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: Теоретическая криптография
по направлению: Прикладные математика и физика
профиль подготовки: Радиотехника и компьютерные технологии
Физтех-школа Радиотехники и Компьютерных Технологий
кафедра системного программирования
курс: 4
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Экзамен

Аудиторных часов: 60 всего, в том числе:
лекции: 30 час.
семинары: 30 час.
лабораторные занятия: 0 час.

Самостоятельная работа: 45 час.

Подготовка к экзамену: 30 час.

Всего часов: 135, всего зач. ед.: 3

Программу составил: Н.П. Варновский

Программа обсуждена на заседании кафедры системного программирования 15.05.2020

Аннотация

Начальные лекции представляют собой введение в криптографию. Студенты знакомятся с тремя задачами криптографии: конфиденциальностью, целостностью и неотслеживаемостью, а также с основными понятиями криптографии: криптографический протокол, криптографический примитив, противник, атака, угроза, стойкости и т.д.

На последующих лекциях изучаются криптосистемы с открытым ключом как пример криптографических протоколов, решающих задачу конфиденциальности. Задача обеспечения целостности иллюстрируется протоколами электронной подписи.

Курс завершается двумя специальными темами: понятие доказательства с нулевым разглашением и протокол электронных платежей. Последний доставляет пример решения задачи обеспечения неотслеживаемости.

1. Цели и задачи

Цель дисциплины

Ознакомить студентов, специализирующихся в области программирования, с основными проблемами, возникающими в современной теоретической криптографии, основными понятиями и криптографическими примитивами, являющимися основой построения доказуемо стойких криптосистем и протоколов.

Задачи дисциплины

Основное внимание в курсе уделяется математически строгим определениям основных понятий современной теоретической криптографии и доказательствам стойкости различных типов криптосистем и криптографических протоколов.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
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
ПК-3 Способен выбирать и применять подходящее оборудование, инструменты и методы исследований для решения задач в избранной предметной области	ПК-3.1 Знает принципы работы и диапазоны рабочих параметров используемого научного оборудования
ПК-4 Способен критически оценивать применимость используемых методик и методов	ПК-4.1 Знает численные порядки величин, характерных для соответствующей профессиональной области

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- фундаментальные понятия, теории современного системного программирования;
- криптографические протоколы - прикладные и примитивные;
- криптографически стойкие генераторы псевдослучайных последовательностей.

уметь:

- разрабатывать, обосновывать и реализовывать новые методы и алгоритмы машинно-независимой оптимизации программ;
- криптографические хэш-функции. Определения семейства односторонних хэш-функций и семейства функций с трудно обнаружимыми коллизиями;
- применять компиляторные методы и компиляторные среды для решения задач обратной инженерии, защиты программного кода, обнаружения дефектов в программах и др.

владеть:

 основными проблемами, возникающими в современной теоретической криптографии;
 основными понятиями и криптографическими примитивами, являющимися основой построения доказуемо стойких криптосистем и протоколов;
 навыками самостоятельной работы в Интернете.

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	Введение. Предмет математической криптографии.	5	5		7
2	Класс P/poly. Теорема об эквивалентности двух определений эффективного алгоритма: через класс P/poly и через семейство схем полиномиального размера. Вложение класса BPP в класс P/po1y.	5	5		7
3	Построение генератора псевдослучайных последовательностей исходя из произвольной односторонней перестановки.	5	5		7
4	Доказательство существования стойкой потоковой криптосистемы с секретным ключом в предположении существования генератора псевдослучайных последовательностей.	5	5		8
5	Схемы электронной подписи. Понятие об аутентификации сообщений. Определение схемы электронной подписи.	5	5		8
6	Протоколы интерактивного доказательства с нулевым разглашением. Понятие интерактивной пары машин Тьюринга. Определение протокола интерактивного доказательства для языка.	5	5		8
Итого часов		30	30		45
Подготовка к экзамену		30 час.			
Общая трудоёмкость		135 час., 3 зач.ед.			

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

Семестр: 7 (Осенний)

1. Введение. Предмет математической криптографии.

Криптографические протоколы - прикладные и примитивные. Криптографические примитивы. Модель противника. Стойкость криптографических протоколов и криптографических примитивов. Три задачи криптографии - обеспечение конфиденциальности, целостности, неотслеживаемости.

Элементы теории сложности вычислений. Вероятностная машина Тьюринга. Классы BPP и RP. Рандомизированные вычисления за полиномиальное в среднем время. Формализация понятия эффективного алгоритма в однородной и неоднородной моделях вычислений.

2. Класс P/poly. Теорема об эквивалентности двух определений эффективного алгоритма: через класс P/poly и через семейство схем полиномиального размера. Вложение класса BPP в класс P/po1y.

Односторонние функции. Определения сильной и слабой односторонних функций. Теорема Яо об эквивалентности предположений о существовании сильных и слабых односторонних функций.

Понятие трудного предиката функции. Теорема Гольдрайха-Левина о существовании у односторонней функции трудного предиката.

Криптографически стойкие генераторы псевдослучайных последовательностей. Понятие вычислительной неотличимости семейств распределений вероятностей.

Два определения генератора псевдослучайных последовательностей: через неотличимость от равномерно распределенных последовательностей и через тест следующего бита. Теорема Яо об эквивалентности этих определений.

3. Построение генератора псевдослучайных последовательностей исходя из произвольной односторонней перестановки.

Теорема Хостада и др. (без доказательства) о необходимом и достаточном условии существования генераторов псевдослучайных последовательностей.

Криптосистемы с секретным ключом. Блоковые и потоковые криптосистемы.

Атаки на криптосистемы и угрозы безопасности криптосистем. Определение стойкости криптосистемы.

4. Доказательство существования стойкой потоковой криптосистемы с секретным ключом в предположении существования генератора псевдослучайных последовательностей.

Генераторы псевдослучайных функций и псевдослучайных перестановок. Определение генератора псевдослучайных функций. Теорема Гольдрайха и др. о существовании генераторов псевдослучайных функций в предположении существования генераторов псевдослучайных последовательностей.

Определение генератора обратимых псевдослучайных перестановок. Преобразование Файстеля. Теорема Луби и Ракоффа (без доказательства) о необходимом и достаточном условии существования обратимых псевдослучайных перестановок.

Построение доказуемо стойких блоковых криптосистем исходя из генераторов псевдослучайных функций или генераторов псевдослучайных перестановок.

5. Схемы электронной подписи. Понятие об аутентификации сообщений. Определение схемы электронной подписи.

Арбитраж. Атаки на схемы электронной подписи и угрозы их безопасности.

Определение стойкости для схемы электронной подписи. Схема Лампорта.

Криптографические хэш-функции. Определения семейства односторонних хэш-функций и семейства функций с трудно обнаружимыми коллизиями. Теорема Наора и Юнга: если существуют односторонние перестановки, то существуют семейства односторонних хэш-функций.

Применение хэш-функций к преобразованию одноразовой схемы электронной подписи в многоразовую. Теорема Ромпеля (без доказательства) о необходимом и достаточном условии существования стойких схем электронной подписи.

6. Протоколы интерактивного доказательства с нулевым разглашением. Понятие интерактивной пары машин Тьюринга. Определение протокола интерактивного доказательства для языка.

Свойство нулевого разглашения: вычислительное, статистическое, абсолютное. Протокол доказательства с абсолютно нулевым разглашением для языка ИЗОМОРФИЗМ ГРАФОВ.

Протокол привязки к биту. Понятие блоба. Теорема Гольдрайха и др. (идея доказательства) о существовании протоколов доказательства с нулевым разглашением для всех языков из класса NP. Понятие интерактивной аутентификации.

Криптосистемы с открытым ключом. Определение криптосистемы с открытым ключом. Атаки и угрозы для криптосистем с открытым ключом.

Определение функции с секретом. Криптосистема Рабина. Доказательство стойкости криптосистемы Рабина в предположении вычислительной трудности задачи факторизации целых чисел.

Понятие неотслеживаемости. Системы электронных платежей. Электронная монета.

Схема электронной подписи вслепую.

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

Необходимое оборудование для лекций и практических занятий: компьютер и мультимедийное оборудование (проектор, звуковая система).

6.Перечень рекомендуемой литературы

Основная литература

1. Van Tilborg H.C.A., Jajodia S., Encyclopedia of Cryptography and Security - Springer, 2011,
2. Фомичев В. М. Методы дискретной математики и криптологии. – М.: Диалог-МИФИ, 2010,
3. Goldreich O., Foundations of Cryptography. Basic Applications, Cambridge university press, 2004,

Дополнительная литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001.
2. Katz J., Lindell Y., Introduction to Modern Cryptography: Principles and Protocols - Chapman and Hall/CRC, 2007
3. Wenbo Mao, Modern Cryptography: Theory and Practice – М.: Издательский дом "Вильямс", 2005,

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

http://www.thefreecountry.com/programming/compilerconstruction.shtml, http://llvm.org/, http://gcc.gnu.org/, http://suif.stanford.edu/suif/suif2/,

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

Программное обеспечение и информационные технологии не требуются.

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

Студент, изучающий дисциплину, должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

В результате изучения дисциплины студент должен знать основные определения, понятия, аксиомы, алгоритмы.

Успешное освоение курса требует напряжённой самостоятельной работы студента. В программе курса приведено минимально необходимое время для работы студента над темой. Самостоятельная работа включает в себя:

– чтение и конспектирование рекомендованной литературы,

– проработку учебного материала (по конспектам лекций, учебной и научной литературе), подготовку ответов на вопросы, предназначенных для самостоятельного изучения, доказательство отдельных утверждений, свойств;

– подготовку к экзамену.

Руководство и контроль за самостоятельной работой студента осуществляется в форме индивидуальных консультаций.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к лектору.

ПРИЛОЖЕНИЕ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Прикладные математика и физика
профиль подготовки: Радиотехника и компьютерные технологии
Физтех-школа Радиотехники и Компьютерных Технологий
кафедра системного программирования
курс: 4
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Экзамен

Разработчик: Н.П. Варновский

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
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
ПК-3 Способен выбирать и применять подходящее оборудование, инструменты и методы исследований для решения задач в избранной предметной области	ПК-3.1 Знает принципы работы и диапазоны рабочих параметров используемого научного оборудования
ПК-4 Способен критически оценивать применимость используемых методик и методов	ПК-4.1 Знает численные порядки величин, характерных для соответствующей профессиональной области

2. Показатели оценивания компетенций

В результате изучения дисциплины «Теоретическая криптография» обучающийся должен:

знать:

- фундаментальные понятия, теории современного системного программирования;
- криптографические протоколы - прикладные и примитивные;
- криптографически стойкие генераторы псевдослучайных последовательностей.

уметь:

- разрабатывать, обосновывать и реализовывать новые методы и алгоритмы машинно-независимой оптимизации программ;
- криптографические хэш-функции. Определения семейства односторонних хэш-функций и семейства функций с трудно обнаружимыми коллизиями;
- применять компиляторные методы и компиляторные среды для решения задач обратной инженерии, защиты программного кода, обнаружения дефектов в программах и др.

владеть:

- основными проблемами, возникающими в современной теоретической криптографии;
- основными понятиями и криптографическими примитивами, являющимися основой построения доказуемо стойких криптосистем и протоколов;
- навыками самостоятельной работы в Интернете.

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

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по теме прошлой лекции или в конце занятия по пройденной теме.

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

1. Стойкость криптографических протоколов и криптографических примитивов. Три задачи криптографии - обеспечение конфиденциальности, целостности, неотслеживаемости.
2. Элементы теории сложности вычислений. Вероятностная машина Тьюринга. Классы BPP и RP. Рандомизированные вычисления за полиномиальное в среднем время. Формализация понятия эффективного алгоритма в однородной и неоднородной моделях вычислений.
3. Класс P/poly. Теорема об эквивалентности двух определений эффективного алгоритма: через класс P/poly и через семейство схем полиномиального размера. Вложение класса BPP в класс P/po1y.
4. Односторонние функции. Определения сильной и слабой односторонних функций. Теорема Яо об эквивалентности предположений о существовании сильных и слабых односторонних функций.

5. Понятие трудного предиката функции. Теорема Гольдрайха-Левина о существовании у односторонней функции трудного предиката.

6. Криптографически стойкие генераторы псевдослучайных последовательностей. Понятие вычислительной неотличимости семейств распределений вероятностей.

7. Два определения генератора псевдослучайных последовательностей: через неотличимость от равномерно распределенных последовательностей и через тест следующего бита. Теорема Яо об эквивалентности этих определений.

8. Построение генератора псевдослучайных последовательностей исходя из произвольной односторонней перестановки. Теорема Хостада и др. (без доказательства) о необходимом и достаточном условии существования генераторов псевдослучайных последовательностей.

9. Криптосистемы с секретным ключом. Блоковые и потоковые криптосистемы.

10. Атаки на криптосистемы и угрозы безопасности криптосистем. Определение стойкости криптосистемы.

11. Доказательство существования стойкой потоковой криптосистемы с секретным ключом в предположении существования генератора псевдослучайных последовательностей.

12. Генераторы псевдослучайных функций и псевдослучайных перестановок. Определение генератора псевдослучайных функций. Теорема Гольдрайха и др. о существовании генераторов псевдослучайных функций в предположении существования генераторов псевдослучайных последовательностей.

13. Определение генератора обратимых псевдослучайных перестановок. Преобразование Файстеля. Теорема Луби и Ракоффа (без доказательства) о необходимом и достаточном условии существования обратимых псевдослучайных перестановок.

14. Построение доказуемо стойких блоковых криптосистем исходя из генераторов псевдослучайных функций или генераторов псевдослучайных перестановок.

15. Схемы электронной подписи. Понятие об аутентификации сообщений. Определение схемы электронной подписи.

16. Арбитраж. Атаки на схемы электронной подписи и угрозы их безопасности.

17. Определение стойкости для схемы электронной подписи. Схема Лампорта.

18. Криптографические хэш-функции. Определения семейства односторонних хэш-функций и семейства функций с трудно обнаружимыми коллизиями. Теорема Наора и Юнга: если существуют односторонние перестановки, то существуют семейства односторонних хэш-функций.

19. Применение хэш-функций к преобразованию одноразовой схемы электронной подписи в многоразовую. Теорема Ромпеля (без доказательства) о необходимом и достаточном условии существования стойких схем электронной подписи.

20. Протоколы интерактивного доказательства с нулевым разглашением. Понятие интерактивной пары машин Тьюринга. Определение протокола интерактивного доказательства для языка.

21. Свойство нулевого разглашения: вычислительное, статистическое, абсолютное. Протокол доказательства с абсолютно нулевым разглашением для языка ИЗОМОРФИЗМ ГРАФОВ.

22. Протокол привязки к биту. Понятие блоба. Теорема Гольдрайха и др. (идея доказательства) о существовании протоколов доказательства с нулевым разглашением для всех языков из класса NP. Понятие интерактивной аутентификации.

23. Криптосистемы с открытым ключом. Определение криптосистемы с открытым ключом. Атаки и угрозы для криптосистем с открытым ключом.

24. Определение функции с секретом. Криптосистема Рабина. Доказательство стойкости криптосистемы Рабина в предположении вычислительной трудности задачи факторизации целых чисел.

25. Вероятностные криптосистемы с открытым ключом и их стойкость.

26. Понятие неотслеживаемости. Системы электронных платежей. Электронная монета.

Примерный перечень билетов:

Билет №1.

1. Криптографически стойкие генераторы псевдослучайных последовательностей. Понятие вычислительной неотличимости семейств распределений вероятностей.

2. Криптосистемы с секретным ключом. Блоковые и потоковые криптосистемы.

Билет №2.

1. Два определения генератора псевдослучайных последовательностей: через неотличимость от равномерно распределенных последовательностей и через тест следующего бита. Теорема Яо об эквивалентности этих определений.

2. Атаки на криптосистемы и угрозы безопасности криптосистем. Определение стойкости криптосистемы.

Критерии оценивания

Оценка отлично 10 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 9 баллов - 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 8 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо 7 баллов - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо 6 баллов - 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 5 баллов - выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно 4 балла - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно 3 балла - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно 2 балла - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно 1 балл - выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

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

Во время проведения экзамена обучающиеся могут пользоваться программой дисциплины, а также справочной литературой, вычислительной техникой, конспектами лекций.

Экзамен проводится путем организации специального опроса, проводимого в устной форме.