Криптография: вчера, сегодня, завтра

Лекция знакомит слушателей с историей создания методов шифрования, начиная с древности до наших дней, намечая возможные дальнейшие направления развития этой области знаний.

В качестве начальных сведений обсуждаются шифры простой замены и, в частности, шифр Цезаря. На его примере рассматривается математическая модель шифрования и расшифровки. Приводится метод взлома шифров простой замены, известный как частотный анализ.

Приводятся примеры шифрования текстов методом простой замены, один из которых описан в рассказе Артура Конан Дойля «Пляшущие человечки» об очередном деле Шерлока Холмса.

Разъясняются основные принципы построения более надежных методов шифрования – криптосистем с открытым ключом, математические и вычислительные основы современной криптографии.

Затрагиваются вопросы расшифровки и надежности шифра, перспективные методы обнаружения перехвата секретной информации.

Приведен ряд конкретных примеров шифрования, в том числе при помощи криптосистемы RSA, для понимания принципа действия которой изложены необходимые теоретико-числовые основы.