МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____
"___"_____20___ г.

Программа дисциплины

Криптоанализ асимметричных шифров Б1.В.ДВ.10

Направление подготовки: 02.03.02 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Системный анализ и информационные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Разинков Е.В.
Рецензент(ы):
Ишмухаметов Ш.Т.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань
2016

Содержание

Программу дисциплины разработал(а)(и) ассистент, к.н. Разинков Е.В. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Evgenij.Razinkov@kpfu.ru

1. Цели освоения дисциплины

В рамках курса "Криптоанализ асимметричных шифров" рассматриваются математические соновы криптографии с открытым ключом, вопросы стойкости асимметричных криптографических систем, возможные атаки на такие криптосистемы.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б1.В.ДВ.10 Дисциплины (модули)" основной образовательной программы 02.03.02 Фундаментальная информатика и информационные технологии и относится к дисциплинам по выбору. Осваивается на 3 курсе, 6 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 3 курсе в 6 семестре для студентов обучающихся по направлению "Фундаментальная информатика и информационные технологии".

Изучение основывается на результатах изучения дисциплин "Алгебра и геометрия", "Дискретная математика".

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-1 (профессиональные компетенции)	способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям
ПК-10 (профессиональные компетенции)	способностью реализовывать процессы управления качеством производственной деятельности, связанной с созданием и использованием информационных технологий, осуществлять мониторинг и оценку качества процессов производственной деятельности
ПК-11 (профессиональные компетенции)	способностью составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы
ПК-2 (профессиональные компетенции)	способностью понимать, совершенствовать и применять современный математический аппарат, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий
ПК-3 (профессиональные компетенции)	способностью использовать современные инструментальные и вычислительные средства
ПК-4 (профессиональные компетенции)	способностью решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-7 (профессиональные компетенции)	способностью разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий
ПК-8 (профессиональные компетенции)	способностью применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства
ПК-9 (профессиональные компетенции)	способностью разрабатывать, оценивать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов информационных технологий, а также реализовывать методы и механизмы оценки и анализа функционирования средств и информационных технологий; разрабатывать проектную и программную документацию, удовлетворяющую нормативным требованиям

В результате освоения дисциплины студент:

1. должен знать:

Студент должен знать:

- Математические принципы, лежащие в основе асимметричных криптографических алгоритмов.
- Существующие атаки на асимметричные криптосистемы.
- Значения параметров криптосистемы RSA, приводящие к возможности проведения криптоаналитической атаки.

2. должен уметь:

Студент должен уметь:

- Проводить анализ стойкости криптографического алгоритма RSA при заданных параметрах.
- Идентифицировать причины снижения криптостойкости RSA.

3. должен владеть:

Студент должен владеть:

- Криптографической терминологией.

Студент должен демонстрировать способность и готовность:

- Анализировать стойкость асимметричной криптосистемы RSA.
- Вырабатывать рекомендации по повышению стойкости криптосистемы RSA.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 6 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);
54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Математические основы асимметричной криптографии.	6		0	3	5	письменное домашнее задание
2.	Тема 2. Криптосистема RSA.	6		0	2	4	письменное домашнее задание
3.	Тема 3. Криптоаналитические атаки на алгоритм RSA.	6		0	3	5	письменное домашнее задание
4.	Тема 4. Решетки.	6		0	3	5	письменное домашнее задание
5.	Тема 5. Криптоанализ RSA с использованием решеток.	6		0	3	5	письменное домашнее задание
6.	Тема 6. Тесты на простоту.	6		0	2	6	письменное домашнее задание
7.	Тема 7. Методы факторизации.	6		0	2	6	письменное домашнее задание
.	Тема . Итоговая форма контроля	6		0	0	0	экзамен
	Итого			0	18	36	

4.2 Содержание дисциплины

Тема 1. Математические основы асимметричной криптографии.

практическое занятие (3 часа(ов)):

Расширенный алгоритм Евклида. Китайская теорема об остатках. Кольца и группы. Кольцо вычетов по модулю. Существование обратного элемента по умножению по модулю. Функция Эйлера. Мультипликативная группа кольца вычетов по модулю n. Теорема Эйлера. Малая теорема Ферма. Алгоритм быстрого возведения в степень.

лабораторная работа (5 часа(ов)):

Программная реализация расширенного алгоритма Евклида.

Тема 2. Криптосистема RSA.

практическое занятие (2 часа(ов)):

Алгоритм RSA. Генерирование модуля RSA, выбор шифрующей экспоненты, вычисление расшифровывающей экспоненты. Реализация шифрования и расшифрования RSA.

лабораторная работа (4 часа(ов)):

Программная реализация эффективного алгоритма расшифрования RSA.

Тема 3. Криптоаналитические атаки на алгоритм RSA.

практическое занятие (3 часа(ов)):

Элементарные атаки: разделенный модуль, малая шифрующая экспонента. Атака Винера. Частичное раскрытие ключа при использовании малой шифрующей экспоненты. Условия успешного проведения атаки Боне-Дерфи. Границы Вегера.

лабораторная работа (5 часа(ов)):

Реализация частичного раскрытия секретного ключа при использовании малой шифрующей экспоненты.

Тема 4. Решетки.

практическое занятие (3 часа(ов)):

Решетки. Базис решетки. Получение другой матрицы базиса. Ортогонализация Грама-Шмидта. LLL-приведенный базис решетки и его свойства. Алгоритм построения LLL-приведенного базиса решетки и его свойства.

лабораторная работа (5 часа(ов)):

Реализация метода ортогонализации Грама-Шмидта.

Тема 5. Криптоанализ RSA с использованием решеток.

практическое занятие (3 часа(ов)):

Теорема Копперсмита. Атака на RSA: известна половина старших битов p или q. Формулировка теоремы Копперсмита для двух переменных. Атака на RSA: известна половина младших битов p или q.

лабораторная работа (5 часа(ов)):

Реализация атаки на RSA: известна половина старших битов p или q.

Тема 6. Тесты на простоту.

практическое занятие (2 часа(ов)):

Тест Ферма. Тест Миллера-Рабина.

лабораторная работа (6 часа(ов)):

Реализация теста Ферма.

Тема 7. Методы факторизации.

практическое занятие (2 часа(ов)):

Метод факторизации Ферма. (p–1)-метод Полларда. ρ-метод Полларда.

лабораторная работа (6 часа(ов)):

Реализация ρ-метода Полларда.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Математические основы асимметричной криптографии.	6		подготовка домашнего задания	4	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Криптосистема RSA.	6		подготовка домашнего задания	3	домашнее задание
3.	Тема 3. Криптоаналитические атаки на алгоритм RSA.	6		подготовка домашнего задания	4	домашнее задание
4.	Тема 4. Решетки.	6		подготовка домашнего задания	4	домашнее задание
5.	Тема 5. Криптоанализ RSA с использованием решеток.	6		подготовка домашнего задания	4	домашнее задание
6.	Тема 6. Тесты на простоту.	6		подготовка домашнего задания	4	домашнее задание
7.	Тема 7. Методы факторизации.	6		подготовка домашнего задания	4	домашнее задание
	Итого				27	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лабораторных занятий, а также самостоятельной работы студентов.

Изучение курса подразумевает овладение теоретическим материалом и получение практических навыков для более глубокого понимания разделов дисциплины "Криптоанализ асимметричных шифров" на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Математические основы асимметричной криптографии.

домашнее задание , примерные вопросы:

Программная реализация алгоритма быстрого возведения в степень по модулю.

Тема 2. Криптосистема RSA.

домашнее задание , примерные вопросы:

Программная реализация алгоритма RSA.

Тема 3. Криптоаналитические атаки на алгоритм RSA.

домашнее задание , примерные вопросы:

Программная реализация атаки Винера.

Тема 4. Решетки.

домашнее задание , примерные вопросы:

Программная реализация алгоритма нахождения LLL-приведенного базиса решетки.

Тема 5. Криптоанализ RSA с использованием решеток.

домашнее задание , примерные вопросы:

Программная реализация алгоритма нахождения малых корней полинома по модулю.

Тема 6. Тесты на простоту.

домашнее задание , примерные вопросы:

Программная реализация теста Миллера-Рабина.

Тема 7. Методы факторизации.

домашнее задание , примерные вопросы:

Программная реализация метода факторизации Ферма.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Контрольная работа 1:

Программная реализация схема Optimal Asymmetric Encryption Padding.

Контрольная работа 2:

Реализация (p-1)-метода факторизации Полларда.

Вопросы к зачету:

1. Кольцо, определение.
2. Группа, определение.
3. Кольцо вычетов.
4. Мультипликативная группа.
5. Алгоритм Евклида с доказательством.
6. Функция Эйлера.
7. Теорема Эйлера с доказательством.
8. Китайская теорема об остатках.
9. Алгоритм шифрования RSA.
10. Алгоритм расшифрования RSA.
11. Эффективная реализация расшифрования RSA.
12. Атака на RSA: разделенный модуль.
13. Атака на RSA: малая шифрующая экспонента.
14. Атака на RSA: метод факторизации Ферма.
15. Решетки.
16. LLL-приведенный базис решетки.
17. Свойства LLL-приведенного базиса решетки.
18. Алгоритм нахождения LLL-приведенного базиса решетки.
19. Теорема Копперсмита.

20. Атаки на RSA с использованием решеток.

Типовой билет:

1. Китайская теорема об остатках.
2. Алгоритм нахождения LLL-приведенного базиса решетки.

7.1. Основная литература:

1. Громкович, Ю. Теоретическая информатика: Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию / Юрай Громкович; Пер. с нем.; Под ред. Б. Ф. Мельникова.?Издание 3-е.?Санкт-Петербург: БХВ-Петербург, 2010.?336 с.

2. Латыпов Р.Х., Разинков Е.В. Электронный образовательный ресурс "Теория кодирования информации и криптография", 2015. - URL: http://tulpar.kfu.ru/enrol/index.php?id=2422

3. Червяков Н.И., Евдокимов А.А., Галушкин А.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - - М.: Физматлит, 2012. - 280 с. URL: http://e.lanbook.com/books/element.php?pl1_id=5300

4. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. URL: http://znanium.com/bookread.php?book=441493

5. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: http://znanium.com/bookread.php?book=420047

7.2. Дополнительная литература:

1. Маскаева А. М. Основы теории информации: Учебное пособие / А.М. Маскаева. - М.: Форум:

НИЦ ИНФРА-М, 2014. - 96 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=429571

2. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=474838

3. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=503511

7.3. Интернет-ресурсы:

Материалы онлайн-курсов Массачусетского Технологического Института - http://ocw.mit.edu/index.htm

Онлайн-курсы лучших университетов мира - https://www.coursera.org

Онлайн-курсы лучших университетов мира - https://www.edx.org

Онлайн-курсы лучших университетов мира - https://www.udacity.com

Онлайн-курсы Стенфордского Университета - http://online.stanford.edu

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Криптоанализ асимметричных шифров" предполагает использование следующего материально-технического обеспечения:

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Практические занятия по дисциплине проводятся в компьютерных классах.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 02.03.02 "Фундаментальная информатика и информационные технологии" и профилю подготовки Системный анализ и информационные технологии .

Автор(ы):
Разинков Е.В. _____
"__" _____ 201 __ г.

Рецензент(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.