Хеш-функция
Аутентификация сообщения

Свойства
-длина (H) - const
-длина (M) - произвольная
- легкость вычисления
-необратимость
-a!=b => H(a)!=H(b)

Коллизия одинаковых хешей (birthday-коллизией)

Назначение
-аутентификация
-защита данных

Алгоритмы
MD5 (message digest)
SHA2 (secure hash algorithm)

Avalanche effect - f всех выходных бит (каждого входного бита)

Лавинный эффект порядка X : 1 бит -> X бит выходной последовательности

Диффузия (перестановки)
Конфузия (замены)

MD5
Вход - 128 бит
Выход - 160 бит
1991->1993

SHA0
Вход - 512 бит
Выход - 160 бит

SHA1
Вход - 512 бит
Выход - 160 бит
1995

SHA2 (SHA224,256,384,512)
Вход - 512/1024 бит
Выход - 224/256 384/512 бит

SHA3
Вход - 512/1024 бит
Выход - 224/256 384/512 бит

Электронная подпись

Свойства собственноручной подписи
- Аутентичность (именно подписант)
- Добровольное согласие
- Неотказуемость подписавшегося
- Скорость
- Непересимость
- Целостность

Алгоритм подписания (секретный ключ)
- Вычисление хеш-функции (данных) - H1
- Шифрование с открытым ключом (секретный ключ)

Проверка подписи (данные, подпись (ЭП), открытый ключ)
- Вычисление хеш-функции (данных) - H2
- Расшифровка подпись с открытым ключом - H1
- Сравнение H1 и H2

63-ФЗ
Электронная подпись (информация, подпись -> лицо-подписант)

Виды подписи
- Простая
- Усиленная
  - Неквалифицированная
  - Квалифицированная (аккредитации в госорганах)

Архитектура клиентской системы
- Доверие к ОС
- CSP <-CryptoAPI
- Любая программа - CryptoAPI

Модели работы с ключами
- Децентрализованная (все со всеми обмениваются открытыми ключами)
- Централизованная (public key infrastructure - PKI)

Удостоверяющий центр (УЦ) - имеет корневой сертификат
Certification Authority (CA)

Сертификат

X.509

- Версия и Название алгоритма ЭП
- Данные и ЭП организации выдавшей сертификат
- Срок действия
- Данные владельца
- Открытый ключ владельца

Certificate Revocation List (CRL)