Программа экзамена по спецкурсу «Криптография» в гр. 08-306, 308 на 2011/12 учебный год

Теория

1. Предмет и задачи криптографии. Сложность. Классы сложности P, NP, BPP Гипотеза $P \neq NP$.
2. Модульная арифметика. Группа. Группы Z_p^*, Z_p^+. Алгоритм Евклида. Китайская теорема об остатках.
3. Квадратичные вычеты. Символы Лежандра и Якоби.
4. Односторонние функции.
5. Псевдослучайные функции.
6. Симметричное шифрование. Блочные шифры. Примеры. Основные типы атак.
7. Режимы шифрования.
8. Парадокс дней рождения.
9. Асимметричное шифрование. Примеры алгоритмов.
10. Хеш-функции. Требования к криптографическим хеш-функциям. Структура Меркля-Дамгарда.
11. Целостность сообщений. MAC, HMAC.
12. Цифровая подпись. Примеры алгоритмов. Типы атак.
13. Обмен ключами. Протокол Диффи-Хеллмана. Сессионные ключи.
14. Забывчивая передача данных. Привязка к биту. Протокол подписания контракта.
15. Доказательства с нулевым разглашением. Примеры.
16. Задача о византийских генералах.

Алгоритмы

1. Алгоритм симметричного шифрования DES. Модификации.
2. Алгоритм симметричного шифрования IDEA.
3. Алгоритм симметричного шифрования AES (Rijndael).
4. Алгоритм симметричного шифрования Blowfish.
5. Алгоритм асимметричного шифрования RSA.
6. Алгоритм асимметричного шифрования ElGamal.
7. Хеш-функция MD5.
8. Хеш-функция SHA-1.
9. Схемы цифровой подписи ElGamal и DSS.
10. Алгоритмы на основе RSA: RSA-OAEP, PSS.
11. Протокол SSH: алгоритм обмена ключами.