

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.

*подписано электронно-цифровой подписью*

**Программа дисциплины**  
Основы криптоанализа Б1.В.ДВ.9

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

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 98218

Казань  
2018

## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

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 основы 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.9 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к дисциплинам по выбору. Осваивается на 4 курсе, 7 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 4 курсе в 7 семестре для студентов обучающихся по направлению "Информационная безопасность".

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
ОПК-2 (профессиональные компетенции)	способностью применять соответствующий математический аппарат для решения профессиональных задач
ОПК-4 (профессиональные компетенции)	способностью понимать сущность и значение информации в развитии современного общества, решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий
ОПК-7 (профессиональные компетенции)	способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности объекта защиты
ПК-1 (профессиональные компетенции)	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных, криптографических и технических средств защиты информации
ПК-10 (профессиональные компетенции)	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности
ПК-12 (профессиональные компетенции)	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-3 (профессиональные компетенции)	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-7 (профессиональные компетенции)	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных, криптографических и технических средств защиты информации
ПК-9 (профессиональные компетенции)	способностью участвовать в разработке подсистемы управления информационной безопасностью

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.

4. должен демонстрировать способность и готовность:

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 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 7 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.	7		5	0	2	Письменное домашнее задание
2.	Тема 2. Криптосистема RSA.	7		4	0	2	Письменное домашнее задание
3.	Тема 3. Криптоаналитические атаки на алгоритм RSA.	7		5	0	2	Письменное домашнее задание
4.	Тема 4. Решетки.	7		5	0	2	Письменное домашнее задание
5.	Тема 5. Криптоанализ RSA с использованием решеток.	7		5	0	2	Контрольная работа Письменное домашнее задание
6.	Тема 6. Тесты на простоту.	7		6	0	4	Письменное домашнее задание
7.	Тема 7. Методы факторизации.	7		6	0	4	Контрольная работа Письменное домашнее задание
	Тема . Итоговая форма контроля	7		0	0	0	Экзамен
	Итого			36	0	18	

#### 4.2 Содержание дисциплины

##### Тема 1. Математические основы асимметричной криптографии.

###### *лекционное занятие (5 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 (2 часа(ов)):*

Программная реализация расширенного алгоритма Евклида.

##### Тема 2. Криптосистема RSA.

**лекционное занятие (4 часа(ов)):**

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

**лабораторная работа (2 часа(ов)):**

Программная реализация эффективного алгоритма расшифрования RSA.

**Тема 3. Криптоаналитические атаки на алгоритм RSA.**

**лекционное занятие (5 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 (2 часа(ов)):**

Реализация частичного раскрытия секретного ключа при использовании малой шифрующей экспоненты.

**Тема 4. Решетки.**

**лекционное занятие (5 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 (2 часа(ов)):**

Реализация метода ортогонализации Грама-Шмидта.

**Тема 5. Криптоанализ RSA с использованием решеток.**

**лекционное занятие (5 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 (2 часа(ов)):**

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

**Тема 6. Тесты на простоту.**

**лекционное занятие (6 часа(ов)):**

Тест Ферма. Тест Миллера-Рабина.

**лабораторная работа (4 часа(ов)):**

Реализация теста Ферма.

**Тема 7. Методы факторизации.**

**лекционное занятие (6 часа(ов)):**

Метод факторизации Ферма.  $(p-1)$ -метод Полларда.  $p$ -метод Полларда.

**лабораторная работа (4 часа(ов)):**

Реализация  $p$ -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.	7		подготовка домашнего задания	6	Письменное домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Криптосистема RSA.	7		подготовка домашнего задания	6	Письменное домашнее задание
3.	Тема 3. Криптоаналитические атаки на алгоритм RSA.	7		подготовка домашнего задания	6	Письменное домашнее задание
4.	Тема 4. Решетки.	7		подготовка домашнего задания	6	Письменное домашнее задание
5.	Тема 5. Криптоанализ RSA с использованием решеток.	7		подготовка домашнего задания	8	Письменное домашнее задание
				подготовка к контрольной работе	4	Контрольная работа
6.	Тема 6. Тесты на простоту.	7		подготовка домашнего задания	6	Письменное домашнее задание
7.	Тема 7. Методы факторизации.	7		подготовка домашнего задания	8	Письменное домашнее задание
				подготовка к контрольной работе	4	Контрольная работа
	Итого				54	

## 5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекций и 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.

Письменное домашнее задание , примерные вопросы:

Программная реализация алгоритма быстрого возведения в степень по модулю.

## **Тема 2. Криптосистема RSA.**

Письменное домашнее задание , примерные вопросы:

Программная реализация алгоритма RSA.

## **Тема 3. Криптоаналитические атаки на алгоритм RSA.**

Письменное домашнее задание , примерные вопросы:

Программная реализация атаки Винера.

## **Тема 4. Решетки.**

Письменное домашнее задание , примерные вопросы:

Программная реализация алгоритма нахождения LLL-приведенного базиса решетки.

## **Тема 5. Криптоанализ RSA с использованием решеток.**

Контрольная работа , примерные вопросы:

Программная реализация схема Optimal Asymmetric Encryption Padding.

Письменное домашнее задание , примерные вопросы:

Программная реализация алгоритма нахождения малых корней полинома по модулю

## **Тема 6. Тесты на простоту.**

Письменное домашнее задание , примерные вопросы:

Программная реализация теста Миллера-Рабина.

## **Тема 7. Методы факторизации.**

Контрольная работа , примерные вопросы:

Реализация  $(p-1)$ -метода факторизации Полларда.

Письменное домашнее задание , примерные вопросы:

Программная реализация метода факторизации Ферма

## **Тема . Итоговая форма контроля**

Примерные вопросы к экзамену:

Вопросы к экзамену:

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. 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>
2. 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>
3. Чечёта, С.И. Введение в дискретную теорию информации и кодирования [Электронный ресурс] : учеб. пособие - Электрон. дан. - Москва : МЦНМО, 2011. - 224 с. - Режим доступа: <https://e.lanbook.com/book/9437>
4. Кельберт, М.Я. Вероятность и статистика в примерах и задачах. Т.3: Теория информации и кодирования [Электронный ресурс] / М.Я. Кельберт, Ю.М. Сухов. - Электрон. дан. - Москва : МЦНМО, 2016. - 567 с. - Режим доступа: <https://e.lanbook.com/book/80125>.
5. Штарьков, Ю.М. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс] Электрон. дан. - М. : Физматлит, 2013. - 280 с. - Режим доступа: [http://e.lanbook.com/books/element.php?pl1\\_id=59667](http://e.lanbook.com/books/element.php?pl1_id=59667)

### 7.2. Дополнительная литература:

1. Сидельников, В. М. Теория кодирования [Электронный ресурс] / В. М. Сидельников. - М.: ФИЗМАТЛИТ, 2008. - 324 с. URL:<http://znanium.com/bookread2.php?book=544713>
2. Масленников М. Е. Практическая криптография: Пособие / Масленников М.Е. СПб:БХВ-Петербург, 2015. - 465 с. URL: <http://znanium.com/bookread2.php?book=944503>
3. 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>
4. 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 "Основы криптоанализа" 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 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность компьютерных систем .

Автор(ы):

Разинков Е.В. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.

Рецензент(ы):

Ишмухаметов Ш.Т. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.