**Арифметические вопросы криптографии. ½ г.**

**Программа курса:**

Глава I. Введение

§ 1. Понятие информации и ее

§ 2. Основные задачи теории кодирования

§ 3. Алфавитное кодирование

§ 4. О помехоустойчивости

§ 5. Об увеличении скорости передачи информации

§ 6. О защите информации

§ 7. О симметричных шифрах

§ 8. О шифровании с открытым ключом

Глава II. Префиксные коды. Коды Шеннона и Гилберта–Мура

§ 1. Префиксные коды. Неравенство Крафта – МакМиллана

§ 2. Теорема о минимальной длине префиксного кода

Глава III. Конечные поля. Циклические коды

§ 1. Конечные поля. Неприводимые многочлены

§ 2. Циклические коды

Глава IV. Рекуррентные соотношения. Производящие функции

§ 1. Рекуррентные соотношения

§ 2. Последовательность Фибоначчи

§ 3. Линейные рекуррентные уравнения второго порядка

§ 4. Линейные рекуррентные уравнения произвольного порядка

§ 5. Рекуррентные соотношения первого порядка в кольцах вычетов

§ 6. Рекуррентные соотношения в конечных полях

**Арифметические вопросы криптографии. Дополнительные главы. ½ г.**

**Программа курса:**

Глава V. Арифметический подход к искажению знаков

в шифрах простой замены и Виженера

§ 1. Введение

§ 2. Метод искажения знаков в шифре простой замены

§ 3. Метод искажения знаков в шифре простой замены

§ 4. Комбинированный метод искажения частот

§ 5. Анализ методов искажения знаков

§ 6. Применение китайской теоремы об остатках

§ 7. Арифметический вариант шифра Виженера

Глава VI. Асимметричные шифры

§ 1. Введение .

§ 2. Задача о рюкзаке

§ 3. Рюкзачная система шифрования

§ 4. Система шифрования RSA

§ 5. Хэш-функции

Глава VII. Задачи по теории чисел

§ 1. Квадратичные вычеты и невычеты по простому модулю

§ 2. Извлечение квадратного корня по простому модулю

§ 3. Символ Якоби

§ 4. Извлечение квадратного корня по составному модулю

§ 5. Целая часть квадратного корня

§ 6. Символ Кронекера

§ 7. Простейшие теоремы о распределении простых чисел

§ 8. Распознавание простых и составных чисел

§ 9. Непрерывные (цепные) дроби

§ 10. Арифметика квадратичных полей

§ 11. Разложение квадратичных иррациональностей

§ 12. Разложение квадратного корня в непрерывную дробь .

§ 13. Вычисление основной единицы

§ 14. Теорема П. Л. Чебышева (постулат Бертрана)

**Экзаменационные вопросы**

I. Алфавитное кодирование

1. Понятие алфавита и слова в алфавите. Кодирование сообще-

ния. Алфавит сообщений. Алфавит кодирования. Однозначное ко-

дирование.

2. Схема, задающая алфавитное кодирование. Примеры схем, за-

дающих однозначное и неоднозначное кодирование. Префикс слова и

определение схемы, обладающей свойством префикса. Достаточное

условие взаимно однозначного кодирования.

II. Помехоустойчивость

1. Многоразрядный код. Расстояние Хемминга. Неравенство тре-

угольника. Теорема об исправлении ошибок в кодах с любым задан-

ным расстоянием.

2. Пример множества 5-разрядных двоичных кодов, в которых

исправляется одна возможная ошибка. Способ построения множе-

ства 5-разрядных двоичных кодов, имеющих кодовое расстояние,

равное 3.

III. Передача сообщения по каналу без шума

1. Пример построения кода Фано в случае 4-х буквенного алфа-

вита сообщений и 2-х буквенного алфавита кодирования. Средняя

длина кодового слова. Общая схема построения кода Фано, постро-

ение таблицы.

2. Бинарное дерево для двоичного кода Фано. Необходимое и до-

статочное условия существования префиксного кода заданного объ-

ема и с заданным набором длин слов. Неравенство Крафта – Мак-

Миллана. Необходимое условие существования однозначно декоди-

руемого кода. Две теоремы об оценке средней длины кодовых слов.

Теорема о минимальной длине префиксного кода

3. Построение оптимального кода Хафмена. Пример.

IV. Способы защиты информации

1. Защита информации с помощью перестановки. Маршрутные

перестановки. Шифры вертикальной замены. Решетка Кардано.

2. Защита информации с помощью шифра замены. Система Це-

заря и система Цезаря с ключевым словом. Блочные и поточные

шифры замены. Примеры блочных шифров замены: шифры Плей-

фера и Хилла.

V. О симметричных шифрах

VI. О шифровании с открытым ключом

VII. Конечные поля. Циклические коды

1. Конечные поля. Неприводимые многочлены над конечным по-

лем.

2. Циклические коды.

VIII. Рекуррентные соотношения. Производящие функ-

ции

1. Примеры рекуррентных соотношений.

2. Последовательность Фибоначчи.

3. Линейные рекуррентные уравнения второго порядка.

4. Линейные рекуррентные уравнения произвольного порядка.

5. Рекуррентные соотношения в кольцах вычетов.

IX. Арифметический подход к искажению знаков в шиф-

рах простой замены и Виженера

1. Примеры шифров со “сжатием” алфавита.

2. Метод искажения знаков в шифре простой замены с помощью

извлечения корня квадратного.

3. Метод искажения знаков в шифре простой замены с помощью

возведения в квадрат.

4. Комбинированный метод искажения частот появления знаков

в шифре простой замены.

5. Анализ методов искажения знаков в шифре простой замены.

6. Применение китайской теоремы об остатках к шифру Виже-

нера.

7. Арифметический вариант шифра Виженера.