Аннотация рабочей программы дисциплины

«Алгебраические основы криптографии»

Направление подготовки - 01.04.04 «Прикладная математика»
Направленность (профиль) - «Математические методы и моделирование в естественнонаучной и технической сферах», Цифровая обработка сигналов и изображений»
Уровень образования - «магистратура»
Форма обучения - «очная»

1. Цели и задачи дисциплины

Цель преподавания дисциплины: формирование способности использовать алгебраические и теоретико-числовые методы для составления алгоритмов шифрования и дешифрования.

Задачи дисциплины: приобретение знаний основ криптографии, алгебраических и теоретико-числовые методов шифрования и дешифрования информации, умения применять простейшие криптографические алгоритмы шифрования и дешифрования на практике, а также осваивать методы решения различных криптографических задач, приобретение опыта составления простейших криптографических алгоритмов.

2. Место дисциплины в структуре ОП

Дисциплина входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы. Для изучения дисциплины студент должен знать базовые понятия курса общей алгебры. Понятия и методы дисциплины могут использоваться при прохождении производственной практики и подготовке ВКР по темам, связанным с технологиями защиты информации.

3. Краткое содержание дисциплины

Деление с остатком. НОД и НОК целых чисел. Алгоритм Евклида. Сравнения по модулю натурального числа. Простые числа. Основная теорема арифметики. Решение линейных диофантовых уравнений. Китайская теорема об остатках. Квадратичные вычеты и невычеты. Функция Эйлера. Малая теорема Ферма. Теорема Эйлера. Теорема Вильсона. Формулы количества делителей и суммы делителей натурального числа. Функция Мёбиуса. Формула обращения. Характеристика поля. Простое подполе. Аддитивная группа конечного поля. Количество элементов конечного поля. Мультипликативная группа конечного поля. Расширения полей. Существование поля из p^n элементов. Количество неприводимых многочленов заданной степени над конечным полем. Построение поля из p^n элементов. Изоморфизм конечных полей одного порядка. Автоморфизмы полей. Автоморфизм Фробениуса конечного поля. Группа автоморфизмов конечного поля. Мультипликативная группа кольца вычетов. Решение сравнений $f(x)\epsilon\ 0$ $(\bmod n)$. Дискретное логарифмирование. Основные задачи криптографии. Схемы шифрований RSA и Эль-Гамаля. Электронная цифровая подпись. Формирование общего секретного ключа двух абонентов. Проективная плоскость. Проективное пространство. Эллиптические кривые на проективной плоскости. Группа точек эллиптической кривой. Криптографические схемы на эллиптических кривых.

Разработчик: профессор каф. ВМ-1, д.ф.м.н., профессор Кожухов И.Б.