Аннотация

Научно-исследовательский семинар "Методы и алгоритмы защиты информации"

Тематически семинар состоит из двух частей. Первая часть посвящена криптографии. Здесь будут обсуждаться классические криптосистемы и криптосистемы с открытым ключом, задача дискретного логарифмирования и система Диффи-Хеллмана обмена ключам, системы Мэсси-Омура и Эль-Гамаля, система RSA, задача о рюкзаке и рюкзачная криптосистема, протоколы с нулевым разглашением. Также мы обсудим криптосистемы, построенные на основе эллиптических кривых, включая метод Поклингтона и метод Ленстры. Параллельно будут сообщены необходимые сведения из теории чисел, дискретной математики, алгебры и алгебраической геометрии.  Во второй части будет изучаться теория кодирования. Мы рассмотрим коды, исправляющие ошибки, поговорим про расстояние Хемминга и совершенные коды, неравенство Синглтона, коды Рида-Соломона и их декодирование, циклические коды и коды Галея, синдромы и декодирование по лидеру смежного класса. Этот раздел базируется на результатах из алгебры многочленов и линейной алгебры над конечными полями. На семинаре будут даны подробные доказательства всех используемых результатов.

Преподаватель: Аржанцев Иван Владимирович