

—



g?

o

Хеши-функции. (Две системы проверки)
(сравнивают m и $H(m)$)

Что считают:

- Длина H -функции
- Длина M - производительность
- Диффузия блоков данных
- Нестратичность $H(M) \neq M$
- $M_1 \neq M_2 \rightarrow H(M_1) \neq H(M_2)$

birthday - атака:

Набухание (avalanche) эффект непрерывно означает
изменение 1го бита D ведет к изменению X

Сам хеш-функция: $X: 1B \rightarrow X$ bit $H(X)$

Алгоритмы:

- Message Digest (MD4, MD5)
- Secure Hash Algorithm (SHA-0 .. SHA-3)

History:

MD5

in: 128 bit

out: 160 bit

SHA0

in: 512 bit

out: 160 bit

SHA3 (Skein)

in: 512 bit

out: 360 bit

SHA2 (расширение) (2002) 18 payload

in: 512 / 1024 bit

out: 256 / 224 bit

SHA3 ↑

in:

512 / 384 bit

out:

Энкапсулированные подписи

Свойства подписей подпись:

- Аутентичность (связь с подписчиком)
- Непрекосимость к другим документам (связь с данными)
- Достоверность
- Удостоверение

Расшифровка подписи: ($H - msg$)

1. Хеширование $H(M)$

2. M \rightarrow подпись S

$E(H(M), k^E - \text{серкт})$

k^E - открытый
ключ
 k^D - секретный
ключ
POT

Проверка подписи S :

1. $H(M)$

2. Расшифровка S : $D(S, k^P)$

3. Правильна? $H(M) = D(S, k^P)$

Виды подписей:

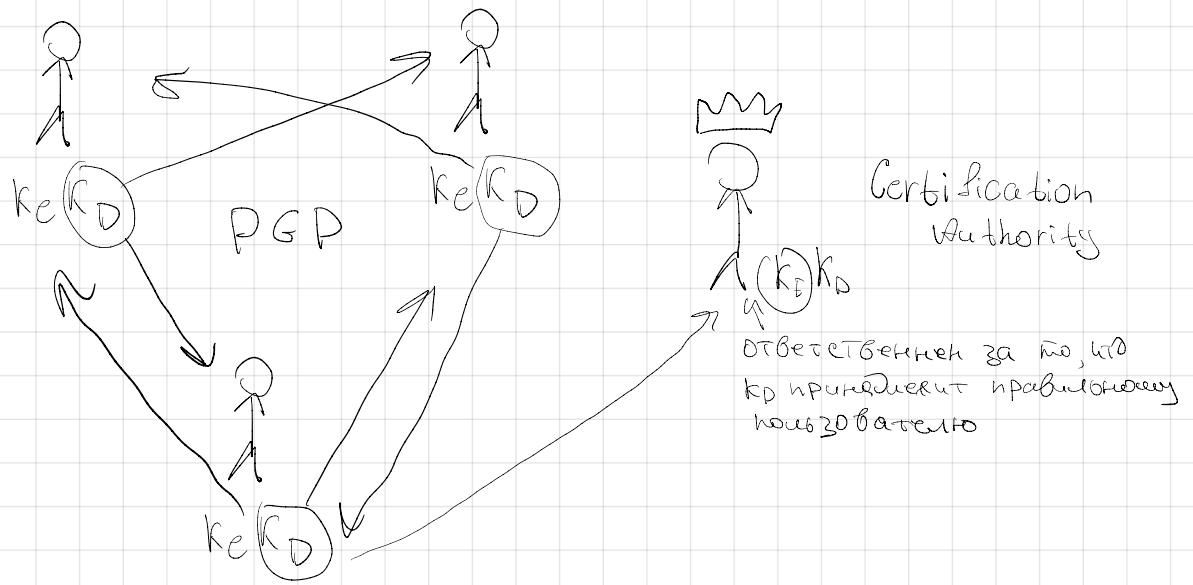
- Ключевые (личный от подписчика)
- Универсальные
 - Криптографические
 - Криптографические (PDT)

Протоколы:

- Доверие DC
- Crypto API (Доверие + носите)

Модели:

- Декларации доверия
- Установление доверия



CRL (Список отозванных сертификатов)

MP 5 Годарение Эл-ои ноИнсе (Ран-
нропозиционные
дикор)