Математическая криптография и коды с исправлением ошибок

Лектор Н.К. Верещагин, 2 семестр.

Математическая криптография - это наука о том, как строить криптографические протоколы, надежность которых либо безусловно доказуема, либо доказуема при условии необратимости некоторой функции. Например, предположив необратимость функции возведения в квадрат по составному модулю, можно построить надежную схему шифрования с открытым ключом.
А предположив существование односторонней функции, можно построить протокол игры в орлянку по телефону. Слово "математическая" в названии намекает на то, что эта наука является математической дисциплиной (содержит аккуратные определения и теоремы с доказательствами).
Коды с исправлением ошибок нужны для передачи информации по ненадежному каналу. Исходное слово в данном алфавите (сообщение) кодируется так, что после любой замены в коде небольшого количества символов по полученному слову можно было восстановить исходное сообщение.
Наиболее известными кодами такого сорта являются коды Хемминга, позволяющие исправлять одну ошибку (в коде разрешается изменить только один символ). В курсе будет рассказано также об обобщении кодов Хемминга на произвольное фиксированное количество ошибок (коды БЧХ). Более того, можно построить коды, количество исправляемых ошибок в которых может составлять фиксированный ненулевой процент от длины кодового слова, причем последняя линейно зависит от длины сообщения слова.

Необходимым условием для прослушивания курса является сдача курса "Сложность вычислений".