

Аннотация дисциплины

Математические основы криптографии и ее применение в банковском деле

Цель дисциплины:

овладение криптографическими средствами защиты банковской информации **и** навыками использования основных криптографических протоколов, применяемых в финансовой и коммерческой деятельности.

Краткое содержание:

Основные задачи современной криптографии в современных условиях. Математический аппарат, используемый в криптографии. Основы одноключевых криптосистем. Шифры Трисемуса, Гронсфельда, «двойной квадрат» Уитстона. Матричный метод шифрования- дешифрования. Асимметричные криптосистемы. Функция Эйлера и её применение в криптосистеме RSA. Шифрование с открытым ключом и простые числа. Односторонние функции и возможности их использования в криптографии. Китайская теорема об остатках и возможности её использования в криптографических целях. Несимметричное шифрование-дешифрование. Операция mod и её использование в криптографии.