Программа курса «Математическая криптография» (весенний семестр 2015/2016 уч. г.)

Семейства хэш-функций с трудно обнаружимыми коллизиями. Теорема о композиции для семейств хэш-функций с трудно обнаружимыми коллизиями.

Универсальные односторонние семейства хэш-функций. Теорема о композиции для универсальных односторонних семейств хэш-функций. Теорема Ромпеля о необходимом и достаточном условии существования универсальных односторонних семейств хэш-функций (без доказательства). Построение универсального одностороннего семейства хэш-функций на основе произвольной односторонней перестановки (теорема Наора — Юнга).

Семейства функций и перестановок с секретом. Примеры гипотетических семейств функций и перестановок с секретом (семейства RSA и Рабина). Доказательство того, что семейство Рабина является семейством функций с секретом в предположении трудности задачи факторизации целых чисел Блюма. Доказательство того, что семейство Рабина, ограниченное на элементы нечетного порядка, является семейством перестановок с секретом в предположении трудности задачи факторизации целых чисел.

Элементы теории Шеннона систем секретной связи (secrecy systems). Понятия замкнутой, совершенной и чистой системы секретной связи. Нижняя оценка числа элементов носителя априорного распределения вероятностей на пространстве ключей совершенной системы секретной связи. Остаточные классы сообщений и криптограмм замкнутой чистой системы секретной связи. Разложение замкнутой чистой системы секретной связи в «дизъюнктное объединение» совершенных систем секретной связи. Пример: система секретной связи Вернама.

Системы шифрования (криптосистемы) с секретным и с открытым ключом. Блоковые системы шифрования. Атаки на системы шифрования и угрозы стойкости последних. IND-стойкость, IND-CPA-стойкость и IND-CCA-стойкость. Построение IND-CPA-стойкой блоковой системы шифрования с секретным ключом на основе произвольного полиномиально инвертируемого псевдослучайного семейства перестановок. Построение IND-стойкой (на основе атаки с открытым ключом) блоковой системы шифрования с открытым ключом, исходя из семейства функций, трудного для некоторого семейства перестановок с секретом. Конструкция системы шифрования сообщений произвольной длины на основе блоковой системы шифрования. Сохранение IND-стойкости на основе атаки с открытым ключом для этой конструкции, примененной к системе шифрования с открытым ключом.