МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт математики и механики им. Н.И. Лобачевского

**УТВЕРЖДАЮ**
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.
_____
"___"_____20___ г.

# Программа дисциплины

Криптография М1.ДВ.2

Направление подготовки: 010100.68 - Математика
Профиль подготовки: Алгебра
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

**Автор(ы):**
Тронин С.Н.
**Рецензент(ы):**
Киндер М.И.

**СОГЛАСОВАНО:**
Заведующий(ая) кафедрой:
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института математики и механики им. Н.И. Лобачевского :
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань
2013

## Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Тронин С.Н. Кафедра алгебры и математической логики отделение математики , Serge.Tronin@kpfu.ru

## 1. Цели освоения дисциплины

Необходимость в защите разнообразной информации возникает в современной жизни буквально на каждом шагу. В основе многих способов такой защиты лежат идеи и методы науки криптографии (или криптологии). Эта наука, крупнейшие достижения которой можно датировать серединой 20-го века, и особенно периодом после 1976 года, широко использует математические методы, в частности, методы современной теории чисел, алгебраической геометрии, теории сложности и т.д. Конечная цель курса? познакомить слушателей с самыми основами современной криптографии, и помочь им овладеть основными понятиями и принципами, лежащими в основе методов этой науки (не вдаваясь в излишние технические детали). Предполагается, что часть материала будет изучена слушателями самостоятельно, и по результатам этого изучения должны быть составлены подробные рефераты (или отчеты о проделанной работе).

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

Данная учебная дисциплина включена в раздел " М1.ДВ.2 Общенаучный" основной образовательной программы 010100.68 Математика и относится к дисциплинам по выбору. Осваивается на 2 курсе, 3 семестр.

Данный курс предназначен для слушателей, которые имеют базовое математическое образование, в том числе прослушали курсы по элементарной теории чисел и вводный курс алгебры.

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

В результате освоения дисциплины формируются следующие компетенции:

В результате освоения дисциплины студент:

1. должен знать:

основные идеи современной криптографии, прежде всего ? криптографии с открытым ключом, некоторые основные алгоритмы шифрования и генерации цифровых (электронных) подписей, а также некоторые важные криптографические протоколы.

2. должен уметь:

применять полученные знания в конкретных ситуациях.

3. должен владеть:

вычислительными навыками, необходимыми при решении простейших криптографических задач.

## 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 3 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. История криптографии. Исторические шифры. | 3 | 1-2 | 0 | 0 | 0 | |
| 2. | Тема 2. Блочные и потоковые шифры. Режимы шифрования. | 3 | 3-4 | 0 | 0 | 0 | |
| 3. | Тема 3. Математический аппарат: кольца вычетов и конечные поля. | 3 | 5-7 | 0 | 0 | 0 | |
| 4. | Тема 4. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана и идея цифровой подписи. Дискретный логарифм. | 3 | 8-9 | 0 | 0 | 0 | |
| 5. | Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи. | 3 | 10-12 | 0 | 0 | 0 | |
| 6. | Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги. | 3 | 13-14 | 0 | 0 | 0 | |
| 7. | Тема 7. Криптографические протоколы. | 3 | 15-16 | 0 | 0 | 0 | |
| 8. | Тема 8. Эллиптическая криптография | 3 | 17-18 | 0 | 0 | 0 | |
| . | Тема . Итоговая форма контроля | 3 | | 0 | 0 | 0 | зачет |
| | Итого | | | 0 | 0 | 0 | |

### 4.2 Содержание дисциплины

**Тема 1. История криптографии. Исторические шифры.**

**Тема 2. Блочные и потоковые шифры. Режимы шифрования.**

**Тема 3. Математический аппарат: кольца вычетов и конечные поля.**

**Тема 4. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана и идея цифровой подписи. Дискретный логарифм.**

**Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи.**

**Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги.**

**Тема 7. Криптографические протоколы.**

**Тема 8. Эллиптическая криптография**

## 5. Образовательные технологии, включая интерактивные формы обучения

Лекции, семинары, доклады на семинарах, рефераты, зачет. Самостоятельная работа с литературой, решение задач в процессе подготовки к докладам.

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

**Тема 1. История криптографии. Исторические шифры.**

**Тема 2. Блочные и потоковые шифры. Режимы шифрования.**

**Тема 3. Математический аппарат: кольца вычетов и конечные поля.**

**Тема 4. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана и идея цифровой подписи. Дискретный логарифм.**

**Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи.**

**Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги.**

**Тема 7. Криптографические протоколы.**

**Тема 8. Эллиптическая криптография**

**Тема . Итоговая форма контроля**

Примерные вопросы к зачету:

На практических занятиях контроль осуществляется при устном опросе и по результатам доклада на семинаре. Оцениваются ткже рефераты (отчеты о самостоятельной работе). Используется балльная система.

## 7.1. Основная литература:

1. Введение в криптографию / Под общ. ред. В.В.Ященко. - 3-е изд., доп. М.:МЦНМО:"ЧеРо", 2000. - 288 с.

2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. - М.: Научный мир, 2004. - 173 с.

3. Смарт Н. Криптография. - М.: Техносфера, 2006. - 528 с.

4. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. - М.:Издат. центр "Академия", 2009. - 272 с.

5. Чмора А.Л. Современная прикладная криптография. - М.: Гелиос, 2001. - 256 с.

## 7.2. Дополнительная литература:

1. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. - М.:"Мир", 1987. - 416 с.

2. Бабаш А.В., Шанкин Г.П. Криптография. - М.:СОЛОН-ПРЕСС, 2007. - 512 с.

3. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. - М.: КомКнига, 2006. - 328 с.

4. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. - М.: КомКнига, 2006. - 328 с.

5. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.: МНЦМО: 2003. - 328 с.

6. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. - М.:"Мир", 1982. - 416 с.

7. Земор Ж. Курс криптографии. - М. - Ижевск: НИЦ "Регулярная и хаотическая динамика"; Ин-т компьютерных исследований, 2006. - 256 с.

8. Коблиц Н. Курс теории чисел и криптографии. - М: Научн. изд-во ТВП, 2001. - 254 с.

9. Лидл Р., Нидеррайтер Г. Конечные поля. Т.1, 2. - М.: Мир, 1988.

10. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. - СПб., БХВ-Петербург, 2005. - 288 с.

11. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. - СПб., БХВ-Петербург, 2007. - 304 с.

12. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. - СПб.: БХВ-Петербург, 2009. - 576 с.

13. Сингх С. Книга шифров: тайная история шифров и их расшифровки. - М.: АСТ: Астрель, 2007. - 447 с.

14. Черчхаус Р. Коды и шифры. Юлий Цезарь, "Энигма" и Интернет. - М.: Изд-во "Весь Мир", 2005. - 320 с.

### 7.3. Интернет-ресурсы:

## 8. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Освоение дисциплины "Криптография" предполагает использование следующего материально-технического обеспечения:

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010100.68 "Математика" и магистерской программе Алгебра .

Автор(ы):
Тронин С.Н. _____
"__" _____ 201 __ г.

Рецензент(ы):
Киндер М.И. _____
"__" _____ 201 __ г.