪОАЕЪАЮГИЮДКЖЩЕБЗДУЭЦБЬВЭЧЮЙ
ИЮВЭЙВШДБЧГБЬГГМЬЬНЮКЛЙПЖВЭЪЖЙПЬЧСГСЫГКЪЛЪААЫЙВОЙЫХХХКЩМББКЪМДЪТ
ЫОЛУПЪЪВЧДЗНАФЙССЗВБЪЖВЧЖЖСЫНАГМЗЯЧЫВЮЩКЖЩТГЗЙХХЯЛЪГЭЪГЕЖАЫОЫАЮВ
КИВТНЮДВШДБЗМЫЦОИЩЬЬНЮКЛЙНВМВВДАОХБЖДЕБФКЮКШЬГАКШБПОИГАНВМВВБИЪФ
ЗКЖМИЧЙТИЮФЧНЖБДДИЪЯЕХЫАБЧЯДПЮЦБЖДШДБШПХПОДАВЫЙЫХВАЭШИАЧЛДПВЪЙЮИ
ВАЙЫКЮХКИМЬЕГГРМБМЫДФЧЮЖГЬЧЙГМАЩАШПШЪЛДАХЭБГЖШФЙАСЧЮДНЛБВНЕСБДДБ
АЛКББАЬЧНИГБАФШЯАЪЙСКАГНЙДФАОДКЗДКВЩБЭЧОЙШЬЖИЩФЕИЫЦМЙБВЫВАЖДЛЗЪО
ЗПЯВКЗЖЫЧЯДЯЮХГГГВАОШГЗЭКГНЮГИДРАЪИШДЭАЯДНЮЬИЫПВОБПГЭЪУЫБЮЯБШЖЦЕ
БЗЙШШБИСВАЙЭВГЮЗЗЖТВНЗГЭЪДЗРЫЯНШЖБДЧШРМЖМГФГЩНАСОВДФЛХГИДРАЯЮЗГЭ
КД

2. Разложить на множители числа:

(a) 109091779963223547059441045095 7

(b) 790970334504650809078086366423117112790485637085330332035267

(c) 191420453456776646808099031768102217305973565352491765627417160425937990317567565285827 3043

(d) 888435398042739309771157311123561371164181752204797801168911713901872540470163335334177076932307858172928027271651066113

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 726907849289803135724476156684753175900577062511453106600809474531803500202 77$
   - $e = 3$

   Сообщение:
   - $M = 594022845079473847991355439075809339890437718113794758952015470185928308698 56$

   В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 240217529197916756706159351973548070789$
   - $q = 278872791206841948328710892932731791589$

   Открытая экспонента:
   - $e = 5$

Зашифрованное сообщение:

- $c = 476187172322568145314768337276023119739502624538190332270981677269265356248 98$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 184441867361683637914822356760760507069$
- $e = 5$

Зашифрованное сообщение:

- $c = 123222008977248036876134435305360451267$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 232610365996756276615724868641503454419$
- $g = 230006901052005391036136618463538782017$
- $y = 133167352004077141610726898746471026260$

Секретный ключ:

- $x = 180895116475924147508523450273758809119$

Сообщение:

- $M = 722894084329800365710509994615635746 16$

Использовать следующий случайный параметр для создания подписи:

- $k = 199580914018397798167558569930497090401$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 281426145453504417535810654365922416551$
- $g = 174612684927441934185129721135842019086$
- $y = 169233303481034102003610793007256425257$

Сообщение:

- $M = 186422682625593499610172910473792687619$

Подпись:

- $a = 878090635972850083486877981313169143 31$
- $b = 441504047548966793392836506237463838 54$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 617$
- $g = 377$
- $y = 313$

Сообщение:

- $M = 594$

Использовать следующий случайный параметр для создания подписи:

- $k = 117$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 8x - 17$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 107

1. (a) Расшифровать текст:

ЧЪМЗСНЧЦЕЭВДГЩГЖДЪАЯВЪБИВДГБГОСЭЧВЭШВЗСЭМЖЯЬАГВГЩГЦЕЪЗВНИБЭЕГЧИУ
ЖЯЪБТЗГБГЮЦЗУНЯЗРЖЖГЕЭАЖБРЦРАГДГЖДГЕЭАЭЩГЧГАСВГЯЕИДВГЖДЪЗЕГБВЩЕЪ
ЭМЪБЬМЗГЗЯЬЖИОИУЦЪЬЩЪАЭЛИЬДЪЖЪВЯИЧЖЭАЭЖЪШГЕГЧВВНАЭЬМЗГЖЖГЕЭЗСЖЬД
ЪЖЪВЯИЩЯЯЫЪТЗГЖАИМЭАГЖСЩЧГЗЯЯДЪЗЕВЩЕЪЭМЖГМЭВЭАВЪЩЧВГДЪЖВУЭЖЪШГЩВ
ЬДЪАЪЪДЕЭБВЪЬЗВИАБГУАУЦЭБИУЯДЭЗВЖЯЩГМСВЪКГЩЭШИАЗСЧДГАВГМСЧРНАЕЬА
ЩЭЛДЪЗЕВЩЕЪЭМЦРАГЭЕЖЖЪЕЩЭАЖВГДГЗГБЕЖЖИЩЭАМЗГЧЖЯЧГАЪВДЪЗСМЗГЯГБИИ
ШГЩВГЗЪБЭЩЪАГЯГВМЭАГЖСЦЪЖЖЗРЩЖЗЧГНЧЦЕЭВМИЗСБЪВВЪЧЬЦЪЖЭАГВГВЭЯЗГЯ
ЕГБЪБЪВВЪДГВАШЕИЦРКЪШГГЦЭВЯГЧДГЯЕЮВЪЮБЪЕЪВЭЯЗГВЪГЦЕЗЭАВВЭКЧВЭБВЭ
ГЗДЪЖЪВГЯЕЬШГЧГЕГЦЕЗЭАЖЯЖЗЭКГЗЧГЕЛБЭЯГБЪВЩВЗЬБЪЗЭАМЗГЧЖЪГВЭАУЩЭЦ
ЪЖДИЗВРЪЭШГЕСЯЭЪДСВЭЛРЭЩЕИЫЪЖЯЭЖГЧЪЗГЧАБВЪГЖЗЧЭЗСЖЗЭКГЗЧГЕЖЗЧГЯЯ
ЩЪАГЖАИЫЦЪДЕГЗЭЧВГЪЭВЭЯМЪБИЩГЦЕГБИВЪЩГЧГЩОЪЪДЕЭЖИЗЖЗЧЭЪНЧЦЕЭВЦРА
ГБВЪВЪЖВГЖВГЖЯГЕГДЕГЖЗЭАЖЖЯГБЪВЩВЗГБЭЖЪШГЖЪБЪЮЖЗЧГБДЕЭНЪЩЩГБГЮГЖ
БГЗЕЪАЖЧГУНДШИДГДЕГЦГЧАЪЪЯГВЪЛЭАЪШЖДЗСДЕЭЯЬЧЖЧЪАСЭМИЕЬЦИЩЭЗСБЪВЧ
ЖЪЩСБГБМЖИВЩЕИШГЮЩЪВСЧВЬВМЪВВГЪЧЕЪБЖЗГАИЫЪЬЖЯЭЕЩБЭГЫЭЩБГЪШГДЕГЗЭ
ЧВЭЯЧЖЯГЕЪЗГВЧЭАЖВЖБГШИЗЬЖЗЗСЖЯЬАГВБВЪВЩГЦВГДГЖДЪНЭЗСБРЖВАЭБИВЩЭ
ЕРГЖЗАЭЖСЧГЩВЭКЯБЬГАКЭГЦВЫЭАЭНДШЭЧТЗИБЭВИЗИЭЬЬЖЯЭЕЩЧЩЕИШДГЧЭАЖЭЧ
ВЭШВЗСЭМЭМЪАГЧЬЯДЗСЭВЧАЭЩГЧГВДГЗЕЪЦГЧАВЖЯЯГБЪВЩВЗИБРДГЧЭВГЧАЭЖСЖ
ЩГЖЩГУЖГАЩЗРВЖГЯЕИЫЭАЭЭБРГЗДЕЧЭАЭЖСЧЯЕЪДГЖЗСЧЖАЪЩЬЭЧВГБЭШВЗСЭМЪБ
ЯГЗГЕРЮЧЪАВЖЧЗГЕЫЪЖЗЧЪНШЖИЩЭЧЭЗЪАСВГЮЧЫВГЖЗЭУБРЧГНАЭЧЯГБЪВЩВЗЖЯГ
ЮЩГБЭЧВЭШВЗСЭМГЗЧГЕЭАЩЧЬЕЭДЕГЧГЬШАЖЭЧЗГЕЫЪЖЗЧЪВВГДЕЭЧЬАВЖЧЖЗЕЪЗЭ
АЧЖЭАЭЖЪШГЕГЧВКБГЭЦЗУНЯЭВМЗГТЗГДГКГЫЪЯЯМЗГЧВНЪЮЯЕЪДГЖЗЭЬЧГЩЭЗСЖБ
ЪЕЗГИЦЭЮЖЗЧГЭЧ

(b) Расшифровать текст:

ЗЩРСТЗЛЦВЖЕСРЬГНВФХДЭСЦБДЪЬНЯЗГАРЭЬДЭНФКВФЯХЪГЫХХЖГУЩВЗГАЪМВЪБШБ
ИЗСЪМИЖБЦСЕУУРББЗЛЦФЯВЭТЮАБЭЛШВРЬЯГЭГШЩВЕЕЭХЪЬЧЫНБЙЪХРВУЧЫНБЙЪЧЫ
ЬЯЕБДШЙГУНЫЕЖЩПЫБГЫНЭЫВБХГГЪУУШЙСЬНЗЬШЭЩВКДШЛЮЙГСРВУБЗЫТЫГЯЦУКЬС
ЪАОЪЫЩТЬЗФНШЕЗЮШТЯБУМФЯБФСШБГЬКЮАКЭЪМВУУНЩВЭЗХШМИЬЩШДЪБМУЫЪХНЬПИ
ЩЫЫЯВКЧЬЛЭЪЦТДРЭЪТЬМЪТЮГЪЬМЭЙНФСБЫЪЪУЮИСУЫАДГЩТГИАКАЫЕЧЦЪШЯВЧОЭЬ
ГЦНАДГШЙЮХЖЛЯВЕЦКХХЮВФФЮЪАТЦБЖГУРТВЩКТЮЫГЖНУЕБКМЮЭЭЪРТИЭЪРБЬШЭШЮ
ЩВВАЫМАЭЧЮЙЗЛЦСЕЗЙНЧЫЪУЦЗЬЕЧШЧЪГСЦАКЯЭФХДЩЬЪЯЗГУЦЫЭААХЮКЫФКЭЬШЭХ
ХГЪЗУБЯВЧЯХЪГЬНБВИЗУЬЗСЧКЭЕЧЬКШВЖЛТГЭЭЬЫСВЪУХШЮДЪТЭДБКЦВКЫЧХЫЯБЭ
УЗЯЧАЪЫЯЭЦЦБЙГЪЩЬЕЕФНЮШРЩХЮЩЪЬХЮЪГЮШЮИЗАДБЕЧАНЬИЪЫНЩИЗСЦЬГРЭЪЯЗЧ
ЧУШИСЮЦФЕБЫХЮДЕЭЯЭЕЬРГЫИЧЭЖИЖШВРТЕЕЭЪШВЖЦХХХДЯНФОИСЩВЩГСУЗЙГЦЩВД
ИЫШМХЭСХЮЩВВЦФДИСЩЬЕБУНЫЬГЬКБЙЕФЪШВБФХТЫЧФШЕЯЧЯЫЗЯАЫХХПДТЫЯЗГИСВ
ЬДФЪАДЩЯНШОЖЩПЫЕВЫХХИГАУХЮБЧФХДДЭЩЛВУБКЮЗЪЬЙГЗШРЫФУЗФОШЩРЧЩЗИЗЪР
ТТБЭОХЙЦКЪМЪГАЧЮЫСЮШШЩЪУНВДБУШГЪЖУШГЪГЫЫТЯЩФЪМИЪАУШЭЪЬНВЙИБЦЭЮЕК
МЫЕЦЬУХЬДЯЦЙАВТНЫГГШЩЪЮАЮШЮРЮЫЦЬЯАЫЦЦЬАЬХЗЙГРГБЕБЬЦОДЭРГЫЕЧФШМОЗ
ЭЧЮИАФМЭГГЫГБВСЧЧЮИАФМЭГГЪРВЩЦВМХЙГБНСЬБЗШЛЫАЮШШВСЬЫТББЭНЩЪЕВМШИ
ЫЯЦЬЬЪЮЦЖВГСУШЖГАЧХПВЭКЛПЪЪРЧБГЫХВТШЪКЯЗЭАЪГЖШЭУЮЩБЭЛЮВГСЫИБШЭУЮ
ЩДЭЩЫКЫЧКЯЕЖЪЫЦЯАЫЦУЕАЭКГПЯЯЦТДГБШШЫЛБДЫЬЗЧЪАЯШЭМЕДЪСГБВИХРЫЪГЪЦ
ТКНЩХШБГЯГБЙЭАНСЬВЧШФЕЖБРЪБВЧЩЫЕЧАНСЬЩЭЙАЕШЭРЭЯЕЬЛГИЪРНТТЖЭТЮЪГ

2. Разложить на множители числа:

(a) 6186290224731869167733195206 49

(b) 607570879936582860458339876017726346906569924474733726115647

(c) 173739769684413938915021574401989382207409088394072082687979655197941300874626698864636 1929

(d) 211406533754960681533056970553218927676720998394598952852495166757672170968837232598575771693312817922948023853522482622 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

- $n = 323364183140776717461528784880875928125636409218774304673526559660752252233 53$
- $e = 5$

Сообщение:

- $M = 143704412870360684083558912876316503681200731738334401801145689982646104852 29$

В ответе привести все промежуточные результаты вычислений.

(b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

- $p = 26802184099726814700091105761021754816 1$
- $q = 31147144910384064480185980675410253944 7$

Открытая экспонента:

- $e = 17$

Зашифрованное сообщение:

- $c = 16875009137961990949660012658170555940863070458403339564716383714546276125029$

В ответе привести все промежуточные результаты вычислений.

(c) Расшифровать сообщение по схеме RSA. Открытый ключ:

- $n = 19040754122012150084711675497196461527 1$
- $e = 3$

Зашифрованное сообщение:

- $c = 12183787698514336888980072354421191243 4$

В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 19202953914537984466334285435712994310 3$
- $g = 55368586658084166156391217256508824012$
- $y = 27463637648205695790227937905259408893$

Секретный ключ:

- $x = 85668811242225664599402838195899452476$

Сообщение:

- $M = 12745604657439804421162391243581588859 6$

Использовать следующий случайный параметр для создания подписи:

- $k = 53744951914096867735120158664770898121$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 26815007444903422711899280468994969227 9$
- $g = 18798196739410923516690393016414181943$
- $y = 21527761700230972645551898169443853540 2$

Сообщение:

- $M = 30950241261863977408627222564448842500$

Подпись:

- $a = 76476136240874651001733177136818641855$
- $b = 13715190861945369020964098684461633458 3$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 743$
- $g = 340$
- $y = 145$

Сообщение:

- $M = 65$

Использовать следующий случайный параметр для создания подписи:

- $k = 127$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 8$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 108

1. (a) Расшифровать текст:

ФГЧХАУАЭЧЧАХАВЙЪЭАЮЧЯЪЩФЧГДЪЧАУАЭЧЩЯЪЮДЧВЪЯЧХАЦАФЭЯГФЧЭОЪЙЯЧГАЮЯ
ЧФГОЙДАБАЧЦЪЯАЬЮАЫГДЭЪЩФЧГДЧЯВАЦЪДЧЭЮЙЧВЧЩЯЧХАКХФЩЦЪФБЧВЧЦБАДЧГЯ
АЫЮАЧЫЬАЮЯДЧАГДЯАФЪЭГБЧВЧЦЯЪЮЪГЬЩЭФЩХЭЯЕФЯЯЧХАХВАЩЯАФЪЦЯАДЧУЧЯЧЦ
АФАЭОЯАЙДАУЭХАЦВДЧУВЯЧЯЪИЧЭНЫЮЧГИУНЭЯЬВРХВАУДНЪЮДОЮАРЗАЙЧКОЕЮАВЪ
ДОГФЧЭОЪЙУНЭБАВШЧЯЬЬХВАЮАЮБАЮЪЭЕЫГЕЦВОГЬЩЭАЯЙЕДОЯЧЩВНЦФЙДАПДАЪЩФ
АЭЪКОХАФАВЪДОБВЪЙЪЯЙДАДНУНЭВЯЧЯУАХФЪЦЪДУЧШЭЩГЭАЯЪДОДЧУГФАЧРХВЕЦО
РАДКБХЪЭЧЬГЧЪФЯНЙГДВАГДОБВАЬЭДБАЮЧКЭЦЙДАШГЦЧЭЭЮДЕКЬЧДАДФАЧЫЙДАДН
ГЦЧЭЭАДФЧЙЭЬДАБВАГЪЭДЧУБЪГДОЯЮЧЯЦАЯАГНВЩФЧДНБВЪГДФЭЧЯЬАЮЯЧФКБЪАЯ
НБЪГЭЯДЧУЦАЯАГНАДФЧЙЭГФЧЭОЪЙГАГЭЧЩЮЪХАГБАЦЪИВРЯЧУЧГЯНЫДЬЪЩФАЭОЬБ
ВАЙЪДДОЙДАБЪКЧДЬАЮЯЧУВЪЯЕФЪЦЪКОЬЬЦАЯАГЪЭЯДЧУДЕДАЯФНЯЕЭЪЩЬВЮЯБЪГО
ЮАЪБВАЙЧЭГЭЧЦЕРЛЧЧГДНЦЯАДЧУЧГДВНЫБЧГЙДАДНЯЧФЩЪВЯЮАЪГДВАХЪЧБВЪЬЩЯ
ЪЮЯЧЯЧЦАЯЧГАГНЯЧЮАЧЮБЧДВЧЯЦВЧЧФЪЙЧЪЙДАБАГДАВАЯЯЪЧБВЪЯЕШЦЧЯНЕФЧЦА
ЮЭДОЮЧЯАЧХАБВАЬЩЗДЬЭЪЪГБАЭЯЧКОДНГФАРЦАЭШЯАГДОЪХАГБАЦГЬЕРФАЭРДЧУГ
ДВАХАБГБАКЭРГФЪЯЧЫБГДЪЩЕДЫЬЕБВФЦНЪБАДФАВГДФАЬЮАЭАЦАЮЕЙЧЭАФЧЬЕГБА
ЭЕЙЧЯЪЧЮГЧХАБВЪЬЩНФРДЧУЧЯЧЮЧЦЭЧЯЯААДБЪГДОЬАЮЯЧЬЬАФАДЧБЧВОЧХАЩЦАВ
АФОЧАЬАДАВАЮБЪКЕДЮЯЧЙДАБАБВФЪЭАГОЦФЬЬАЧЪЮЧЯЯАЮЧГДААЯВЯЧЯЪЗАВАКАЭ
ЪЧХАЩЭЧЙЪЭЪАЙЧФЪЦЯАУНЭАЙДАГФЧЭОЪЙБЧВЧЦАЮЯАРУНЭБВФЪЙДАЯБВГЯААГЬАВ
УЪЭЧХАЕБВЧЬАЮЪБАЦАЩВЧЯЪЧЮБВАГЪЭЕЯЧХАБВАЛЧЯЪЯАГДВЬЬУНЭЯЧЕДЧКЧЯФАД
ЦАЙЧХАЦАШЪЭБАФДАВЭАЯФАДЬЬЪЗЮЪЭАГДЧЫЦАГЭЕШЪЭГАДГФАЪЗХАГБАЦЪГДВНЫБ
ЧГЪГФЪЯАБГЦШЪБВЪЙЪЯДФАЧЫВЯНЯЧДУДРКЬБЧДВЯЦВЧЪЙЯЧБВАЬЭДНЫЮЕГОЧФГЧЮ
ЕФЪЯАФДАЯЯЕЙЪЭДЧУДНЬДОГШЧЭЧЩЯНЮЪФЧВДЧЭЮЪЦБВЪДАБНФДОЬЬУЕЦДАДНЬЯЪЧ
ЮЦДАБЯЪЧЮЕУЧВЧШЧКОГАДЩЭАХАЙЧЭАФЧЬЯЕШЯАУНЭАЯЯЪЮДОЮЕГОЧЦДВД

   (b) Расшифровать текст:

УККОЧБОЖЪЫШБШЯРЛЧХЬТУФСЭХФЗЛВЩСУЬРЖФФЦЭЬЛРЕЭПЧЧСЧЧФЙРЪЦТКФЮПОТИШ
ШЙФУФМЛЦХФМХУУРШРСЮЭХОЦПЯГЛТРЗПЧЧСЧЖЩЛФЩЕТНЕЫПЭЧОСЧОСЛЩПОМЕСЫШТС
ЭЬВУФЯОВЖИШЪВНЛОЧФЗРЗЩЩЮИОЫЛИСШПУСЦГТСИЗСШУЬХЪЫУКБЯЫХКОЧТЧФУЮЬВЦ
РРПМТСЧТЛКЦНПМНЬСЩФРРЗУШХИОШМТЮШТТАФЧЦОЗСДПСЗНЪЦЛТЗЩЬЧПСХОФСЕЭПЗ
АОЪЩЩЦХЪЫШШОИЫШУОЗЫЩТЗЯФОЖЮЧТХКУСХФСРЗЩФЦЦРЩЛХИНТШЗФСЪЧЧФЦЧФЗКНП
МРТЪЦСКРИФФООСЫШТЛВПРУХЪЬИКООЫИКХЧТЬШЛОЩЛХЕЗУЦМСЮЪФЙЦОШЮКООФФСРЮ
ЭТХЯФТИТСОЧБШЕФОЛРИСЩФЦХСХДФИЬПЦАХЯИЦМДЪУУННШТЮПТНЕСХКЧШТТЛЬНЦЖО
СЧССТРФШКТЧТСЦЯСГЛФИЬПКУТЯЫШКОЗЦРНЕЪЬФСЦВПСКОЪТНКУЦХВЫСОТЧКЕДПЛЗ
ТЬШЧЧИЩФЛИЗСРЗАОБШНОНЙЬФОФШТЦКРЩШПЙИОТЭКФЦШППИЧЖОЦХЬВУСЮЭХВСИЧЖР
ТЦЧМЩСИШШЛСЕЪШЗХКФХЛКЕЬЭРЪЦЬСЗУМЩТРУЕЭПЦЙЩСЦФКФТХФЦЯПШЦБНЪНФХЯЦШ
НФОЦХОИУЪЦРУТЬШОМРСЫОСПЪППРБНПНТСХМГЧЦШТУШХЯЩФЦОЗВСЦОСНРНМДЭТНЛУ
СЮПТОТСЦЯЫХЮЖОСОУНХЬПХКЬЯГЫФИЮЪУЙУСТЭЦНУХФТФЫХЛЦРЯМЦШНШТРПСХОЛТИ
ЦФРНИЭЬЦЦХФЦЦБЛОЧФЗРЭЩЦУФФХУКХСЪХКОФМФЬХЪЦЦБЛОЧФЗРНЪБЭРТТИУХОПЭР
ТЧВФТФЫЪШТЦЦЭСНРЗЩТШЛЧШИТЮЯЩФФЗИТИЦНЬТЭРФЯРЧУПНШМКПЪУКЧПЫЭЙЬИОЛЦ
УФФХЧЗСЩТНПСШЧШАПФНФССГЭШНОЭЧЩРЛВПОУТЬШТКХИИХУДСРСЗЗЪЦЧЗИЕПУТЛЦЧ
ОЬИПШУКЕФООТИГЭИЦХОЭШСУУОИРЛЭЖРХЛЦТЫУШЪЬОФИЭЧОФЦПБЛЗТФЪФЗОЭЫИУЛШ
ТШУЕЬТЯСЛЫХЮФУФЛЛЛОЮЭКЛИУЦУУБЫШКУФЧХЛКЕЗСИЧЯЮТЫУРИФФПЦЧТУШТШЮОРС
ОЧЩЬИЬПНСЛЩЭШШТЪЩКБЕЗВСПСШЧЛЗФСЧОЦТЯЫШАПДЬФЩСШМЦШНБЪКНДЪНЙЙИШЪВН
ЕЩШИТФЫЪФЦЛЧЫУКЛУДЧТЛШЕТЗСЧЧЛТЛСЦСКЙФЬТУЖЪХЩЖЦДФЩСИЩЧРХСОЬОЧПУЩЛ
ХИПШЦУЗЦШДУХОПЭРТЪЩКБРЯЩЛЧУЩОЦКЛГБЩЧЯНЕСУРСЫШХФЧЫВЖИРОЧРЕНШЙШЕЭП
ХХСДХФЖОПШХУОЯБУУКЧШККМЮШСБНЪБШУЦЭПСЦСНПКЧЯЦФ

2. Разложить на множители числа:

   (a) 100619437154843215819039171785 7

   (b) 837840761843144423459262028319924082985703686339139888635957

(c) 68869481059867509601924106474266018610163454202305918526483832437773840171556754934538290 9

(d) 12446591181167927444281771862184583800713591324753649506729896104806160710769000003954243336154113027497614427254852447 61

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 563396915089454552614470331785609687964806243287110208294872773814644467460 89$
   - $e = 257$

   Сообщение:
   - $M = 553112337634457835896958126302551673184079780849650987093119653640283009468 7$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:
   - $p = 221357553360686922254472053004258569261$
   - $q = 269820173829191120292400023609302815409$

   Открытая экспонента:
   - $e = 3$

   Зашифрованное сообщение:
   - $c = 41096867767933208971806341166090675953587380774777712642134849261599155864 22$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:
   - $n = 296853703547567252577110429378758021603$
   - $e = 3$

   Зашифрованное сообщение:
   - $c = 771563754475493841963847875927294700 33$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 286640511962138863956895044700780874197$
   - $g = 805157302947353061220126563817013798 34$
   - $y = 214702810995929205210348183917656574792$

   Секретный ключ:
   - $x = 457282673674834510432132738260130552 79$

   Сообщение:
   - $M = 221539152187969964582631747032248885771$

   Использовать следующий случайный параметр для создания подписи:
   - $k = 280091774836883054295379470293966475 73$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:
   - $p = 213928992029238923018563811277555363007$
   - $g = 182152162218895182982202447931131160893$
   - $y = 27628921482657015896980806420644834931$

   Сообщение:
   - $M = 142146756642503940493431299431289597260$

   Подпись:
   - $a = 118965599561980098200153786014238138939$
   - $b = 122330442813710164870995413785611410086$

   В ответе привести все промежуточные результаты вычислений.

   (c) Подписать (подделать подпись) сообщения. Открытый ключ:
   - $p = 937$

- $g = 735$
- $y = 156$

Сообщение:

- $M = 320$

Использовать следующий случайный параметр для создания подписи:

- $k = 475$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 4x - 10$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 109

1. (a) Расшифровать текст:

БЬЮЬГШЕЯАХФТЮФШВХЫОЪЮВЮАЛЩФЮЯГБВШЫХУЮЪБТЮХЩАГЪХШФЮЫУЮБЭШЬАЧУЮТАШ
ТЫЪЮЬХЭФЭВЭХЬХФЫХЭЭЮЯЮБФШЫГАФЭШЪЯЮФЪАГЫОЫЭЧЭЗШЫЭХУЮЬХБВЮНВЭЮТЮБВ
МЯАШЭВСЛЫЪЧЪЬШБТЭЛЬЭХГФЮТЮЫМБВТШХЬЮЭШУАЮЬЪЮАЮЯВЫШШШТЭШУЭВМШЗШБЯЮ
ЫЭШВХЫМЪЮЬХЭФЭВБЪЮУЮАБЯЮАЦХЭШБЫЛИЫБТЮШЬШГИЬШЪЪЮЭШУЮТЮАШЫШТЮВГЦЮВ
ХСХСГФХВУАЭШЧЮЭЭЪАЛБЪЮЬХЭФЭВФГЬЫТВЮВЦХФХЭМФЮЯАЮБШВМБТЮХУЮАХБВЭВЭ
ЮГАФЭШЪСХЦЫШЧЯЮФЪАГЫТХАЮВЭЮЯАШЯЮЬЮЙШБТЮШЕХФШЭЮЬЛИЫХЭЭШЪЮТЭЮТЮХЮС
ББЮВХЫМБВТЮГБШЫШЫЮСХБЯЮЪЮЩБВТЮЪЮЬХЭФЭВБЕТЗХЭСЛЫСИЪШАХЖБТЮЧЬГВШВХ
ЫМЭЛЬШЫШБВЬШЯЮБХЬГБЫГЗОЪЮЬХЭФЭВФГЬЫЮЯВМБЮСАВМБТЮШЕЮДШЖХАЮТШФЫВЮУ
ЮЕЮВХЫЮЯВМГФЫШВМТБШЫШБГХУЮАЮТЭГЯЮФСЫУЮТШФЭЛЬЯАХФЫЮУЮЬЭЮЪЪШТЭЪГЧЬ
ШЗСЛЫЗХЫЮТХЪБЬЛЩЯАЬЮФГИЭЛЩШЯАТФШТЛЩВЮШЭХЭИХЫФАГУЮУЮБЯЮБЮСЪАЮЬХЪЪ
ХФШЭЮЦФЛГЦХШЬГЯЮВАХСЫХЭЭЮУЮБЫЛИМВЛТБШЫШБХУЮАЮТЭБЪЧЫЮЭХЩЯЮЪИЫШТЮВ
ХЖУХАБШЬЯЮЫГЗШЫУЮТЮАВШЧУЮАЮФЯЮЫЭЮТАВМШТЭЪГЧЬШЗЯХАХАТЫЪЮЬХЭФЭВИВЛ
ЧЭВМЕЮЗХИМБЮСАВМБЮТХЙЭШХФСХЧЬХЭЯЮВЮЫЪЮТВМЮСХЬХЫМЭХЯГУЗХТХФЫШЕЭХЯ
АЮТХФХИМШТЭЪГЧЬШЗТЛВАЙШЫУЫЧЭГЬВГИЪБЪЧЫЮЭЪЮЫШВЛГЦХТБХЧЭХИМВЪЯЮЦЫГ
ЩЮБВТЩБЬЛЯЮВЮЫЪГХЬШЯАШВХСХВЮВЮСВМЪЮЬЮЩЮВТХЗЫЮЭЭХВХСХСЛЕШВАШВМЯЮБ
ЛЫЩЪЧЮДШЖХАЬШЬЛБЮСАЫШБМЮЯВМШТЭЪГЧЬШЗТЯАШБГВБВТШШЦХЭЛЯАЮЗХЫЭЬТЮЧЧ
ТЭШХЯГУЗХТЯШБЭЭЮХЪЬШЬЭШСГФМЯЮЫГУАЬЮВЭЛЬЪЧЪЮЬАЧСЮЩЭШЪЮСКТЫЫОБТЮХЬ
ЭЬХАХЭШШЭХЬХФЫХЭЭЮШФВШЭЭИГЪАХЯЮБВМЯАШУЫИЫЪЧЪЮТШБЮЫФВТБТЮООИЩЪГЪЮЬ
ЭФШАЮТГТХЙХТЫЭХБГЯАЮВШТЫВМБГУАЮЦЪЧЭШОТЯАЮВШТЭЮЬБЫГЗХТЮЧЧТЭШХЭЯШБ
ЭЮСЛЫЮТУАГСЛЕЭЮБШЫМЭЛЕТЛАЦХЭШЕШФЮЫЦЭЮСЛЫЮЯАЮШЧТХБВШЮЯБЭЮХТЯХЗВЫХ
ЭШХЭГЬЛЯАЮБВЛЕЫОФХЩЪЪЮТЬЮИХЭЭШЪТЮБЪЫШЪЭГЫЪЮЬХЭФЭВИЗВЮБЬХХВХЙХЭЬЯ
АХФЫУВМТЛФВШЪЭХЬГЭТБВАХЗГШЯЮЫЮЦШВМЪЭЮУЬХУЮЧЭЬХЭЕЮЭБЮСЗШЩБЛЭФАЧТХ
ЭХЧЭХВЮЭЗВЮЬЛГЦХБЮАЮЪ

   (b) Расшифровать текст:

МЙЫУУЛРРЬОРПЦОПИТХЪПИЧЬЭПЙПОШОШННЮЩВЖЦЩЙСМРУШВХУУДИЖЩТМРОЪЦЕЗТКЖ
МЛХШЩИКЖЫЗТЙСОЪСВОЩЬООЦЧМПЖЗЩЮТПСЧОСРХЫШПНХЪЭГПАЪОСРХЫШПЮЧНЭПЮЯЪ
ПФХТТАЖНХУЩГНСЧЮУНТХЫИЮЧНУМЙЙЦМСЮСШЩЩВПЦЬВЛФЦШЖЙЙЪЭППРЪЭСЛМФУТЩЧ
ПРУЛПШЖРРЗАРГООСРПЗТФЩГЕХОЦЙУЯМПЖЯХОРЪВЖСЬЖИМЛВЖНЬЦУЖГЙЩЭГШОРХЙО
ЦЧЦЙЯЙЩАНЕХЧЦЕПЯШЩЕНЧПЗЖЙЛЦЧЖКФРНЖЯПСЬЭКЙЪХПИАУЩРРЬОХНВКНЮЛЛМЮЮИ
КПСШЩРУЧЬУЯПОШЬЮЯФУОМТЮЩЕКЯОЦХВЦДНТВКСЭЖИМЦАПБМФУТЩЦЬЭЗВТПУЕОРЧТ
ГКЪЬХСШПЕБЛЛРОШЕКЦЪХПАТНЩНЗЛУПЖНКФЪПБЧЪЭЧШУЩРЛНХЦЮЯЮЙФЮЯИТБПЭЗМЩ
ОЙДХУЩКМТЩЩЕШМЪХМАПРЧЙПЙФХПЙЙЦПОПЬСЩОЛЕДЦПЛЦЦРТВСЧШЖЙСЧОПЯХЫЩСЛС
ЬУРНМУЫЬПТЩЩДЛКОЙОЗТЦРЧМЧМВЖЯЖДГЖИМРЬЖКЙТШСЛИЪШМХУУУРРЗАРГЛХЫШПЯ
МФЬОЗФДЦЭУЙСЬПЯХОЧЙМТРППНТЛЦТЛИСШЙДХЫЫЩЕСШЩЕИЙХЮНВЬЧХТЙЙНШЬЙМНРО
ЩЗХУЙЛСЪЭМЕЩХРУПАШЫЙАТЩГОЙМЦЫПБХУЫЙЗТХМСЛХСЦТЕЩШЩЕЮМЩЭЭЕИОЦПЛЕЧГ
МЛХЕШЖЮЙРЮГВЫЕЪФАЫОНПЗФЬСМЕЗФНОШЙСТЖАТЪЩПЮЭЦУЛЛЖХРЗБЧСЧЙОЦЧЦЙХЖК
ЫЙКЖРЩСШСБУГОЦЩРУЕПСЬЭЯРЧРНЛСХЩДМФЧВЖОЦЕЪСВЛЩРОЕЙСЩОЛЦЛЩСЛЦСЦТОЖ
ДЫЗВССРНЕХУЫЖКСОФИИТКЖЙМФСЭГЛФЦЩККХХРЩИМЛЩТПМШЮДФЙЛЮГЕИОННВСЛЭПИ
УОХЙЯСЬЦНКЙМЩМЛЖЧЙЙМТНЩИЯПУЬЖЮЙЪЦФХНЪХИИТЦЧОВХЫЮРЖХОФЗВЫЪНПНЙЦМФ

НЗСЩВЧЖСЩУЙЙЦОФЮЙЩШУЛФЬУГОЙХОЖКЙЩЦНФЦЧМПГМНЦЙЙЙЦХТВЕОВЖНЙРШЖБЙФЙ
РНМЪЩГВЦЬФЙЙЖЪЭСВЦСЭЭЙЙЦЬЕВЦЪХПЖПЗМПЯМЗУРЛХФЮЩКМОЧОВЦЧШЖЕЛКРЗПАС
ЧМЫЦЧФЛДССЬШОЦФУГШНШЮУЩЖБРВИЗЧЫПБМОЪППТХЩВНЦСЦТЛСУШСЛИЬУТЗЛФЮЛДЯ
ЛШЩЯЕЩУОЯТЫННБЙЫЮЩЗМЦЩГШНУЩНКИСЫТИЧБФУВХЕРДЛЖЧНТВРЧШППЖОВЖПРЦРИЯ
ХСТЛНЙШЩТПАЪЮЗОТХЮТИЯБЦТЕМЪЦПЯЬЛМСЕСНРМИХЦВМЩССХПЙОЩРРЛХЫУННАСНО
ЛЖЦЩТПЖФЬЭЯЙМЩГИХЫУВЛКОВУЛХЦРЯ

2. Разложить на множители числа:

   (a) 722857558903119556565575555501

   (b) 11924972644394384829031420946190090839640845669020097477167 69

   (c) 625088155703739016186788959302201974214566691398585166442309329324634547999620457425402263

   (d) 116063204249980901203274552211322322411970652149116281421547148089864716631629501908467027604540093065039814576984094178 1

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 85375113152148513779512855349284128999035423570436444024670467148620733645471$
   - $e = 5$

   Сообщение:

   - $M = 65916323374648750772301333580147676379153662907945756869670281154284111959866$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 26749052545301160275955728280813890741 3$
   - $q = 19303181965638278977698523654758628606 1$

   Открытая экспонента:

   - $e = 3$

   Зашифрованное сообщение:

   - $c = 49651363397223905823361405524754222201232061708861391313885228248581660863824$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 13975144861324973727168741450542395505 9$
   - $e = 5$

   Зашифрованное сообщение:

   - $c = 28045934616670439169021532888630371382$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 29476251748531250412118023365033090099 3$
   - $g = 10697752022076912396874444005546124518 3$
   - $y = 86524560236338478130330076820283729157$

   Секретный ключ:

   - $x = 28241618731981559448165005887638539016 0$

   Сообщение:

   - $M = 25843691891077317437456744997048997311 8$

   Использовать следующий случайный параметр для создания подписи:

   - $k = 17338763629120264374977302520765605573 1$

   В ответе привести все промежуточные результаты вычислений.

   (b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 28393284735728991627853926067529584723 1$
   - $g = 19847716249004837773970237695782960634 3$

- $y = 163076126750657879491456639292675362574$

Сообщение:

- $M = 197259025844103689744084613814483250525$

Подпись:

- $a = 256782231473474163773161517561004794605$
- $b = 183124274277617019956398878497970453200$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 1013$
- $g = 548$
- $y = 712$

Сообщение:

- $M = 150$

Использовать следующий случайный параметр для создания подписи:

- $k = 197$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 15x - 14$ над конечным полем n=17. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).

Вариант № 110

1. (a) Расшифровать текст:

ЯЬЯЕЕЯВМШЬШДЗЧЬЩГВЕЮЮЯЬБЫШЦЫЧЯБЗЯБАДРТЬЦБВЦБЗГВДЪЩББЦЬШВАВЮДВЦЦЯ
ЩББВЭЧВЯВЦПТЯВЧЯЗМЩББЫЯГВАВБЮЫЯЕРХЩЫГАЖЬЮВАЩБШБЖГВШВЫЦЯЮГДЯЬЦЩЯЩ
ЯЩАЗЦЫЖРЯЬЕЖЬЫДЗЮЗХЬЖВЧВЮЫЮЮГДЯЦПМЩЯЦГВЯЩЬЦВЫЦДЖЬЯЕЦЩШГВШЗЕЖКПЯВ
МШРЗХЬЖВЧВВБЦДЗЛЬЯЮВАЩБШБЖЗГЬЕРАВЬЦБЮЗЫАЬЛГДВЛЩЯЩЧВГДВЕЩХЬДЫВДЦЯ
ГВЖВАЦЮЯВЛЮЬАЩЪШЗЖЩААЖЩЪББЮЬЦЬШЬАВГДЬЧВЖВЦЯЯЬЕРЮШЩЭЕЖЦЬТЦЕЮВДЩГЗ
ЯЬБЛЯЬЕЦЬЕЖЖРВЮВЯВБМЬЙЗМЩЭЬБЩЕЮВЯРЮВЕЖДЩЯЦВЖЮБЗЯЬЕРВЮВЯВБЕЦЫЩАЯТ
ЬЦЛЕЖВЮВЯЦЕЬЯЬЕЩЧВДВЦБЕЮЫЯЮВАЩБШБЖЫШЩЕРБЩХХРЩШЩЯВЗЦЩШЬАМЗЦЬШЬМРШ
ЩЦЮББЪЬЦБЬАЩДЖЦЦЕЬЯЬЕЩЧВДВЦБГДЬЕАЬДШЦМГВШГЗЯАЬЦЫЧЯБЗЯБЕЖЩГРБЮВЖВ
ДВЭЫАЩЖБВХПЯВХВЯРМВЩШЦЬЪЩБЬЩГВЖВАВХВДВЖЬЯЕРЮАЗЪЗЬЕЮЫЯЩАЗЬЦБЮЗЫАЬ
ЛЦЪЬЦВЖЩЬЕАЩДЖЬХВЧЦВЯЩБХЯЧВЕЯВЦЬАМЗАМГВШВЭШЬЮВЖКЗАМХЯЩШБЬЖДЩГЩНЗ
НГВШВМЯЮЬЦБЗЮЗЫАЬЛЗЕЖЯБЮВЯЩБЬЬГВЮЯВББЬЯЕРЩАЗЦЫЩАЯТЕЖДПЭЮВАЩБШБЖГЩ
ДЩЮДЩЕЖЬЯЩЩЖДЬЪШПГВЖВАГВШБЯЬГВКЯВЦЦЕЮЫЯЩЭЬЫАЩБЬЦМЬАЕЧВЯВЕВАБЗАМХ
ЗШРЕЛЕЖЯЬЦАВЯЬЕРХВЧЗВБЖЩХБЩВЕЖЦЬЖЮВЯЬБЭШЩЖЕШВХДПЭЛЩЯВЦЩЮШЭХВЧЦАЯ
ТХВЦРШЕВЦЩЖЪЬЦЬЖЩЮЮЪЬЯЬАПЕЦЕЬЯЬЕВЭЩЧВДВЦБВЭБЗГДВНЭАМЦЕЬЯЬЕЩЧВДВЦ
БЗЦЩШЬЪЩЩЩГВЕЮВДЩЭАМЮЬБЗЯЕРЩАЗБМЩТЬЫДПШЯГВКЯЗЩАЕЪЬАПЕЮЫЯЫГЯЮЦЮВА
ЩБШБЖМГДВНЭАВЭЬЦБЮЗЫАЬЛВЖГЗЕЖЬАБЩЮВЯЬЦЛЩАЖЩХЩШВЕШЬЯГДВНЭГДВНЭАЖЗ
МЮЕЮЫЯЮВАЩБШБЖВХБЦЕЦВТЕЖДЗЙЗБЗШВЦВЯРБВЕЖЗГЭЖЩЕЖЗГЭЖЩШВАВЭШЮВЯЬЗЕ
ГЩЩМРБШЩБРБАМЗЕДИБЮВАЩБШБЖМЕШВЛЩДРТЗШЯЬЯЬЕРЧЯШЩЯЦВЕЯЩШАДРЬЬЦБВЦБ
ПВББВЧЯБЗЯЕРЬЮЬЦБЗЯАБЩЧВЯВЦВЭЖЗЖЬЦБЮЗЫАЬЛВХВДВЖЬЯЕЮБАЬЦЕЩЦБЬАБЬЩЩ
ЧВЗЕЖДЩАЬЯВЕРББЩГДЬЖЩЯАЖЩЪББЮЬЕОЩЫЪЯЬЕРВЮВЯВЕЦВЩЧВГДЩШЦВШЬЖЩЯЬЦШ
ДЗЧБЛЯЬЕЯЩЫЖРЕЯВМШЩЭЖЩГЩДРЕЖВЭЖЩЮДЩГЮВЕЮЫЯЮВАЩБШБЖХЗШЩЖГДЬЕЖЗГЦС
ЖЗАЬБЗЖЗДЫШЯЕЕЖДМБПЭЦЬЫЧЬЮДЬЮЬАЖЩЪББЮЬХЩЧВ

(b) Расшифровать текст:

ЕУНЕЯЭТПТНЛММЩЛФСКЕЗЬЮДАВАТКЯЪЭЫЮАВЩИЮЬЖФЕОВЕДЬБЭЕКЬМВБУЯКЦЩИЖББ
БЖЯИБЩЕЦБАЧЖЯЛВШАЫЛДГЖЮХЬЮЙЬЯЯЕЭЫДХВДЫББЬЭЯДЩВЙЫКЦБЖЫЮЕЩНЭМЦЬГГГ
ШДЪЬЕЖЮКЦЖЬЮЖАКДЦЙУЯШГЖЕОЬБЙАПГЖЭЩШБПЭТЮЬЪЭЫДВХЖЮКБЬКУЗРБУЪЛДЩЬЭ
КЛЬКУОЖЗКЬЙВЕКЫКЦЬГЯДЕЖГЫЭЬЦККНЦВЦАМЗХВБНАВГМЭЬЩДЬБЖВИФБЕЖЪЬЮЯВЫ
ЬМШВЗЬНАВКЮБЯБПЦЙВЦЕЦЖВЦВЬОВДУУИЩЪЬБНВХЖМЛЩДЭЖБГЖУРЗЬЕФЯЮЬШЖЪЙЩЗ

ЬЬЮВЯФЯОЦЬАПБЕГЖШКЭЕКРЙВЧЖЯПШДАЪКЬГИЬАВЯЮЩКБЦУЭПЕЖАРЮАЩЙАБЕЧГБЭВ
ЮАЪЮЫШЖГКАЧЛЯОЗТЙАМЗТКПУБВЫЬАПАЛЫБЕАЭМЮЫЖФЫНЩХЙАКЯРЪУЗЬЮЛМКЖЦЭАН
ЖЦЭЫЙВЕККЖВЧЬТБЯВАТБЖВЩУГВГЙЫКЕЖАРЮЩДЭЫЙПЙДЫБГДЖРДБКАЧБЩЬДЭБДЖЖЮ
НЮЬДРБЯЬПУНЖЦЖЪЮЕЩДЦЗВЕКЦЮЩЭРУЕАВЭМЯВЕЛТМПБЭЧДЖЮЙЬЯЯМЦЯШЕХЖЩШМЬЕ
ЯОЦВДСКЯВЙЬЮЮВКЬМВЩИУФЬЯЖЕОВЦЙУЯВХГСКДЫЛЪЙЩЩАПБЫВЗЯЙЩЩЪЫПЖДАСКДВ
ЬЬВЬШКККЕШУЫЛШЩЕЦЙШГИЦОЩЯЙЦЗВЭИАДЯЯЭЮДЬЬЩБАЩВВФБЖЕЪЬГАВЮЫЧАЦУЩГЮ
ААЬОДЪККУЬБЖРЙЬЮАРНЦВЦЬУЩДЭТШБЕДУФЯЬЪЬЛВЧГТБЯЬЕЪББЕЖРБЖДЯЬФЩЯЙЫБ
АВЫЫБЕВЮЩБЖРЖЯЗХВЙАДГВПАББЖСКЦВАЫЖВЖЖЮЧЭБЗУМЩЮЖЮНВХЙАЮЩБЕЬИЗЗЩУ
ВШЩЕЦЪДЩРЩНЕЯЭТКЦЖФЪЙЩБАЪЗТШЭЧЙЩЕЪУАЗНАГДБЩЖЭЧЖБУГНГЗЙАЙЩЕВЬЗРЮЖ
ТЙЩЭЗЬНЯЩЙУЯВЫЕЪББЬКЬЯВЕЖРБЖЗЯЫЗЬАУЕОВГЛСУЩЦЪУМБПБЯЮВЩДБКХЩСЫДТГ
ИЦЭЯЬЮЦЗЕЮЖЮББХЛЮЯЗЗЪЦАЩЯЪЬЕЕЮЖЪОЩЪЕЦЖВЦЙРЧЕВКЙЯВДЖТНЮВБЯОЩБУЪЙЩ
ГЖШГЯВЙКУЖВПЦНЯВАГЮШЩЙАБДВЛРБЯЬПЦЗВЕФЯКЦДЭЪББЬЗЬНЯЩЬЫБЧВЗЮДЕЖЛЭЖ
ВЩДБЭПЯЙРДШЩКУЗРГИЦЙЬЙЩЙЗЬДКЦЗЯЩИЦЮЫЖЗБЯЛЩЪЙИЦАГЙСЮДЭЭКЕЖНЦИЗЪЭЭ
КЮВИУЙБПНРНГВДЫМЩМЭЫДЩЕЖРБЖГИУАЦЬЬУЗШВГСКЦДЭЪББЖУГЮЯЦЕББЬЭРНЖЩЕ
ГКДЩЕППДЧЙШДЙЬПБОРБЭЭЗЮЯЖААВЕЬЙЙЩЕКЫПВГАЯЧЦЖФЬМЩБЩБМЧЕВБЪВЕЬБЖВЖ
ЖЮЛДЬЕТЗЩЪААДЕЖЖЮДЬБЭЯБАЩБЯОЦЩЕЫЧАЫЗЦНЮАЙШВЗЦВЮОКЩПАКЕЬЖЯАГВЕУКЕ
ЖЖЮКЪБЖЯОЬАЭЯОББЫЬЙЛЯФЯОЦХУЩЯЬХЭЩШБШГФДЖЩГУЕЮВКЬМПЩЗЮБЖЩИЭБЯЬЫЬЗ
ВШАРНЩЦЖХИВЪЕЙБХЩЬЯОЦЬГУЯЮВДЬВВЙУЭЩЦЖЬЭДЫААШЛЖЖФДЫБФРКДЩЕППДЧЭП
ЧЯЕДЫБЕБЖЯЙЦЕЭЯПБПЕЦБАВЮЦАЯЬИУФЩБАЯЮВЩББУЕ

2. Разложить на множители числа:

   (a) 1124404311355118919948532368907

   (b) 9531753372734657681867648505389073752963816304609711060288209

   (c) 1552169414728385242998993140686291924816305249821621442061805691407299339203677584542210707

   (d) 1167247849909130104088590275411978402209983359910640413568670428994010624115063684726365127282165791301487084678071884817

3. (a) Зашифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 342244270762635379021258360208489247521281045349424076582380647915157677291 29$
   - $e = 5$

   Сообщение:

   - $M = 193184034200394339280126584324742495180021722972287328701406894725429115362 48$

   В ответе привести все промежуточные результаты вычислений.

   (b) Расшифровать сообщение по схеме RSA. Для генерации пары открытого и секретного ключа использовались числа:

   - $p = 335532158307560127146376017237069947313$
   - $q = 194211371001032852261720156631902694001$

   Открытая экспонента:

   - $e = 17$

   Зашифрованное сообщение:

   - $c = 170968415672627813302215166146949617093219768396823501837357584129048162281 44$

   В ответе привести все промежуточные результаты вычислений.

   (c) Расшифровать сообщение по схеме RSA. Открытый ключ:

   - $n = 206543682856068152383937647529343730189$
   - $e = 3$

   Зашифрованное сообщение:

   - $c = 182150649892770281304243678635874619 16$

   В ответе привести все промежуточные результаты вычислений.

4. (a) Вычислить подпись по схеме Эль-Гамаля. Открытый ключ:

   - $p = 268382606147239589786783550861914756167$
   - $g = 573050747372465729678627166575264670 8$
   - $y = 184247488415154203377105941638319467524$

Секретный ключ:

- $x = 158790243328145665998335339406221374 86$

Сообщение:

- $M = 107254483866622624154614989896045221154$

Использовать следующий случайный параметр для создания подписи:

- $k = 229584366118182845935247093885660268883$

В ответе привести все промежуточные результаты вычислений.

(b) Проверить подпись по схеме Эль-Гамаля. Открытый ключ:

- $p = 282528005426046152797053183213848617571$
- $g = 111685517351465788888134051462247981225$
- $y = 209819268803539003915488122657863195925$

Сообщение:

- $M = 108435981283308067868720490071648308225$

Подпись:

- $a = 253779698201821954076408191500492401624$
- $b = 135581751359783809471975836178899882733$

В ответе привести все промежуточные результаты вычислений.

(c) Подписать (подделать подпись) сообщения. Открытый ключ:

- $p = 827$
- $g = 226$
- $y = 676$

Сообщение:

- $M = 563$

Использовать следующий случайный параметр для создания подписи:

- $k = 575$

В ответе привести все промежуточные результаты вычислений.

5. Найти группу точек (перечислить все точки) эллиптической кривой $y^2 = x^3 - 2x - 12$ над конечным полем n=19. Для каждой точки определить, является ли она генератором всей группы точек, либо подгруппы. В последнем случае для каждой из подобных точек указать генерируемую подгруппу (все точки).