Кирпичики криптографии

https://www.cypherpunks.ru/

Шифрование

Идеальный шифр

P открытый текст (plaintext)

C зашифрованный текст (cyphertext)

K ключ шифрования (key)

E функция шифрования

D функция дешифрования

- $E(P, K) = C$
- $D(C, K) = P$

OTP (One Time Pad)

- $len(P) = len(K)$
- $E = D = XOR$

Шифрование

Идеальный шифр

P открытый текст (plaintext)

C зашифрованный текст (cyphertext)

K ключ шифрования (key)

E функция шифрования

D функция дешифрования

- $E(P, K) = C$
- $D(C, K) = P$

OTP (One Time Pad)

- $len(P) = len(K)$
- $E = D = XOR$

Шифрование

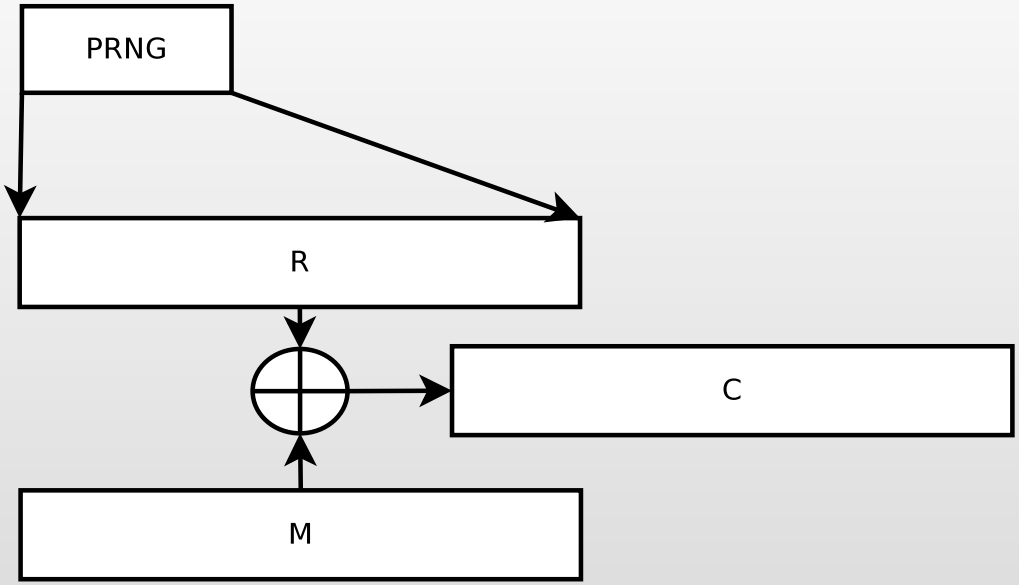
Атаки на OTP

- Использование ключа (R–последовательности) дважды: $C_1 \oplus C_2 = M_1 \oplus R \oplus M_2 \oplus R = M_1 \oplus M_2$
- Инвертирование бита шифротекста инвертирует бит в открытом тексте

Шифрование

Потоковый шифр

- Случайную последовательность генерируют CSPRNG (cryptographically secure pseudorandom number generator)
- Зерном (начальным состоянием) PRNG является ключ короткий
- Выход последовательности XOR с данными $\Rightarrow$ симметричный потоковый шифр



Шифрование

Блочный шифр

- PRNG/потоковый шифр это PRF: $XxK \to Y$
- Блочный шифр это PRP: $XxK \to X$

Симметричные шифры

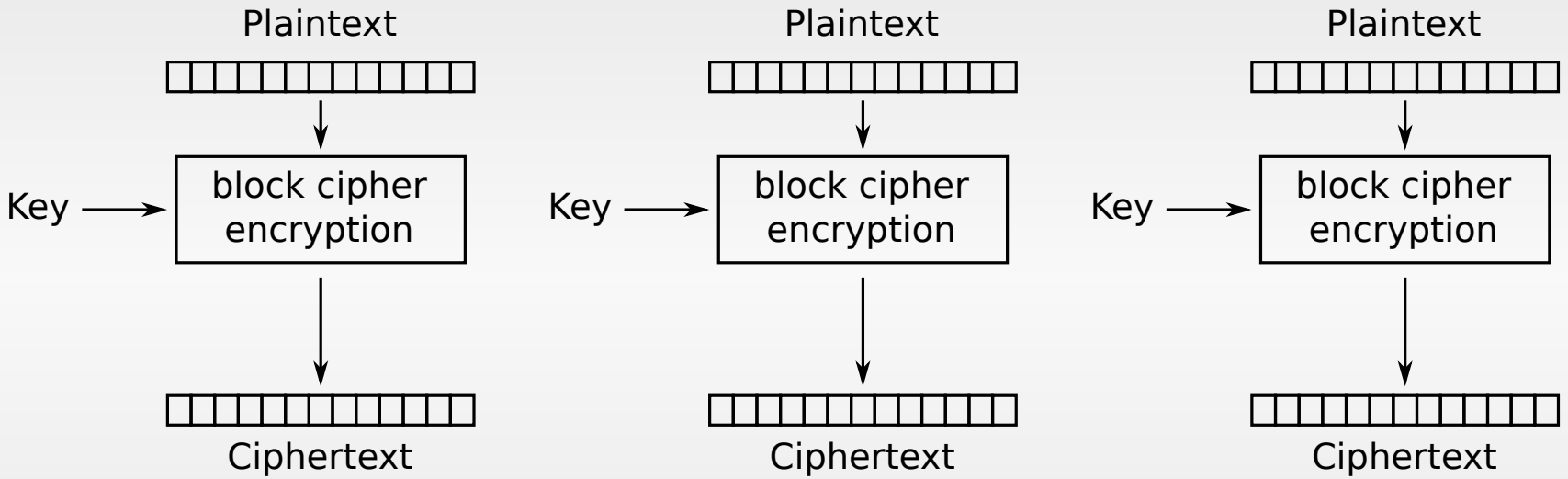
- A5/*, KASUMI
- RC4
- Phelix
- HC–128, HC–256
- Salsa20, ChaCha

Блочные шифры

- DES, 3DES
- AES/Rijndael
- Blowfish, Twofish, Threefish
- Serpent
- CAST–128, Camelia, IDEA
- GOST

Режимы шифрования

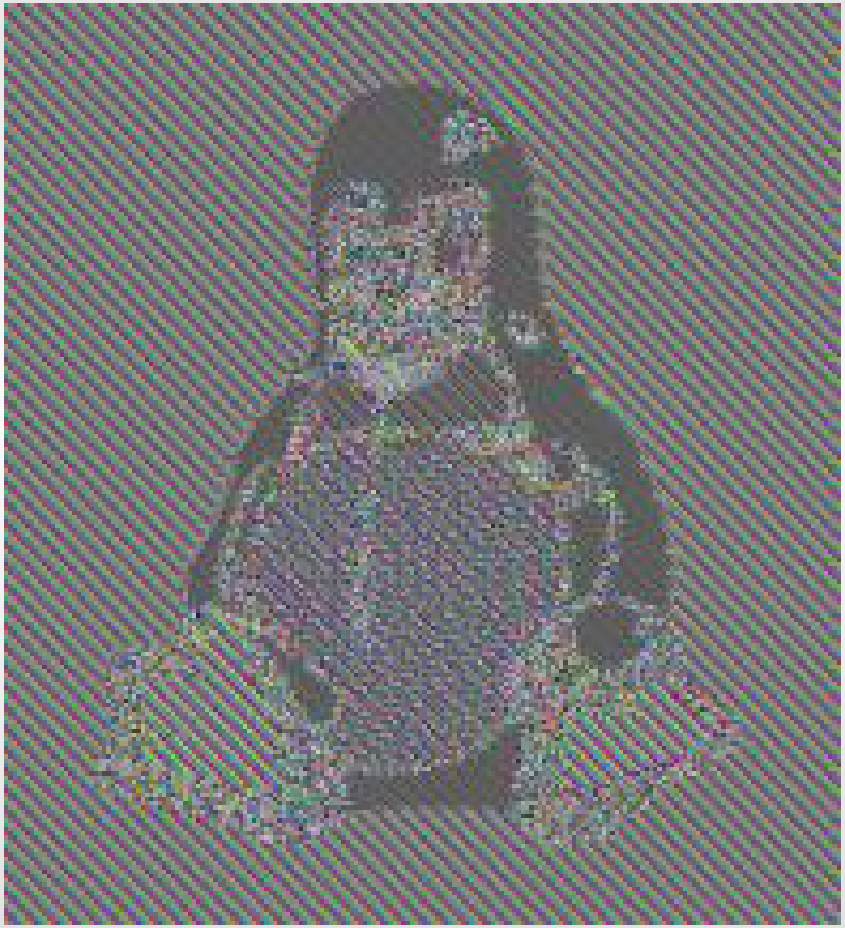
Encrypted CodeBook (ECB)



Electronic Codebook (ECB) mode encryption

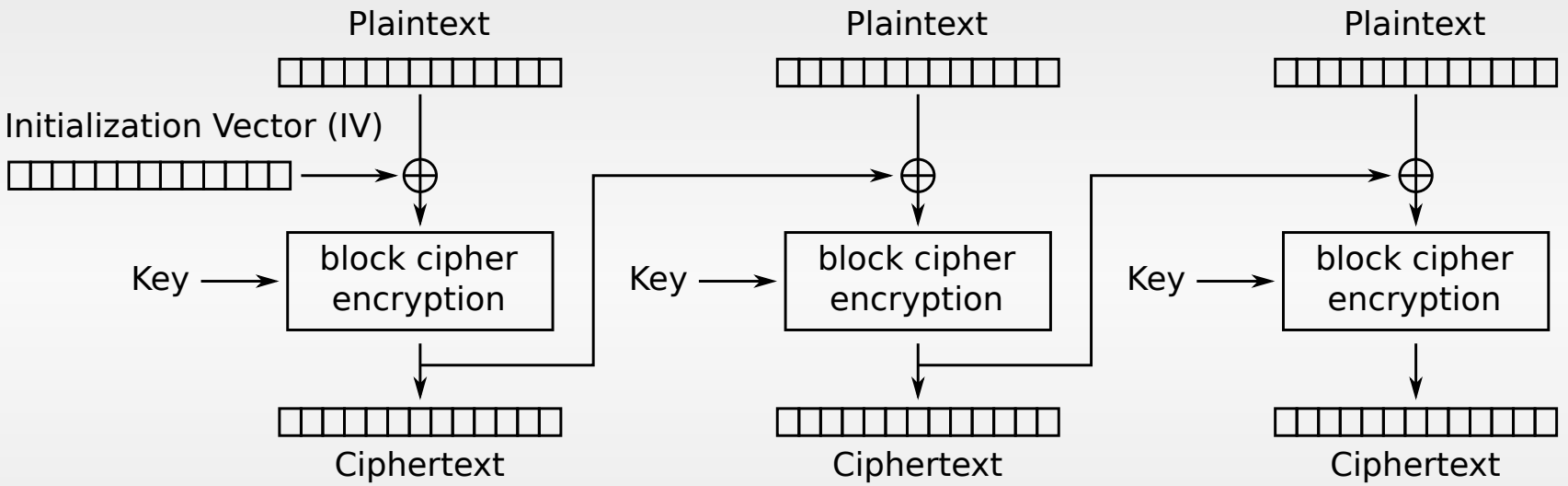
Режимы шифрования

Encrypted CodeBook (ECB)



Режимы шифрования

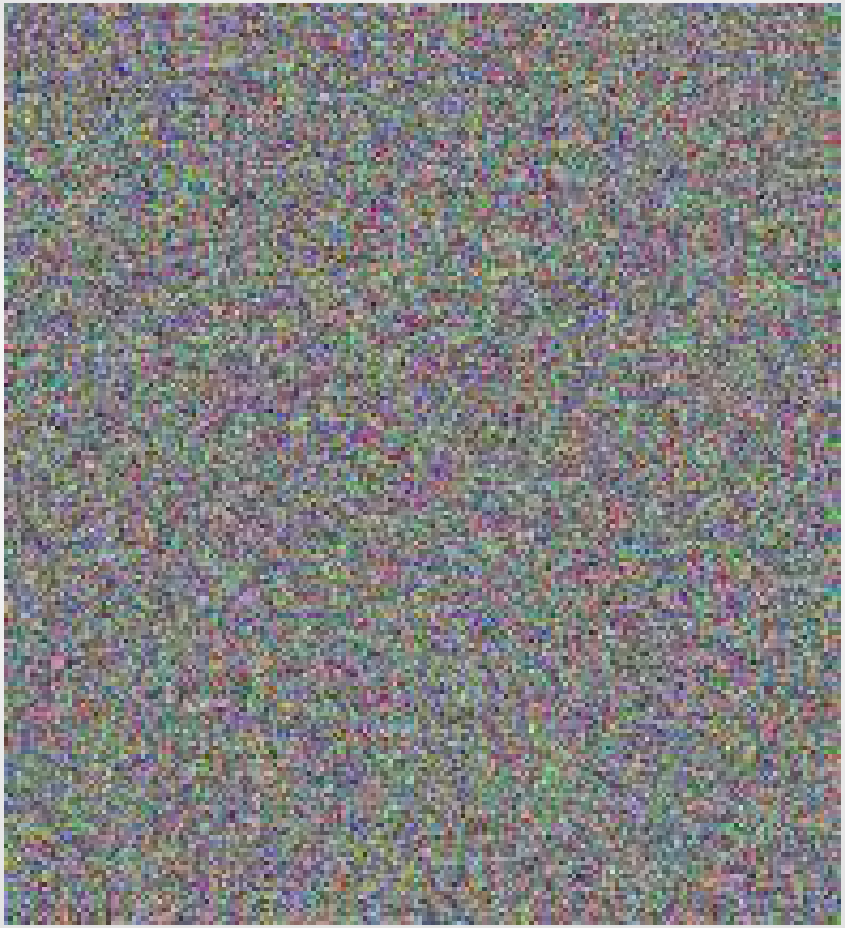
Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

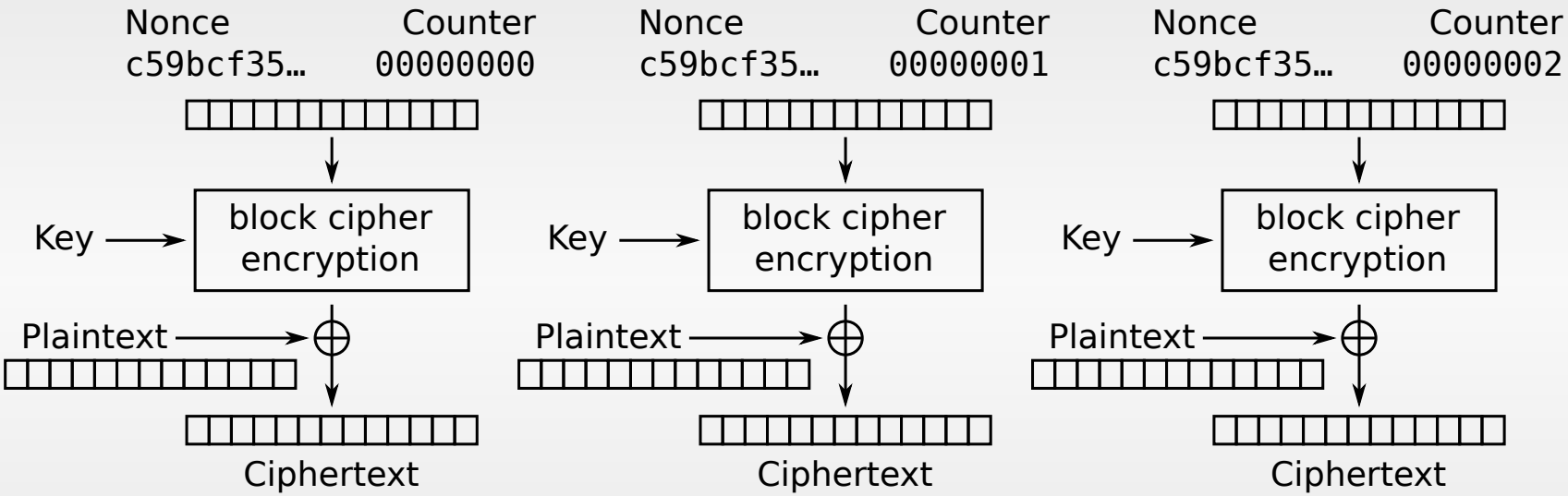
Режимы шифрования

Cipher Block Chaining (CBC)



Режимы шифрования

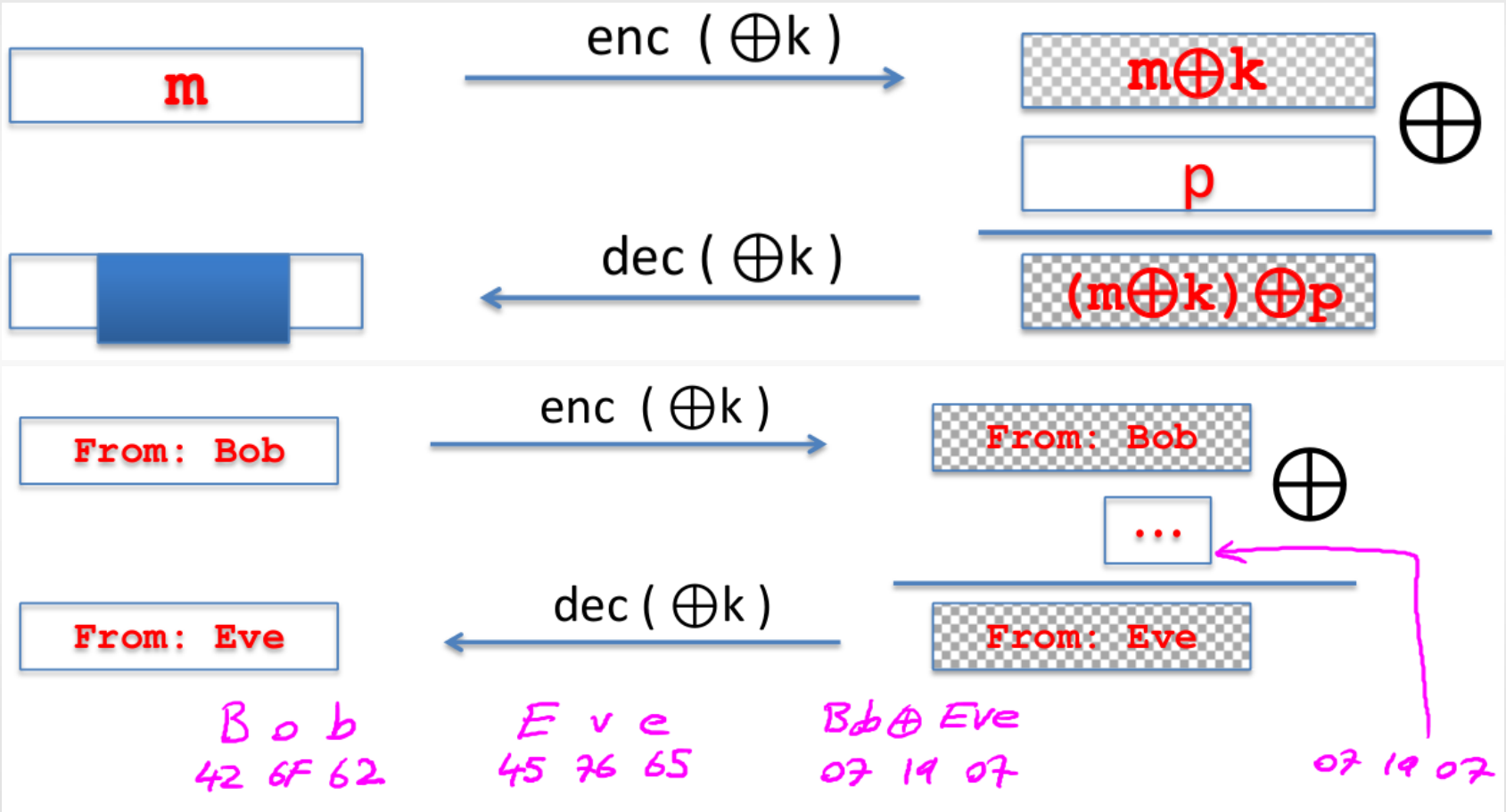
Counter (CTR)



Counter (CTR) mode encryption

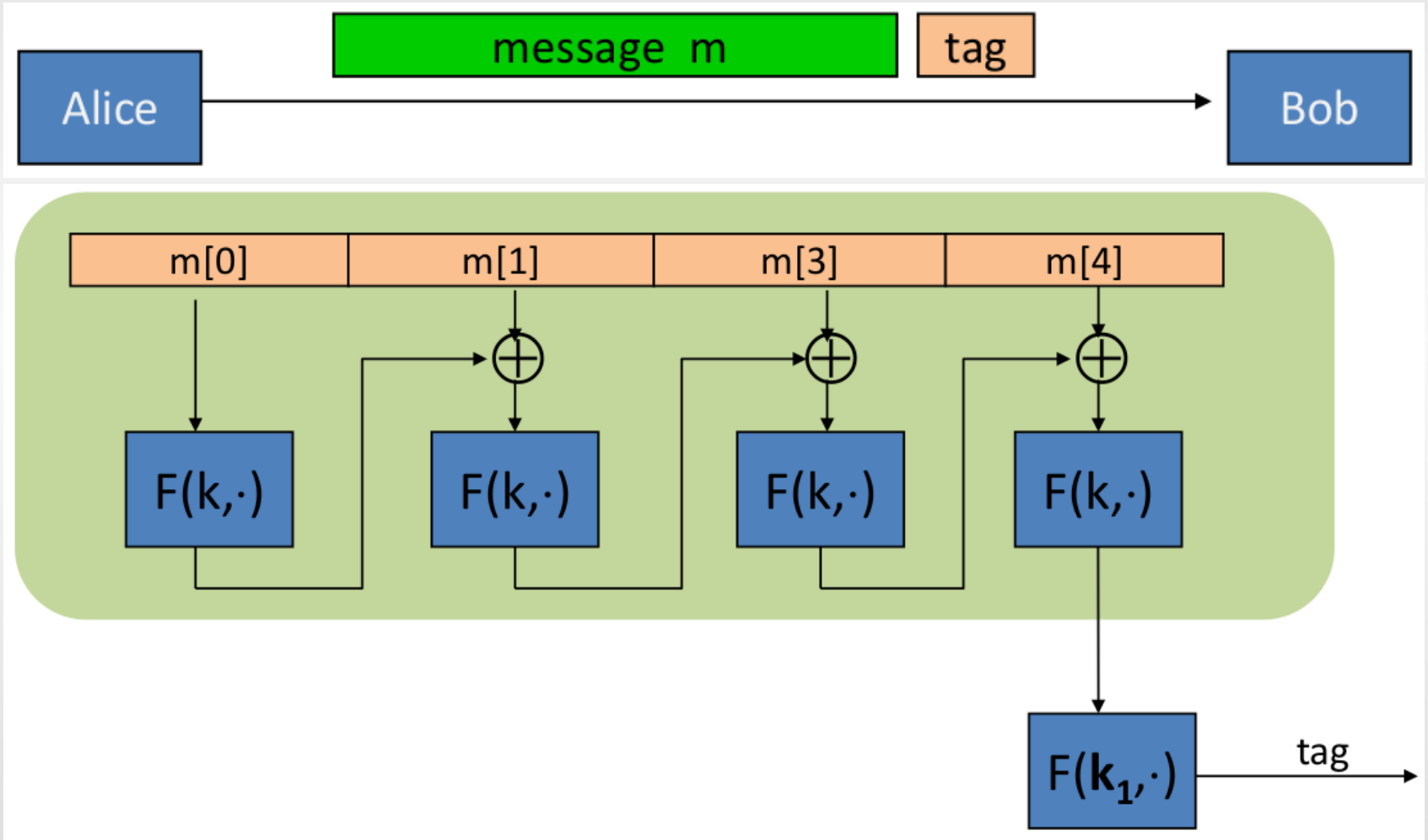
Аутентификация

Malleable encryption



Аутентификация

AEAD, MAC



Аутентификация

Хэш функции

- Лёгкость вычисления
- Односторонняя (зная хэш нельзя найти сообщение)
- Изменение даже бита изменяет и хэш
- Сложно найти сообщения с одинаковыми хэшами (коллизии)

Примеры функций

- MD5
- SHA1, SHA2, SHA3/Keccak
- RIPEMD, GOST
- Tiger
- BLAKE, BLAKE2, Skein

MAC особенности

- Противостоять подмене подписи
- Противостоять CPA

Аутентификация

Хэш функции

- Лёгкость вычисления
- Односторонняя (зная хэш нельзя найти сообщение)
- Изменение даже бита изменяет и хэш
- Сложно найти сообщения с одинаковыми хэшами (коллизии)

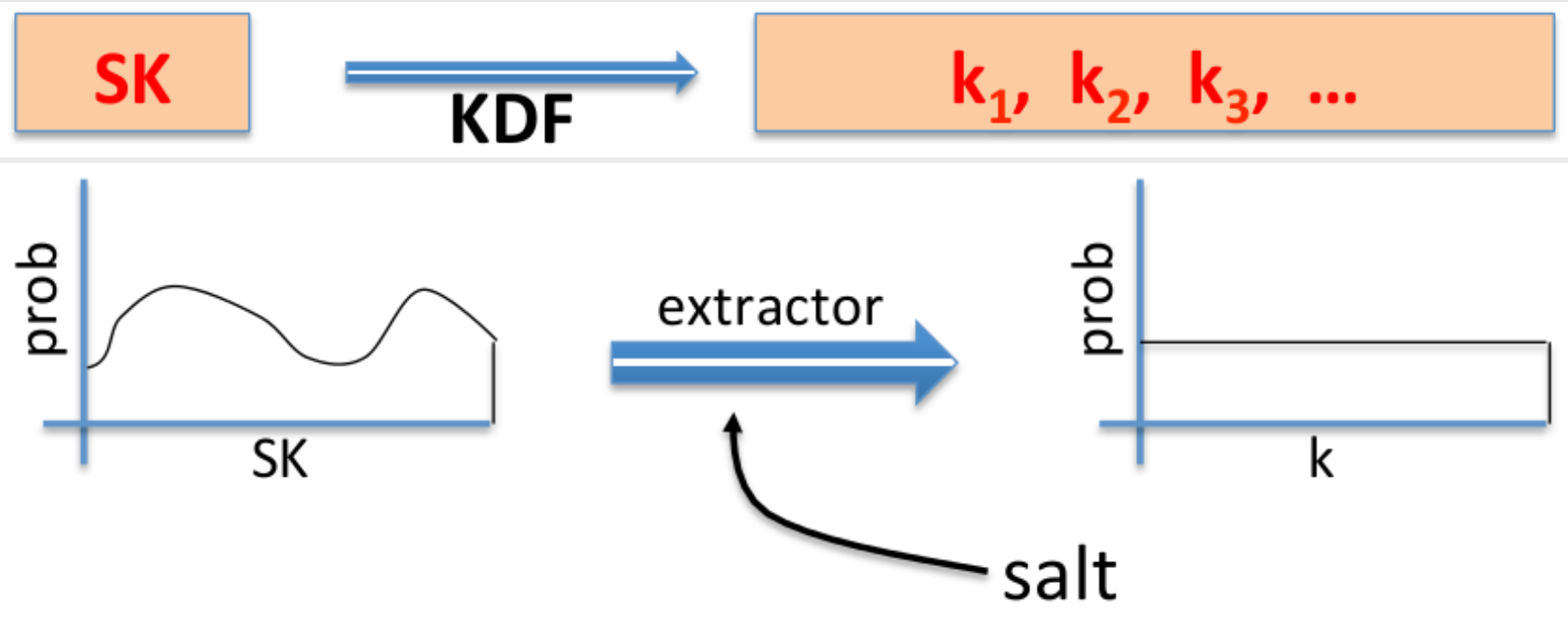
Примеры функций

- MD5
- SHA1, SHA2, SHA3/Keccak
- RIPEMD, GOST
- Tiger
- BLAKE, BLAKE2, Skein

MAC особенности

- Противостоять подмене подписи
- Противостоять CPA

Генерирование ключей (KDF)



Extract

$k = HMAC(salt, SK)$, соление

Expand

$k_1, k_n = HMAC(k, 1), HMAC(k, n)$

Для низкоэнтропийных паролей: $PBKDF = H^c(password + salt)$

Асимметричная криптография

Обмен ключами, DH

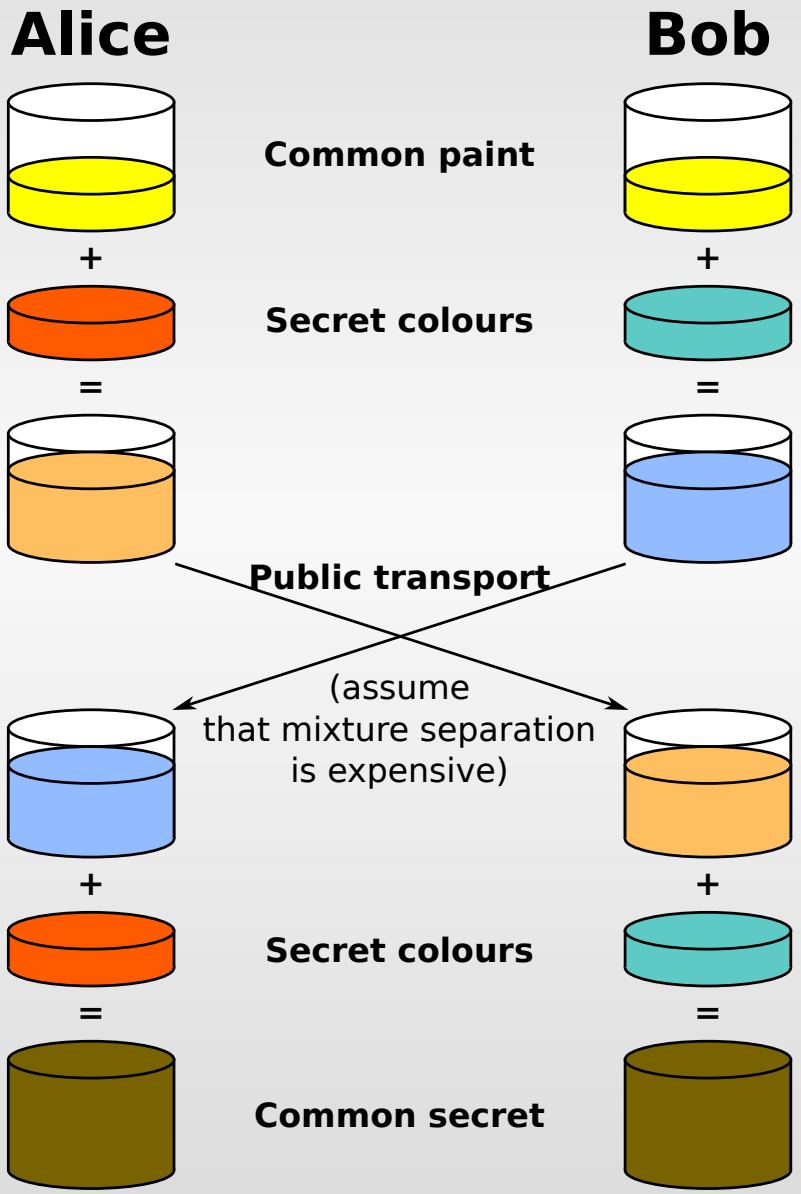
g — большое простое число

x,y — секретный ключ

обмен — одна сторона посылает g^x, другая g^y

вычисление — одна сторона вычисляет $(g^y)^x$, другая $(g^x)^y$

общий ключ — g^{xy}



Асимметричная криптография

Парные ключи

- Ключи разделены на две части, одна из которых считается публичной, другая приватной
- $E(M, K_{pub}) = C$, $D(C, K_{priv}) = M$
- $E(M, K_{priv}) = C$, $D(C, K_{pub}) = M$

Алгоритмы

- RSA
- ElGamal, DSA, DSA2, ECDSA
- GOST
- DH, ECDH, MQV, ECMQV

Асимметричная криптография

RSA

Генерирование ключей :

- p, q — большие простые числа
- $n = pq$ — модуль
- $1 < e < (p-1)(q-1)$
- $de = 1 mod (p-1)(q-1)$
- e, n — открытый ключ
- d, n — закрытый ключ

Шифрование $C = M^e mod\ n$

Дешифрование $M = C^d mod\ n$

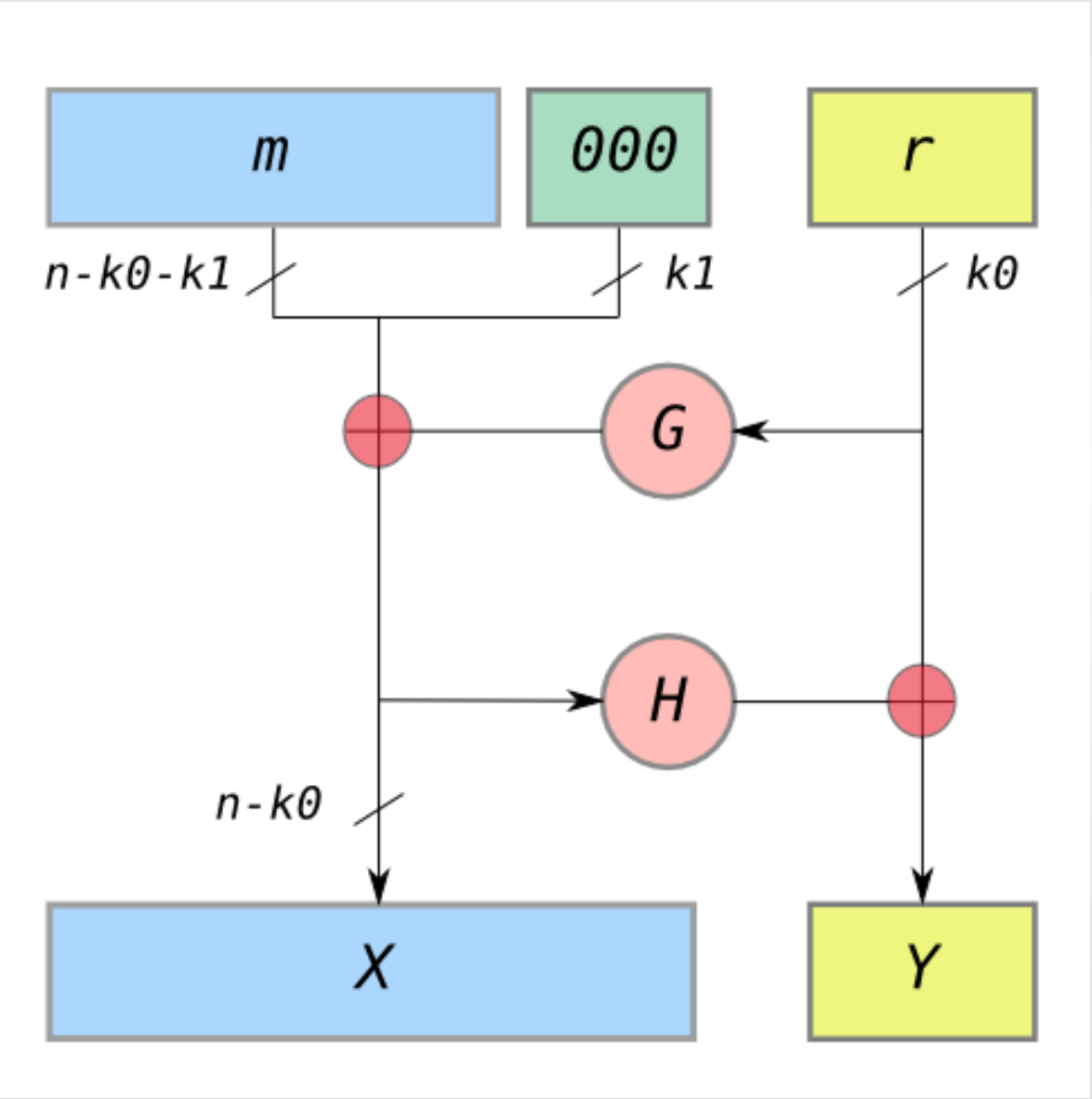
Асимметричная криптография

Тьма атак

- Малые значения e и $m \rightarrow$ шифротекст дешифруется
- Посылка одного сообщения с одним $e \rightarrow$ шифротекст дешифруется
- Детерминированный алгоритм $\rightarrow$ как и ECB не используется
- $m_1^e m_2^e = (m_1 m_2)^e mod\ n \rightarrow$ CCA может дешифровать

Асимметричная криптография

RSA дополнения



- PKCS1 v1.5
- RSAES–OAEP
- RSASSA–PSS
- ANSI X9.31
- RSA-KEM
- Ferguson–Schneier

Трудозатраты на взлом

Симметричный шифр

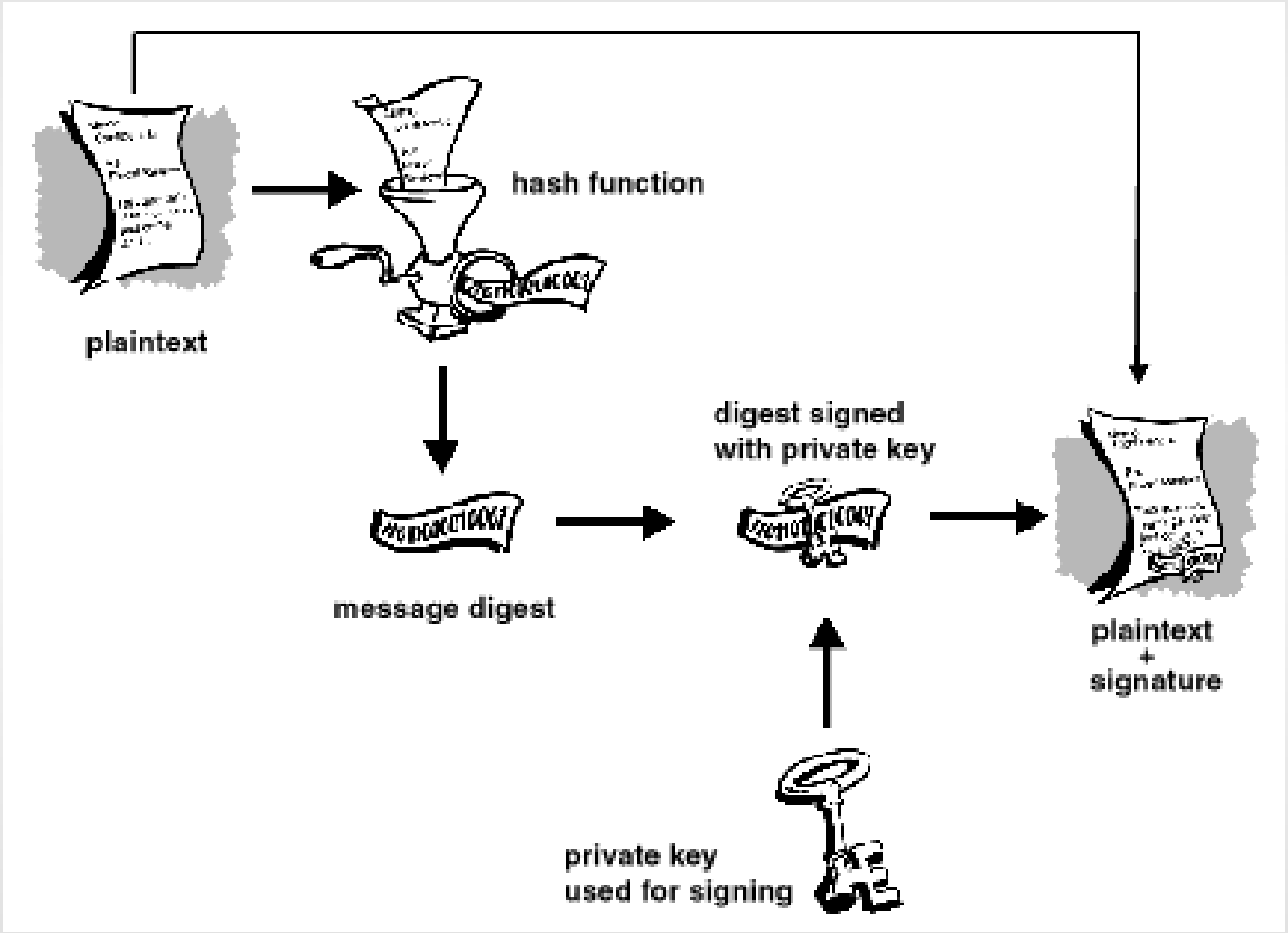
Стоимость	40бит	56бит	80бит	128бит
\$ 100 K	2 сек	35 ч	70 000 лет	10^{19}
\$ 1 T	0.02 мкс	1 мс	6 ч	10^{11}

Факторизация

Кол-во бит	MIPS/часов
512	< 200
768	100 000
1024	$3 \cdot 10^7$
2048	$4 \cdot 10^{14}$

Pretty Good Privacy

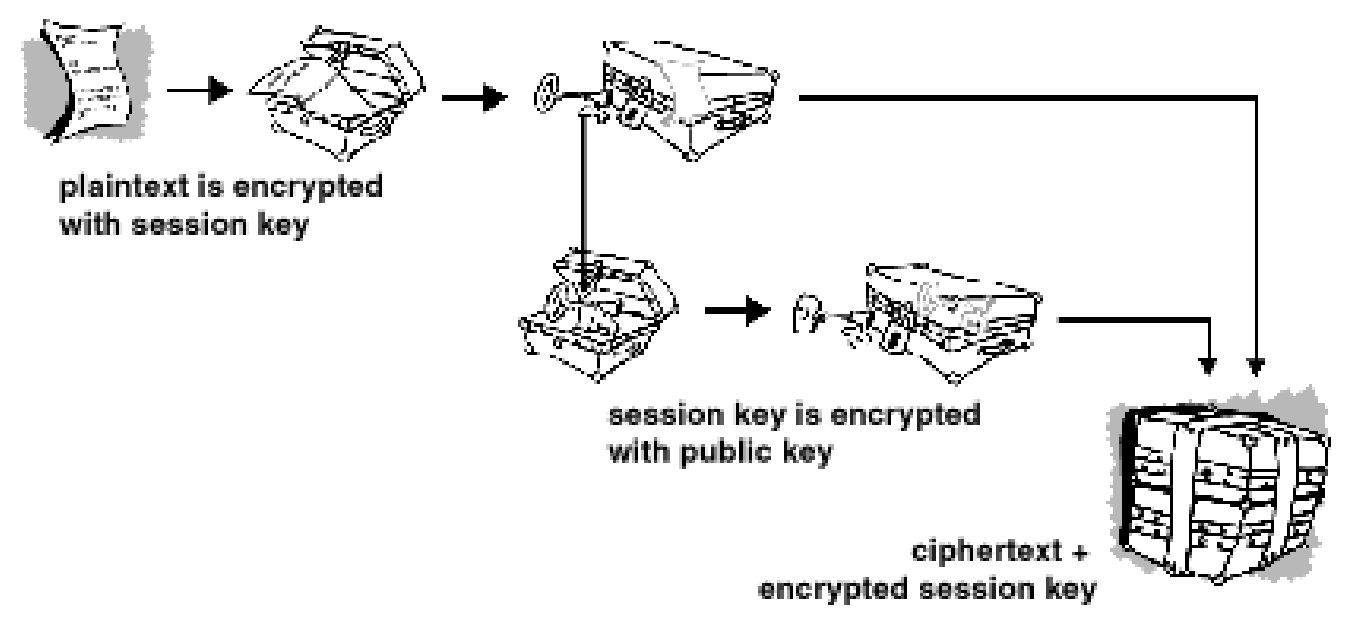
Подпись



Вычисление хэша (MD5, SHA1/2, RIPEMD) $\rightarrow$ Подпись хэша (дополнение PKCS1 v1.5) (RSA, DSA)

Pretty Good Privacy

Шифрование



Подпись → Компрессия (zlib, bzip2) → Генерирование ключа сессионного эфемерного (EGD, /dev/random) → Шифрование открытого текста и подписи (CFB режим, нулевой IV) (AES, Twofish, IDEA, CAST5) → Шифрование ключа (дополнение PKCS1 v1.5) (RSA, ElGamal)

Вопросы?