С/к естественно-научного содержания ``Основы криптографии’’, ½ г.

Профессор В.Н.Чубариков

1. Криптография: конфиденциальность, целостность, хеш-функция, цифровая подпись.
2. Секретные ключи: распределение, пересылка, разделение секретов. Открытые ключи. Математические модели открытого текста. Классификация шифров. Шифры замены и перестановки. Шифры гаммирования. Блочные шифры. Восстановление текстов, зашифрованных с неравновероятностной гаммой. Повторное использование гаммы. Криптоанализ шифра Виженера.
3. Блочные системы шифрования: анализ алгоритмов.
4. Системы шифрования с открытыми ключами. Идентификация. Криптопротоколы. Функции хеширования. Протоколы распределения ключей.
5. Квантово-криптографический протокол открытого распределения ключей.