Программа курса лекций
«ТЕОРИЯ ЧИСЕЛ»
Лектор: **ЗУДИЛИН В. В. ,** доцент

В настоящее время теоретико-числовые методы криптографии активно проникают в сферу экономики и финансов. Этому во многом способствует бурное развитие информационных и компьютерных технологий.

Цель курса – обеспечить усвоение основ элементарной теории чисел и понимание ее базовых алгоритмических концепций:

a) для повышения уровня общей математической подготовки;
b) для получения простейших навыков оценки сложности вычислений;
c) для понимания принципов работы современных алгоритмов шифрования и цифровой подписи.

В теоретической части курса излагаются основы элементарной теории чисел и иллюстрируется их применение для построения алгоритмов (алгоритм быстрого возведения в степень по модулю m, алгоритм факторизации целого числа, детерминированные и вероятностные алгоритмы проверки чисел на простоту и т. д.).

Для закрепления материала курса «Теория чисел» в течение учебного года проводятся семинарские занятия.

1. Делимость. Основная теорема арифметики. Алгоритм Евклида и его сложность. Решение линейных уравнений в целых числах. Конечные непрерывные дроби.
2. Бесконечные непрерывные дроби. Свойства подходящих дробей. Квадратичные иррациональности. Теорема Эйлера-Лагранжа.
3. Мультипликативные функции и их свойства. Формула обращения Мёбиуса. Функция Эйлера.
4. Теория сравнений. Кольцо вычетов. Группа обратимых элементов кольца вычетов. Теоремы Ферма и Эйлера. Теорема Вильсона и ее обращение. Китайская теорема об остатках. Решение систем сравнений.
5. Квадратичные вычеты. Свойства символов Лежандра и Якоби. Квадратичный закон взаимности.
6. Первообразные корни и индексы. Существование первообразных корней по простому модулю и модулям p^a, $2p^a$. Структура и порядок группы Z_m^* для произвольного m.
7. Арифметическая сложность алгоритмов. Быстрый алгоритм возведения в степень. Простейшие детерминированные и вероятностные тесты на простоту. Построение больших простых чисел. Псевдопростые числа. Тест Соловея—Штрассена. Разложение чисел на множители. Методы Ферма и Лежандра. Дискретное логарифмирование.
8. Понятие о криптографии с открытым ключом. Система шифрования RSA. Система Диффи-Хелмана. Электронная подпись.

ЛИТЕРАТУРА

1. Бухштаб А.А. Теория чисел. М.: Учпедгиз, 1960.
2. Виноградов И.М. Основы теории чисел. М.: Наука, 1953.
3. Коблиц Н. Курс теории чисел и криптографии. М.: ТВП, 2001.
4. Ленг С. Введение в теорию диофантовых приближений. Библиотека сборника «Математика». М.: Мир, 1970.
5. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002.
6. Ященко В.В. (ред.) Введение в криптографию. М.: МЦНМО–ЧеРо, 1998.