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

Программирование криптографических алгоритмов Б1.В.ДВ.5

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

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

**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
2017

## Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Shamil.Ishmukhametov@kpfu.ru

## 1. Цели освоения дисциплины

Данный курс входит в систему специализации по направлению информационной безопасности и является продолжением курсов "Основы информационной безопасности". В ходе этого курса студенты должны получить основные знания о математических основах построения криптографических алгоритмов, понятия о вычислительной сложности односторонних функций, используемых в криптографии, методах построения надежных систем защиты и о возможных атаках.

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

Данная учебная дисциплина включена в раздел " Б1.В.ДВ.5 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к дисциплинам по выбору. Осваивается на 3 курсе, 6 семестр.

"Программирование криптографических алгоритмов" входит в состав профессиональных дисциплин. Читается на 4 курсе в 7 семестре.

## 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) | способность применять соответствующий математический аппарат для решения профессиональных задач |
| ОПК-4 (профессиональные компетенции) | способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации |
| ОПК-7 (профессиональные компетенции) | способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты |
| ПК-1 (профессиональные компетенции) | способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации |
| ПК-10 (профессиональные компетенции) | способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности |
| ПК-11 (профессиональные компетенции) | способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов |

В результате освоения дисциплины студент:

4. должен демонстрировать способность и готовность:

работать с использованием знаний по основным разделам информационной безопасности и криптографии

## 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 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. Введение в теорию сложности алгоритмов. Получение верхних оценок сложности. | 6 | | 2 | 0 | 2 | Письменное домашнее задание |
| 2. | Тема 2. Потоковые и блочные шифры. Криптографические примитивы: подстановки, перестановки, гаммирование. Метод DES. | 6 | | 2 | 0 | 6 | Письменное домашнее задание |
| 3. | Тема 3. Методы шифрования с двумя ключами. Метод RSA. | 6 | | 2 | 0 | 6 | Контрольная работа Письменное домашнее задание |
| 4. | Тема 4. Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля. | 6 | | 2 | 0 | 6 | Письменное домашнее задание |
| 5. | Тема 5. Контрольная работа по RSA. | 6 | | 0 | 0 | 2 | Контрольная работа |

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические занятия | Лабораторные работы | |
| 6. | Тема 6. Вычисления в конечных полях. Задача вычисления дискретного логарифма. Метод Шенкса. Оценки сложности для задачи дискретного логарифмирования. | 6 | | 2 | 0 | 6 | Письменное домашнее задание |
| 7. | Тема 7. Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами. Контрольная работа по теме. | 6 | | 2 | 0 | 10 | Контрольная работа Письменное домашнее задание |
| 8. | Тема 8. Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера. | 6 | | 2 | 0 | 8 | Письменное домашнее задание |
| 9. | Тема 9. Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита. | 6 | | 4 | 0 | 8 | Письменное домашнее задание |
| . | Тема . Итоговая форма контроля | 6 | | 0 | 0 | 0 | Экзамен |
| | Итого | | | 18 | 0 | 54 | |

**4.2 Содержание дисциплины**

**Тема 1. Введение в теорию сложности алгоритмов. Получение верхних оценок сложности.**

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

Основные понятия теории сложности алгоритмов. Верхние и нижние оценки. Классы сложности алгоритмов. Полиномиальные и экспоненциальные алгоритмы.

***лабораторная работа (2 часа(ов)):***

Реализация и оценка эффективности алгоритмов подстановки и перестановки в криптографии.

**Тема 2. Потоковые и блочные шифры. Криптографические примитивы: подстановки, перестановки, гаммирование. Метод DES.**

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

Потоковые и блочные шифры. Криптографические примитивы: подстановки, перестановки, гаммирование. Метод DES

***лабораторная работа (6 часа(ов)):***

Реализация и оценка эффективности алгоритмов подстановки и перестановки в криптографии. Оценки криптостойкости алгоритмов подстановки и перестановок.

**Тема 3. Методы шифрования с двумя ключами. Метод RSA.**

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

Методы шифрования с двумя ключами. Метод RSA.

***лабораторная работа (6 часа(ов)):***

Программирование RSA. Разработка процедур для теста простоты Миллера-Рабина и расширенного алгоритма Евклида.

**Тема 4. Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля.**

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

Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля. Шифрование и создание электронной подписи на основе метода Эль-Гамаля.

***лабораторная работа (6 часа(ов)):***

Программирование метода Эль-Гамаля. Методы вычисления дискретного логарифма.

**Тема 5. Контрольная работа по RSA.**

***лабораторная работа (2 часа(ов)):***

Контрольная работа по RSA.

**Тема 6. Вычисления в конечных полях. Задача вычисления дискретного логарифма. Метод Шенкса. Оценки сложности для задачи дискретного логарифмирования.**

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

Вычисления в конечных полях. Задача вычисления дискретного логарифма. Метод Шенкса. Оценки сложности для задачи дискретного логарифмирования.

***лабораторная работа (6 часа(ов)):***

Реализация метод Шенкса и оценка сложности для задачи дискретного логарифмирования.

**Тема 7. Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами. Контрольная работа по теме.**

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

Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами.

***лабораторная работа (10 часа(ов)):***

Программирование процедур работы с точками эллиптической кривой. Проективные координаты. Шифрование на ЭК.

**Тема 8. Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера.**

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

Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера.

***лабораторная работа (8 часа(ов)):***

Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера.

**Тема 9. Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита.**

***лекционное занятие (4 часа(ов)):***

Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита.

***лабораторная работа (8 часа(ов)):***

Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита.

## 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. Введение в теорию сложности алгоритмов. Получение верхних оценок сложности. | 6 | | Изучение конспекта лекций | 2 | Домашнее задание |
| 2. | Тема 2. Потоковые и блочные шифры. Криптографические примитивы: подстановки, перестановки, гаммирование. Метод DES. | 6 | | Программирование потоковых и блочных шифров. | 2 | домашнее задание |
| 3. | Тема 3. Методы шифрования с двумя ключами. Метод RSA. | 6 | | Изучение RSA | 1 | Проверка домашнего задания |
| | | | | подготовка к контрольной работе | 1 | контрольная работа |
| 4. | Тема 4. Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля. | 6 | | Изучение метода Эль-Гамаля. | 2 | домашнее задание |
| 5. | Тема 5. Контрольная работа по RSA. | 6 | | Подготовка к контрольной работе | 2 | домашнее задание |
| 6. | Тема 6. Вычисления в конечных полях. Задача вычисления дискретного логарифма. Метод Шенкса. Оценки сложности для задачи дискретного логарифмирования. | 6 | | Реализация метода Шенкса | 2 | Проверка домашнего задания |
| 7. | Тема 7. Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами. Контрольная работа по теме. | 6 | | подготовка к контрольной работе | 1 | контрольная работа |
| | | | | Реализация вычислений на эллиптических кривых | 1 | домашнее задание |

| N | Раздел Дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной работы |
|---|---|---|---|---|---|---|
| 8. | Тема 8. Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера. | 6 | | Изучение теоретического материала. | 2 | домашнее задание |
| 9. | Тема 9. Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита. | 6 | | Разработка клиент-серверного приложения | 2 | Сдача проекта |
| | Итого | | | | 18 | |

## 5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекций, лабораторных занятий и самостоятельной работы студентов.

Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать 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.

Чтение лекций предполагает использование электронных презентаций и электронного учебника.

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

**Тема 1. Введение в теорию сложности алгоритмов. Получение верхних оценок сложности.**

Домашнее задание , примерные вопросы:

Выполнить оценку сложности алгоритмов умножения и деления целых чисел, поиска элемента в масиве, сортировки массива.

**Тема 2. Потоковые и блочные шифры. Криптографические примитивы: подстановки, перестановки, гаммирование. Метод DES.**

домашнее задание , примерные вопросы:

Выполнить разбор методов подстановки, перестановки и гаммирования. Оценить их криптостойкость.

**Тема 3. Методы шифрования с двумя ключами. Метод RSA.**

контрольная работа , примерные вопросы:

Изучить алгоритмы, входящие в RSA. Подготовка к контрольной работе.

Проверка домашнего задания , примерные вопросы:

Изучить алгоритмы, входящие в RSA. Выполнить генерацию параметров метода, шифрование и расшифрование тестового текста. Изучить алгоритм Миллера-Рабина проверки простоты.

**Тема 4. Электронная подпись. Алгоритмы построения ЭЦП. Метод Эль-Гамаля.**

домашнее задание , примерные вопросы:

Изучить алгоритм Эль-Гамаля, решение задач на построение электронной подписи по методу Эль-Гамаля.

**Тема 5. Контрольная работа по RSA.**

домашнее задание , примерные вопросы:

Подготовка к контрольной работе.

**Тема 6. Вычисления в конечных полях. Задача вычисления дискретного логарифма. Метод Шенкса. Оценки сложности для задачи дискретного логарифмирования.**

Проверка домашнего задания , примерные вопросы:

Решение задач на выполнение операций в конечных полях. Рассмотреть конечные расширения полей, полученных добавлением кореней неприводимых многочленов.

**Тема 7. Эллиптические кривые. Вычисления сумм точек эллиптической кривой в конечном поле. Работа с проективными координатами. Контрольная работа по теме.**

домашнее задание , примерные вопросы:

Изучить теоретический материал и выполнить решение задач на вычисление координат суммы точек и кратного точек для эллиптических кривых.

контрольная работа , примерные вопросы:

Изучить операции с точками эллиптических кривых. Оценить число точек на кривой. Подготовка к контрольной работе.

**Тема 8. Преобразование Вейля-Тейта. MOV-атака. Реализация функции Миллера.**

домашнее задание , примерные вопросы:

Изучить теоретический материал, решение задач на построение функции Миллера и построение преобразования Вейля-Тейта.

**Тема 9. Разработка клиент-серверного приложения с решениями задач аутентификации, авторизации и аудита.**

Сдача проекта , примерные вопросы:

Подготовка и сдача проекта. Ответы на контрольные вопросы.

**Тема . Итоговая форма контроля**

Примерные вопросы к экзамену:

Вопросы к экзамену:

1. Основные принципы организации и задачи сетевой безопасности
2. Описание модели OSI межсетевых взаимодействий.
3. Общая характеристика TCP/IP
4. Протоколы IPv4.
5. Односторонние функции. Хеш-функции. Алгоритм HMAC
6. Метод RC4.
7. Метод RSA.
8 Алгоритм шифрования Эль-Гамаля.
9. Метод выработки секретного ключа Диффи-Хелмана.
10 Электронно-цифровая подпись. Ее свойства и правовые основы. Алгоритм создание ЭЦП.
11 Эллиптические кривые. Операции сложения и удвоения на множестве точек ЭК.
12 Криптографические протоколы на эллиптических кривых.
13 Разработка клиент-серверных приложений в C++.
14 Стандарт сертификации X.509. Состав сертификата.
15 Организация защиты данных в сетях. Протокол IPsec.

11. Защита Web. Архитектура SSL. Протокол квитирования SSL.
12. Протокол SET. Сравнительные характеристики протоколов SSL и SET.
13. Организация сетей GSM .
14. Защита сетей GSM.
15. Алгоритм проверки простоты целых чисел Ферма.
16. Алгоритм проверки простоты целых чисел Рабина-Миллера.
17. Методы факторизации целых чисел. Ро-метод Полларда.
18. Методы факторизации целых чисел. (p-1)-метод Полларда.
19. Факторизация на основе эллиптических кривых.
20. Метод факторизации квадратичного решета.

Приложение 2.

Вариант контрольной работы 1.

Вычисления в конечных полях и кольцах.

1. Решить уравнение 2-й степени в конечном поле.
2. Вычислить символ Лежандра для заданного элемента в кольце вычетов.
3. Решить реккурентное уравнение с использованием производящих функций.

Вариант контрольной работы 2. Шифрование с использованием криптографических методов.

1. Проверить число n=57 на простоту, используя одну итерацию теста Миллера-Рабина с базой a=2.
2. Используя заданные значения p, q и e, вычислить остальные параметры RSA и расшифровать число m. Для вычисления d использовать расширенный

алгоритм Евклида: p=17, q=29, e=239, m=24.

3. Выполнить шифрование текста на основе методов перестановки, подстановок и гаммирования.

### 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. Электронный образовательный ресурс "Кодирование информации и криптография - Математические основы", 2012 http://zilant.kpfu.ru/course/view.php?id=3

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. Мальцев, Ю. Н. Элементы дискретной математики: элементы комбинаторики, теории графов теории кодирования и криптографии / Ю.Н. Мальцев, Е.П. Петров; М-во образования и науки РФ, Алт. гос. ун-т.?Барнаул: Изд-во Алт. гос. ун-та, 2004.?174 с

2. Латыпов, Р. Х. Математические основы кодирования информации и криптографии: учеб. пособие / Р. Х. Латыпов; Казан. гос. ун-т.?Казань: [КГУ], 2005.?59 с

3. Земор, Жиль. Курс криптографии / Жиль Земор; пер. с фр. В.В. Шуликовской.?Москва; Ижевск: Ин-т компьютер. исслед.: Регуляр. и хаотич. динамика, 2006.?255 с.

### 7.3. Интернет-ресурсы:

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет--портал ресурсов по математическим наукам - http://www.math.ru/

Интернет--портал ресурсов по математическим наукам - http://www.mathnet.ru

Интернет--портал ресурсов по математическим наукам - http://www.allmath.com/

Интернет--портал ресурсов по программированию - http://algolist.manual.ru/

### 8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Программирование криптографических алгоритмов" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

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.

Локальная сеть

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):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

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