Пичкур А.Б.

«ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ»

090301 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Квалификация (степень) выпускника

«**Специалист**»

Общая характеристика

1. Цели и задачи дисциплины
2. Место дисциплины в структуре образовательной программы
3. Объем дисциплины и виды учебной работы
4. Содержание разделов дисциплины
5. Требования к результатам освоения дисциплины
6. Литература

Цели и задачи дисциплины

Целью преподавания дисциплины "Теоретико-числовые методы в криптографии" является:

- изложение студентам основных понятий и методов теории чисел с ее приложениями в современной криптографии,
- ознакомление с методами оценки сложности применяемых на практике алгоритмов
- построение эффективных алгоритмов решения некоторых прикладных задач в области информационной безопасности.

Место дисциплины в структуре образовательной программы

Дисциплина «Теоретико-числовые методы в криптографии» относится к числу дисциплин *базовой части профессионального цикла*.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Математический анализ» – основы теории пределов, дифференциального и интегрального исчисления,

«Алгебра» – линейная алгебра, группы, кольца и поля.

Место дисциплины в структуре образовательной программы

«Теория вероятностей и математическая статистика» – классические вероятностные схемы и классические предельные теоремы, случайные величины и их числовые характеристики.

«Дискретная математика» - основы комбинаторики

Знания, полученные при изучении дисциплины "Теоретико-числовые методы в криптографии", используются при изучении дисциплин

«Криптографические методы защиты информации»,

«Криптографические протоколы».

Объем дисциплины и виды учебной работы

Всего часов	**144**
Семестр	**6**
Аудиторные занятия (всего)	**78**
Лекции 40	
Практические занятия	34
Контрольные работы	4
Самостоятельная работа (всего)	**30**
Вид итоговой аттестации (экзамен)	**36**

Содержание разделов дисциплины

Тема 1. Введение.

Тема 2. Арифметика колец вычетов

Тема 3. Цепные дроби

Тема 4. Простые числа

Тема 5. Методы разложения чисел на множители

Тема 6. Вычисления в кольцах многочленов

Тема 7. Методы дискретного логарифмирования.

Тема 8. Элементы криптографии на эллиптических кривых

Тема 1. Введение.

1.1. Место теории чисел среди других математических дисциплин. Краткая история развития теории чисел.

1.2. Приложения теории чисел в информационной безопасности. Литература по дисциплине

Тема 2. Арифметика колец вычетов

2.1. Вычисления в кольце целых чисел. Алгоритм Евклида и его сложность.

2.2. Вычисления в кольцах вычетов. Китайская теорема об остатках. Алгоритм Монтгомери.

2.3. Строение мультипликативной группы кольца вычетов. Критерий цикличности. Первообразные корни.

2.4. Квадратичные вычеты и невычеты. Квадратичный закон взаимности. Символы Лежандра и Якоби, их свойства и алгоритмы вычисления.

2.5. Решение степенных и показательных сравнений.

Тема 3. Цепные дроби

3.1. Понятие конечной и бесконечной цепной дроби. Подходящие дроби и их свойства.

3.2. Представление действительных чисел цепными дробями. Теорема Лагранжа о представлении квадратичных иррациональностей периодическими цепными дробями.

3.3. Цепные дроби как наилучшие рациональные приближения действительных чисел.

Тема 4. Простые числа

4.1. Частные виды простых чисел: простые числа Ферма и Мерсенна, их свойства.

4.2. Критерии простоты. Необходимые условия простоты.

4.3. Вопросы распределения простых чисел в натуральном ряду. Теорема Чебышева и асимптотический закон распределения простых чисел.

4.4. Алгоритмы проверки чисел на простоту. Тесты Соловея-Штрассена и Миллера-Рабина.

4.5. Методы построения больших простых чисел.

Тема 5. Методы разложения чисел на множители

5.1. Алгоритмы экспоненциальной сложности. Метод Ферма и его модификации. Вероятностный алгоритм факторизации Полларда. Алгоритм факторизации Полларда-Штрассена.

5.2. Субэкспоненциальные алгоритмы, основанные на идее метода Ферма. Алгоритм Диксона. Оценка сложности алгоритма Диксона. Алгоритм Брилхарта-Моррисона. Метод квадратичного решета Померанца.

5.3. "p-1" и "p+1" - методы разложения.

5.4. Криптографическая система RSA и основы ее анализа.

Тема 6. Вычисления в кольцах многочленов

6.1. Алгоритмы нахождения значений многочленов, произведения многочленов.

6.2. Использование быстрых преобразований Фурье для нахождения произведения многочленов.

Тема 7. Методы дискретного логарифмирования

7.1. Методы логарифмирования в произвольной циклической полугруппе. Алгоритмы Полларда, А.О.Гельфонда, В.И.Нечаева.

7.2. Индекс-метод Вестерна-Миллера для логарифмирования в простом поле и поле малой характеристики.

7.3. Криптографические системы, построенные на основе задачи дискретного логарифмирования: ключевой обмен Диффи и Хеллмана, системы открытого шифрования и цифровой подписи Эль-Гамаля и их анализ.

Тема 8. Элементы криптографии на эллиптических кривых

8.1. Эллиптические кривые. Группа точек эллиптической кривой.

8.2. Применение эллиптических кривых при построении криптосистем.

8.3. Применение аппарата теории эллиптических кривых к проверке простоты и факторизации целых чисел.

Требования к результатам освоения дисциплины

Знать:

- строение мультипликативной группы колец вычетов;
- способы представления действительных чисел цепными дробями;
- основные свойства символов Лежандра и Якоби,
- критерии простоты и их использование для факторизации натуральных чисел;
- алгоритмы проверки чисел на простоту; построения больших простых чисел;
- алгоритмы разложения чисел и многочленов на множители,
- методы дискретного логарифмирования в конечных циклических группах;
- основные свойства групп точек эллиптических кривых.

Требования к результатам освоения дисциплины

Уметь:

- исследовать и решать системы сравнений по произвольному модулю;
- представлять действительные числа цепными дробями;
- строить большие простые числа,
- применять алгоритмы проверки чисел на простоту; построения больших простых чисел;
- применять алгоритмы разложения чисел и многочленов на множители,

Требования к результатам освоения дисциплины

Владеть:

- навыками применения теории чисел в криптографии и других дисциплинах;
- навыками применения основных вычислительных алгоритмов в кольцах вычетов и кольцах многочленов.

Основная литература

1. *Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.* Введение в теоретико-числовые методы криптографии. – СПб: «Лань», 2010. Учебное пособие гриф УМО
2. *Коблиц Н.* Курс теории чисел и криптографии. – М.: ТВП, 2001. – 262 с.
3. *Виноградов И.М.* Основы теории чисел. – СПб.: «Лань», 2004. – 176 с.
4. *Черемушкин А. В.* Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с. Учебное пособие гриф УМО

Дополнительная литература

1. *Ахо А., Хопкрофт Дж., Ульман Дж.* Структуры данных и алгоритмы. – Москва – Санкт-Петербург – Киев: Издательский дом «Вильямс», 2001. – 384 с.
2. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2007.
3. *Ростовцев А. Г.* Алгебраические основы криптографии. – СПб.: НПО «Мир и семья», ООО «Интерлайн», 2000. – 354 с.
4. *Нестеренко Ю.В.* Теория чисел: учебник для студентов высших учебных заведений. – М.: Издат. центр «Академия», 2008. – 272 с.

Дополнительная литература

4. *Гашков С.Б., Чубариков В.Н.* Арифметика, алгоритмы, сложность вычислений. Учебное пособие. — М.: Высшая школа, 2000.
5. *Ноден П., Китте К.* Алгебраическая алгоритмика. С упражнениями и решениями. — М.: Мир, 1999.
6. *Акритас А.* Основы компьютерной алгебры с приложениями. — М.: Мир, 1994
7. *Саломаа А.* Криптография с открытым ключом. — М.: Мир, 1996.