

**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:	Криптография
по направлению:	Прикладная математика и информатика
профиль подготовки:	Информатика
	Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
курс:	4
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Дифференцированный зачет

Аудиторных часов: 60 всего, в том числе:

лекции: 30 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Всего часов: 90, всего зач. ед.: 2

Количество контрольных работ, заданий: 1

Программу составил: Д.В. Мусатов, канд. физ.-мат. наук, доцент

Программа обсуждена на заседании кафедры дискретной математики 05.03.2020

Аннотация

Курс ориентирован прежде всего на теоретические основы криптографии: криптографические примитивы, связи между ними и построение протоколов на их основе. В курсе почти не уделяется внимания конкретным функциям, реализующим те или иные криптографические задачи, и тем более конкретным их реализациям. Вместо этого вначале вводятся базовые понятия криптографии (криптографические примитивы), доказываются теоремы об их связях между собой, а затем строятся протоколы решения различных криптографических задач на основе этих примитивов. Про эти протоколы доказывается корректность при условии, что примитивы удовлетворяют определённым требованиям.

1. Цели и задачи

Цель дисциплины

освоение основных современных методов криптографии.

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
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-5 Способен участвовать в проведении фундаментальных и прикладных исследований и разработок, самостоятельно осваивать новые теоретические, в том числе, математические методы исследований и работать на современной экспериментальной научно-исследовательской, измерительно-аналитической и технологической аппаратуре	ОПК-5.2 Обладает способностью к освоению новых знаний на основе изучения литературы, научных статей и других источников

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- ☐ фундаментальные понятия, законы, теории части криптографии;
- ☐ современные проблемы соответствующих разделов криптографии;
- ☐ понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла криптографии;
- ☐ основные свойства соответствующих математических объектов;
- ☐ аналитические и численные подходы и методы для решения типовых прикладных задач криптографии.

уметь:

- ☐ понять поставленную задачу;
- ☐ использовать свои знания для решения фундаментальных и прикладных задач криптографии;
- ☐ оценивать корректность постановок задач;
- ☐ строго доказывать или опровергать утверждение;
- ☐ самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;
- ☐ самостоятельно видеть следствия полученных результатов;
- ☐ точно представить математические знания в области в устной и письменной форме.

владеть:

- ☐ навыками освоения большого объема информации и решения задач (в том числе, сложных);
- ☐ навыками самостоятельной работы и освоения новых дисциплин;
- ☐ культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов;
- ☐ предметным языком дискретной математики и навыками грамотного описания решения задач и представления полученных результатов.

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	Лаборат. работы	Самост. работа
1	Комбинаторный подход к понятию информации	6	6		
2	Генераторы псевдослучайных чисел	6	6		
3	Надежные схемы шифрования	6	6		
4	Псевдослучайные перестановки	6	6		
5	Определение надёжной схемы аутентификации	6	6		30
Итого часов		30	30		30
Подготовка к экзамену		0 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

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

Семестр: 7 (Осенний)

1. Комбинаторный подход к понятию информации

Односторонние функции. Определение количества информации в конечном объекте (информация по Хартли).

2. Генераторы псевдослучайных чисел

Вероятностный подход к понятию информации.

3. Надежные схемы шифрования

Энтропия Шеннона: определение и основные свойства.

4. Псевдослучайные перестановки

Задача о совершенном разделении секрета. Пороговые структуры доступа, схема Шамира. Идеальное разделение секрета; структуры доступа, не допускающие идеального разделения секрета.

5. Определение надёжной схемы аутентификации

Комбинаторные модели канала с шумом. Линейные коды. Простейшие границы для параметров кодов, исправляющих ошибки.

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)

1. Рекомендуется успешно сдавать контрольные работы, так как это упрощает итоговую аттестацию по предмету.
2. Для подготовки к итоговой аттестации по предмету лучше всего пользоваться материалами лекций.

ПРИЛОЖЕНИЕ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Прикладная математика и информатика
профиль подготовки:	Информатика Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
курс:	4
квалификация:	бакалавр
Семестр, формы промежуточной аттестации: 7 (осенний) - Дифференцированный зачет	
Разработчик:	Д.В. Мусатов, канд. физ.-мат. наук, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
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-5 Способен участвовать в проведении фундаментальных и прикладных исследований и разработок, самостоятельно осваивать новые теоретические, в том числе, математические методы исследований и работать на современной экспериментальной научно-исследовательской, измерительно-аналитической и технологической аппаратуре	ОПК-5.2 Обладает способностью к освоению новых знаний на основе изучения литературы, научных статей и других источников

2. Показатели оценивания компетенций

В результате изучения дисциплины «Криптография» обучающийся должен:

знать:

- ☐ фундаментальные понятия, законы, теории части криптографии;
- ☐ современные проблемы соответствующих разделов криптографии;
- ☐ понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла криптографии;
- ☐ основные свойства соответствующих математических объектов;
- ☐ аналитические и численные подходы и методы для решения типовых прикладных задач криптографии.

уметь:

- ☐ понять поставленную задачу;
- ☐ использовать свои знания для решения фундаментальных и прикладных задач криптографии;
- ☐ оценивать корректность постановок задач;
- ☐ строго доказывать или опровергать утверждение;
- ☐ самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;
- ☐ самостоятельно видеть следствия полученных результатов;
- ☐ точно представить математические знания в области в устной и письменной форме.

владеть:

- ☐ навыками освоения большого объема информации и решения задач (в том числе, сложных);
- ☐ навыками самостоятельной работы и освоения новых дисциплин;
- ☐ культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов;
- ☐ предметным языком дискретной математики и навыками грамотного описания решения задач и представления полученных результатов.

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

Оценка за курс складывается из двух компонентов: решения домашнего задания и письменной контрольной (в случае перехода на онлайн-обучение она может быть заменена на тест). Домашнее задание состоит из 12-13 задач, оцениваемых в 10 баллов, из которых засчитываются 8 наилучших. Контрольная состоит из двух частей. В первой части даются 5 простых вопросов по 5 баллов на 30 минут, в процессе написания ничем нельзя пользоваться. Во второй части даются 4 задачи по 15 баллов на 90 минут, при решении можно пользоваться конспектами и литературой.

Примеры задач из домашнего задания

1. Докажите, что найдутся случайные величины X_n и Y_n , не отличимые вероятностными полиномиальными алгоритмами, но отличимые схемами полиномиального размера.

2. После того, как трое студентов, изучающих криптографию, пообедали в ресторане, выяснилось, что кто-то заплатил за всех. Это мог быть либо один из студентов, либо преподаватель. Студенты хотят выяснить, был ли это преподаватель или кто-то из них, не раскрывая, кто именно. Как им это сделать? Можно ли этот протокол обобщить на n студентов? Сколько битов при этом нужно будет передать?

3. Предложите аналог протокола Bingo Voting, при котором в результате подведения итогов выборов с n кандидатами и результатами T_1, \dots, T_n становятся известны числа R_1, \dots, R_n , такие что $T_i \leq R_i \leq T_{i+m}$ для некоторого m .

Примеры задач из первой части контрольной

1. Дайте определения сильно и слабо односторонних функций. Докажите, что любая сильно односторонняя функция является слабо односторонней.

2. Опишите какой-нибудь протокол шифрования с открытым ключом (на базе произвольной функции с определёнными требованиями к ней, либо конкретной предположительно сложной задачи).

3. Изложите требования к надёжному протоколу электронных выборов.

Примеры задач из второй части контрольной

1. Пусть $f: \{0,1\}^n \rightarrow \{0,1\}^n$ – односторонняя функция, $g: \{0,1\}^n \rightarrow \{0,1\}^n$ – полиномиально вычислимая функция. Докажите, что функция $h: \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$, определённая равенством $h(xy) = f(g(x))y$, также односторонняя.

2. Пусть генераторы псевдослучайных чисел существуют. Рассмотрим преобразование функций $H'(x) = H(xx)$ (неявная операция – конкатенация). Докажите, что существуют генераторы псевдослучайных чисел G , такие что G' также является генератором, и такие что это неверно.

3. Описан некоторый протокол криптографического взаимодействия. Проанализируйте его с точки зрения надёжности.

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

1. Односторонние функции. Определение и примеры предположительно односторонних функций.
2. Слабо односторонние функции. Построение односторонней функции по любой слабо односторонней функции.
3. Генераторы псевдослучайных чисел. Два определения надёжности и теорема Яо об их эквивалентности.
4. Построение генератора, преобразующего случайное зерно из p битов в псевдослучайное слово из $\text{poly}(p)$ битов, на основе генератора, преобразующего зерно из p битов в слово из $p + 1$ бита.
5. Построение генератора псевдослучайных чисел на основе любой труднообратимой перестановки с трудным битом.
6. Построение труднообратимой перестановки с трудным битом на основе любой труднообратимой перестановки.
7. Построение надёжной схемы шифрования с закрытым ключом на основе генератора.
8. Труднообратимые перестановки с секретом. Определение и два примера предположительно труднообратимой перестановки с секретом: функция RSA, функция Рабина.
9. Определение надёжной схемы шифрования с открытым ключом. Построение такой схемы на основе труднообратимой перестановки с секретом.
10. Интерактивные доказательства и класс IP. Интерактивное доказательство неизоморфности данных графов.
11. Интерактивные доказательства с нулевым разглашением. Доказательство с нулевым разглашением изоморфизма данных графов.
12. Определение надёжной схемы аутентификации. Построение такой схемы в предположении необратимости функции, дающей по графу и перестановке его вершин исходный граф и граф с переставленными вершинами.

13. Определение надёжного протокола запечатывания бита. Построение такого протокола на основе генератора псевдослучайных чисел.
14. Доказательство с нулевым разглашением существования раскраски данного графа в 3 цвета.
15. Определение надёжной схемы бросания монетки по телефону. Построение такой схемы на основе протокола запечатывания бита.
16. Определение надёжной схемы удостоверения сообщения. Построение такой схемы на основе псевдослучайной функции.
17. Определение надёжной схемы цифровой подписи. Построение такой схемы для сообщений произвольной длины на основе схемы для сообщений фиксированной длины.
18. Определение надёжной схемы одноразовой цифровой подписи. Построение такой схемы на основе односторонней функции.
19. Построение надёжной схемы многоразовой цифровой подписи на основе схемы одноразовой цифровой подписи.
20. Общая задача безопасных распределённых вычислений. Построение схемы безопасных двусторонних вычислений в полустечной модели на основе протокола слепой передачи бита.
21. Определение протокола слепой передачи бита и его построение на основе улучшенного семейства труднообратимых функций.
22. Построение псевдослучайного генератора на основе произвольной инъективной односторонней функции.
23. Построение псевдослучайного генератора на основе произвольной односторонней функции.
24. Псевдослучайные перестановки: определение и построение на основе псевдослучайных функций.
25. Построение доказательства с нулевым разглашением для произвольного языка из NP.
26. Доказательства знания (Proofs of knowledge)
27. Доказательства с нулевым разглашением с ограниченным числом раундов.
28. Нсинтерактивные доказательства с нулевым разглашением.
29. Схемы шифрования, устойчивые относительно выборочной атаки на шифруемый текст.
30. Построение семейства хеш-функций, свободного от коллизий.
31. Универсальное семейство хеш-функций: конструкция и применения.
32. Безопасные многосторонние вычисления в полустечной модели.
33. Безопасные многосторонние вычисления в модели с приватными каналами связи.

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.