МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственное образовательное учреждение

высшего профессионального образования

«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Механико-математический факультет

Кафедра алгебры и геометрии

УТВЕРЖДАЮ

Проректор по учебной работе

_____В.П.Гарькин

«_____»_____2011 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Теоретико-числовые методы в криптографии

(блок «Общие математические и естественнонаучные дисциплины»; раздел «Федеральный компонент»; основная образовательная программа специальности 090102 Компьютерная безопасность)

Самара
2011

Рабочая программа составлена на основании Государственного образовательного стандарта высшего профессионального образования специальности 090102 Компьютерная безопасность, утвержденного 05.04.2000г.(номер государственной регистрации 283 ИНФ/СП) и типовой (примерной) программы дисциплины «Теоретико-числовые методы в криптографии»,одобренной Советом УМО по образованию в области информационной безопасности.

Составитель рабочей программы: канд. ф.-м. н., доцент Азовская Т.В.
Рецензенты: д. ф.-м. н., профессор Панов А.Н. **,** канд. ф.-м. н., доцент Воскресенская Г.В.

Рабочая программа утверждена на заседании кафедры алгебры и геометрии (протокол № 6 от «17» января 2011 г.)

Заведующий кафедрой
17 января 2011 г. _____ А.Н.Панов

СОГЛАСОВАНО

Декан
факультета
″____″ _____ 2011 г. _____ С.Я.Новиков

Начальник
методического отдела
″____″ _____ 2011 г. _____ Н.В.Соловова

ОДОБРЕНО
Председатель
методической
комиссии факультета
″____″ _____ 2011 г. _____ Е.Я.Горелова

1. **Цели и задачи дисциплины, ее место в учебном процессе, требования к уровню освоения содержания дисциплины.**

1.1. Цели и задачи изучения дисциплины

Цель дисциплины - формирование у студентов понимания основных методов теории чисел, которые используются в криптографических методах защиты информации и при построении криптографических протоколов.

Задачи дисциплины:

- обозначить классические вопросы криптографии и указать пути и способы их разрешения;
- научить пользоваться алгоритмами, предусмотренными курсом и основным теоретико-числовым методам криптографии.

1.2. Требования к уровню подготовки студента, завершившего изучение данной дисциплины

Студенты, завершившие изучение данной дисциплины, должны:

Иметь представление:

- о значении теории чисел в криптографии, ее роли в решении практических задач, а также о методологических вопросах криптографии.

Знать:

- основные понятия теории чисел.

Уметь:

- применять стандартные методы к решению типовых теоретико-числовых задач; пользоваться при решении таких задач расчетными формулами, таблицами, графиками.

1.3. Связь с предшествующими дисциплинами

Для усвоения курса по криптографии требуются знания классического курса теории чисел и теории конечных полей.

1.4. Связь с последующими дисциплинами

Приобретенные в ходе изучения дисциплины знания и практические навыки используются при дальнейшем изучении **общепрофессиональных** и специальных дисциплин, а также при выполнении курсовых и дипломных работ.

2. Содержание дисциплины

2.1. Объем дисциплины в виде учебной работы (в часах)

ОЧНАЯ ФОРМА ОБУЧЕНИЯ, 8-й семестр – зачет

Вид учебных занятий	Количество часов
	Семестр8
Всего часов аудиторных занятий	**52**
Лекции	**34**
Практические занятия (семинары)	**18**
Всего часов самостоятельной работы	**38**
Подготовка к практическим занятиям	**38**
Всего часов по дисциплине	**90**

2.2. Разделы дисциплины и виды занятий

№ п/п	Название раздела дисциплины	Количество часов		
		лекции	практические занятия	лабораторные занятия
1	Элементы алгебры и теории чисел	4	2	--
2	Оценки сложности арифметических опера	4	2	--
3	Тестирование чисел на простоту	4	2	--
4	Алгоритмы факторизации целых чисел	6	4	--
5	Алгоритмы дискретного логарифмировани	8	4	--
6	Криптографическая система RSA	4	2	--
7	Криптосистемы на эллиптических кривых	4	2	--
	Итого:	34	18	--

2.3. Лекционный курс

Раздел 1 . ***Элементы алгебры и теории чисел.***

Числовые сравнения и их свойства. Полная и приведенная система вычетов, свойства. Функция Эйлера, ее свойства. Теорема Эйлера, малая теорема Ферма. Сравнения первой степени: анализ, способы решения. Системы линейных сравнений. Китайская теорема об остатках, ее использование при упрощении вычислений. Теория сравнений второй степени, символ Лежандра, его свойства,

символ Якоби. Первообразные корни и индексы. Теорема Гаусса. Решение степенных сравнений. Критерий степенного вычета.

Кольцо классов вычетов по модулю m, обратимые элементы, делители нуля, мультипликативная группа кольца, ее строение. Интерпретация китайской теоремы об остатках с точки зрения колец классов вычетов.

Строение конечной абелевой группы. Порядок элемента, свойства порядка. Конечные поля, порядок поля, характеристика поля, строение мультипликативной группы конечного поля. Построение поля из p^m элементов.

Раздел 2. ***Оценки сложности арифметических операций.***

Свойства оценочных функций. Сложности арифметических операций с целыми числами; сравнение функций сложности умножения, деления с остатком, обращения, возведения в квадрат. Быстрый алгоритм умножения n-значных чисел, его оценка. Алгоритм возведения в степень, его оценка. Сложность алгоритма Евклида. Вычисления с многочленами.

Раздел 3. ***Тестирование чисел на простоту.***

Критерий Вильсона. Вероятностный тест на основе малой теоремы Ферма. Псевдопростые числа, их свойства. Числа Кармайкла, их свойства. Теорема Корселта- Кармайкла (критерий числа Кармайкла).

Числа Мерсенна и числа Ферма. Тесты на простоту для чисел специального вида.

Тест Соловея-Штрассена. Тест Рабина-Миллера.

Раздел 4. ***Алгоритмы факторизации целых чисел.***

Метод Полларда (ро-метод). Оценка сложности.

Факторизация Ферма с факторными базами. Оценка сложности.

Метод квадратичного решета.

Раздел 5. ***Алгоритмы дискретного логарифмирования.***

Задача дискретного логарифмирования. Постановка задачи дискретного логарифмирования в криптографии. Система Диффи-Хеллмана обмена ключами. Криптосистема Мэсси- Омуры. Криптосистема Эль- Гамаля.

Логарифмирование в простых полях. Алгоритм Адлемана. Алгоритм Полига-Хеллмана. Индексный алгоритм дискретного логарифмирования в полях Галуа.

Раздел 6. ***Криптографическая система RSA.***

Система шифрования RSA, проблема подписи.

Условия на выбор чисел p и q. Выбор параметров e и d .

Раздел 7. *Криптосистемы на эллиптических кривых.*

2.4.Практические (семинарские) занятия

№	№ разделы	Наименование лабораторных работ
1.	1.	Элементы алгебры и теории чисел
2.	2	Оценки сложности арифметических операций
3.	3.	Тестирование чисел на простоту
4.	4.	Метод Полларда (ро-метод).
5.	4.	Факторизация Ферма с факторными базами.
6.	5.	Алгоритм Адлемана
7.	5.	Алгоритм Полига- Хеллмана
8.	6.	Система шифрования RSA
9.	7.	Криптосистемы на эллиптических кривых

2.5.Лабораторный практикум

Курсом не предусмотрен.

3. Организация текущего и промежуточного контроля знаний

3.1.Контрольные работы

Курсом не предусмотрены.

3.2.Комплекты тестовых заданий

Курсом не предусмотрены.

3.3.Самостоятельная работа

3.3.1. Поддержка самостоятельной работы (сборники тестов, задач, упражнений и др.)

3.3.2. Тематика рефератов

- Написание рефератов по курсу не предусмотрено.

3.4.Курсовая работа, ее характеристика; примерная тематика

- Написание курсовых работ не предусмотрено.

Итоговый контроль проводится в виде экзамена. Экзаменационная оценка ставится на основании письменного и устного ответа по экзаменационному билету.

4. Технические средства обучения и контроля, использование ЭВМ

Нет.

5. Активные методы обучения (деловые игры, научные проекты)

Лекционным курсом не предусмотрены.

6. Материальное обеспечение дисциплины

Нет.

7. Литература

7.1.Основная

1. Виноградов И.М. Основы теории чисел. – Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика» 2003
2. Окунев Л.Я. Краткий курс теории чисел. М., 1956.
3. Коблиц Н. Курс теории чисел и криптографии. М.: ТВП, 2001.
4. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002.

7.2.Дополнительная

1. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М., 1987.
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.

7.3.Учебно-методические материалы по дисциплине

1. Задачи по теории чисел / для студентов 2 курса механико-математического факультета, издательство « Самарский университет» - 1996