

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
прикладной математики и
информатики
А.М. Райгородский**

| | |
|----------------------------|---|
| | Рабочая программа дисциплины (модуля) |
| по дисциплине: | Теоретико-числовые алгоритмы и криптография |
| по направлению: | Прикладная математика и информатика |
| профиль подготовки: | Информатика |
| | Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики |
| курс: | 3 |
| квалификация: | бакалавр |

Семестр, формы промежуточной аттестации: 6 (весенний) - Дифференцированный зачет

Аудиторных часов: 60 всего, в том числе:

лекции: 30 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 75 час.

Всего часов: 135, всего зач. ед.: 3

Программу составил: А.М. Райгородский, д-р физ.-мат. наук, доцент

Программа обсуждена на заседании кафедры дискретной математики 16.03.2023

Аннотация

Теория чисел начала широко применяться в криптографии примерно 30-40 лет назад. Криптографические потребности стимулировали развитие ряда областей теории чисел и стали источником появления новых фундаментальных проблем. Стойкость целого ряда криптографических алгоритмов напрямую зависит от сложности решения некоторых задач вычислительной теории чисел. Целью курса является изучение основных теоретико-числовых алгоритмов, имеющих приложения в теории информации.

1. Цели и задачи

Цель дисциплины

Формирование у студентов навыков, необходимых для разработки математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность

Задачи дисциплины

- освоение студентами базовых знаний (понятий, концепций, методов и моделей) в области криптографии;
- приобретение теоретических знаний и практических умений и навыков в области криптографии;
- оказание консультаций и помощи студентам в проведении собственных теоретических исследований в области криптографии.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

| Код и наименование компетенции | Индикаторы достижения компетенции |
|---|---|
| УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи |
| | УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи |
| | УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки |
| | УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки |
| | УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи |
| ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук и использовать их в профессиональной деятельности | ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки |
| | ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения |
| | ОПК-1.3 Способен определять границы применимости полученных результатов |
| ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности | ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности |
| | ОПК-2.2 Знает и умеет применять численные математические методы и прикладное программное обеспечение для решения научных задач в профессиональной области |
| | ОПК-2.3 Знает основные требования информационной безопасности |
| ОПК-3 Способен составлять и оформлять | ОПК-3.1 Знает основные правила оформления научных публикаций и научно-технической документации, в том числе с использованием прикладного программного обеспечения |

| | |
|---|---|
| научные и (или) технические (технологические, инновационные) отчеты (публикации, проекты) | ОПК-3.2 Владеет на практике методологией составления научно-технических отчетов (проектов) |
| | ОПК-3.3 Владеет методами визуального и графического представления результатов научной (научно-технической, инновационной технологической) деятельности в виде отчетов, научных публикаций |
| ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты | ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности |
| | ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели |
| | ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты |
| ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию | ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива |
| | ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации |
| | ПК-2.3 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях |

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- базовые алгоритмы теории чисел, уметь доказывать их корректность и оценивать сложность;
- основные результаты о распределении простых чисел;
- основные методы проверки чисел на простоту, решения задач факторизации и дискретного логарифмирования; уметь доказывать их корректность;
- зависимость между стойкостью криптосистем с открытым ключом, а также сложностью их реализации с сложностью теоретико-числовых алгоритмов.

уметь:

- доказывать простоту больших целых чисел;
- строить простые числа заданного размера;
- решать задачу разложения больших целых чисел на множители;
- решать задачу дискретного логарифмирования.

владеть:

- навыками нахождения корней многочленов над конечным простым полем;
- построения простых чисел заданного размера;
- разложения чисел на множители и вычисления дискретных логарифмов в мультипликативной группе конечного простого поля.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

| № | Тема (раздел) дисциплины | Трудоемкость по видам учебных занятий, включая самостоятельную работу, час. | | | |
|---|--------------------------|---|----------|---------------------|---------|
| | | Лекции | Семинары | Лабораторные работы | Самост. |

| | | лекции | семинары | лаборат. работы | работа |
|-----------------------|--|---------------------|----------|-----------------|--------|
| 1 | Базовые сведения из теории чисел. | 5 | 5 | | |
| 2 | Криптографические алгоритмы, основанные на теории чисел. | 5 | 5 | | 15 |
| 3 | Распределение простых чисел. | 5 | 5 | | 15 |
| 4 | Исследование чисел на простоту | 5 | 5 | | 15 |
| 5 | Задача дискретного логарифмирования | 5 | 5 | | 15 |
| 6 | Задача факторизации | 5 | 5 | | 15 |
| Итого часов | | 30 | 30 | | 75 |
| Подготовка к экзамену | | 0 час. | | | |
| Общая трудоёмкость | | 135 час., 3 зач.ед. | | | |

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 6 (Весенний)

1. Базовые сведения из теории чисел.

Алгоритм Евклида вычисления наибольшего общего делителя, решения линейного сравнения и его сложность. Квадратичные вычеты и символ Якоби. Первообразные корни, показатели и их основные свойства. Решение полиномиальных сравнений. Быстрое возведение вычетов в степень. Алгоритм быстрого умножения Карацубы.

2. Криптографические алгоритмы, основанные на теории чисел.

Односторонние функции с секретом. Схема криптосистем с открытым ключом и электронных цифровых подписей. Алгоритмы шифрования RSA, Рабина, Эль-Гамала. Цифровые подписи RSA, Эль-Гамала. Старый стандарт цифровой подписи России. Криптостойкость указанных выше алгоритмов и требования к выбору параметров.

3. Распределение простых чисел.

Оценки Чебышева и их следствия. Постулат Бертрана. Асимптотический закон взаимности и его следствия. Открытые проблемы.

4. Исследование чисел на простоту

Числа Кармайкла. Вероятностные тесты простоты: тест Люка, Поклингтона, Прота, Соловья-Штрассена, Милера-Рабина. Алгоритмы доказательства простоты. Полиномиальный детерминированный тест простоты (тест Агравала — Каяла — Саксены). Алгоритмы построения больших простых чисел заданного размера.

5. Задача дискретного логарифмирования

Задача дискретного логарифмирования в произвольной группе. Алгоритм Гельфонда (алгоритм больших и малых шагов). Алгоритм Полига-Хеллмана. Субэкспоненциальные алгоритмы Адлемана и Копперсмита-Одлыжко-Шреппеля (алгоритм COS).

6. Задача факторизации

Экспоненциальные алгоритмы (Метод Ферма, методы Полларда-Флойда и Брента, методы $p-1$ и $p+1$). Решето Крайчика. Метод непрерывных дробей (Лемера), метод Моррисона-Бриллхарда, метод квадратичного решета и его дальнейшие модификации. Метод общего решета числового поля (обзор).

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Стандартная учебная аудитория.

6. Перечень рекомендуемой литературы

Основная литература

1. Основы современной криптографии для специалистов в информационных технологиях [Текст] / Б. Я. Рябко, А. Н. Фионов ; Ин-т вычислительных технологий СО РАН ; Сибирский гос. ун-т телекоммуникаций и информатики .— М. : Научный мир, 2004 .— 173 с.
2. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо .— М. : Техносфера, 2006 .— 528 с.

Дополнительная литература

1. Основы криптографии [Текст] : учеб. пособие для вузов / А. П. Алферов [и др.] .— 3-е изд., испр. и доп. — М. : Гелиос АРВ, 2005 .— 480 с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

<http://dm.fizteh.ru/>

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

На лекционных занятиях используются мультимедийные технологии, включая демонстрацию презентаций.

В процессе самостоятельной работы обучающихся возможно использование таких программных средств, как Mathcad, MATLAB, Maple и др.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Рекомендуется успешно сдавать контрольные работы, так как это упрощает итоговую аттестацию по предмету.

Для подготовки к итоговой аттестации по предмету лучше всего пользоваться материалами лекций.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

| | |
|----------------------------|--|
| по направлению: | Прикладная математика и информатика |
| профиль подготовки: | Информатика Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики |
| курс: | 3 |
| квалификация: | бакалавр |

Семестр, формы промежуточной аттестации: 6 (весенний) - Дифференцированный зачет

Разработчик: А.М. Райгородский, д-р физ.-мат. наук, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

| Код и наименование компетенции | Индикаторы достижения компетенции |
|---|---|
| УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи |
| | УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи |
| | УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки |
| | УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки |
| | УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи |
| ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук и использовать их в профессиональной деятельности | ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки |
| | ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения |
| | ОПК-1.3 Способен определять границы применимости полученных результатов |
| ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности | ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности |
| | ОПК-2.2 Знает и умеет применять численные математические методы и прикладное программное обеспечение для решения научных задач в профессиональной области |
| | ОПК-2.3 Знает основные требования информационной безопасности |
| ОПК-3 Способен составлять и оформлять научные и (или) технические (технологические, инновационные) отчеты (публикации, проекты) | ОПК-3.1 Знает основные правила оформления научных публикаций и научно-технической документации, в том числе с использованием прикладного программного обеспечения |
| | ОПК-3.2 Владеет на практике методологией составления научно-технических отчетов (проектов) |
| | ОПК-3.3 Владеет методами визуального и графического представления результатов научной (научно-технической, инновационной технологической) деятельности в виде отчетов, научных публикаций |
| ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты | ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности |
| | ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели |
| | ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты |
| ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию | ПК-2.2 Способен планировать и проводить научные исследования самостоятельно или в качестве члена (руководителя) малого научного коллектива |
| | ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации |

2. Показатели оценивания компетенций

В результате изучения дисциплины «Теоретико-числовые алгоритмы и криптография» обучающийся должен:

знать:

- базовые алгоритмы теории чисел, уметь доказывать их корректность и оценивать сложность;
- основные результаты о распределении простых чисел;
- основные методы проверки чисел на простоту, решения задач факторизации и дискретного логарифмирования; уметь доказывать их корректность;
- зависимость между стойкостью криптосистем с открытым ключом, а также сложностью их реализации с сложностью теоретико-числовых алгоритмов.

уметь:

- доказывать простоту больших целых чисел;
- строить простые числа заданного размера;
- решать задачу разложения больших целых чисел на множители;
- решать задачу дискретного логарифмирования.

владеть:

- навыками нахождения корней многочленов над конечным простым полем;
- построения простых чисел заданного размера;
- разложения чисел на множители и вычисления дискретных логарифмов в мультипликативной группе конечного простого поля.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Домашние задания: часть материала из лекций будет предлагаться учащимся в виде задач для самостоятельного решения. Желаящие могут получить задание, связанное с реализацией на ЭВМ алгоритмов из лекций.

Коллоквиум: в середине семестра планируется провести коллоквиум, который будет заключаться в письменном ответе на один (или два) теоретических вопроса.

Примерный список вопросов к коллоквиуму:

1. Сложность алгоритма Евклида. Сложность вычисления символа Якоби.
2. Квадратичные вычеты и первообразные корни (основные свойства).
3. Методы решения квадратного сравнения по простому модулю.
4. Алгоритм быстрого умножения Карацубы.
5. Криптографические алгоритмы RSA и Рабина.
6. Криптографические алгоритмы Эль-Гамала.
7. Оценки Чебышева и их следствия.
8. Постулат Бертрана.
9. Асимптотический закон распределения простых чисел и его следствия.
10. Тест простоты Ферма и числа Кармайкла.
11. Тесты простоты Люка, Поклингтона и Прота.
12. Тест простоты Соловея-Штрассена.
13. Тест простоты Миллера-Рабина.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

1. Сложность алгоритма Евклида. Сложность вычисления символа Якоби.
2. Квадратичные вычеты и первообразные корни (основные свойства).
3. Методы решения квадратного сравнения по простому модулю.
4. Алгоритм быстрого умножения Карацубы.
5. Криптографические алгоритмы RSA и Рабина.

6. Криптографические алгоритмы Эль-Гамала.
7. Оценки Чебышева и их следствия.
8. Постулат Бертрона.
9. Асимптотический закон распределения простых чисел и его следствия.
10. Тест простоты Ферма и числа Кармайкла.
11. Тесты простоты Люка, Поклингтона и Прота.
12. Тест простоты Соловея-Штрассена.
13. Тест простоты Миллера-Рабина.
14. Полиномиальный детерминированный тест простоты.
15. Задача дискретного логарифмирования. Основные свойства. Метод Гельфонда.
16. Задача дискретного логарифмирования: алгоритм Полига-Хеллмана.
17. Задача дискретного логарифмирования: алгоритм Адлемана.
18. Задача дискретного логарифмирования: алгоритм COS.
19. Задача факторизации: решето Эратосфена, метод Ферма, методы Полларда-Флойда, Брента.
20. Задача факторизации: методы $p-1$ и $p+1$.
21. Задача факторизации: решето Крайчика.
22. Задача факторизации: метод непрерывных дробей.
23. Задача факторизации: метод Моррисона-Бриллхарда.
24. Задача факторизации: метод квадратичного решета.

Критерии оценивания

- оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений
- оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач

- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения дифференцированного зачета обучающиеся могут пользоваться программой дисциплины.