Шифрование

Криптосистема — {шифрование, дешифрация}

Секретный ключ - параметр алгоритма шифрования

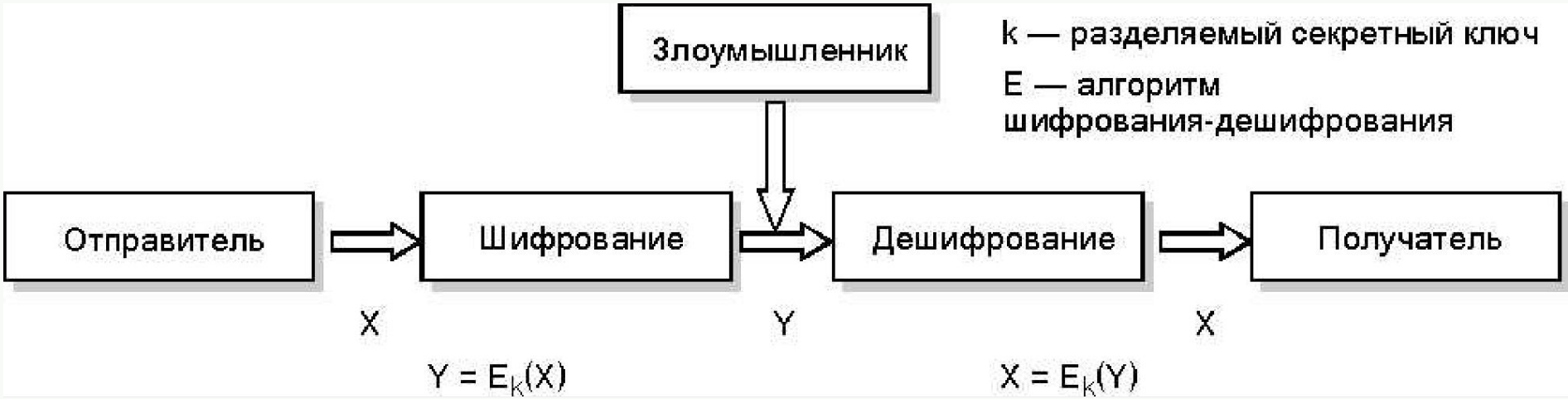
ПРАВИЛО КЕРКХОФФА
стойкость шифра должна определяться только секретностью ключа

Два типа криптосистем:

(1) симметричные

(2) асимметричные

Симметричное шифрование



в 1949 г. Клод Шеннон

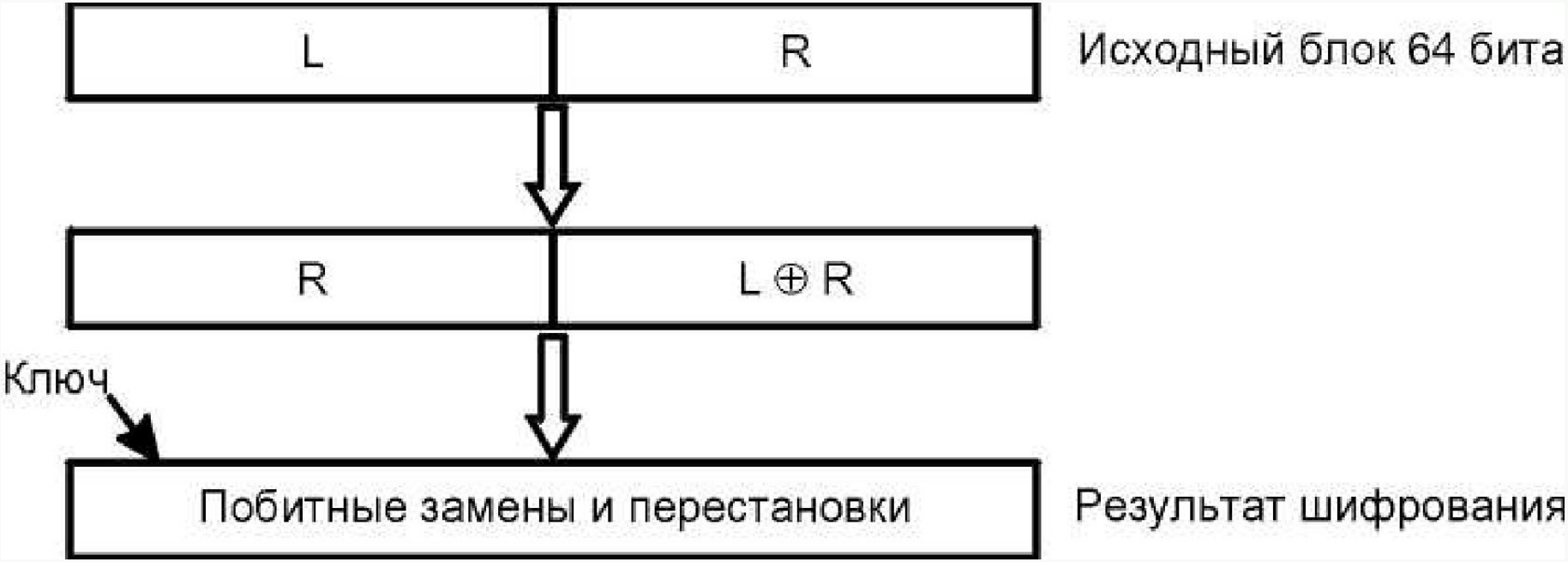
Недостатки симметричного шифрования

- Критичны к надежности канала передачи ключа
- Плохая масштабируемость схемы распределения ключей. Требуется n(n-1)/2 ключей
- Проблема генерации криптостойких ключей (56 бит)

Концепция шифрования по алгоритму DES

DES (Data Encryption Standard)

Алгоритм разработан фирмой IBM в 1976



Triple DES (112 бит) – менее производительный

Недостатки DES

- Диффи и Хеллман в 1977 году описали машину, способную за один день подобрать ключ DES. Стоимость оценивалась в 20 млн. долл.
- К началу 1990-х годов прогнозируемые затраты на создание машины, способной взломать DES, снизились в десять раз.
- В 1997 году группа из нескольких тысяч добровольцев, работавших параллельно в течение нескольких месяцев, расшифровала сообщение, закодированное с помощью DES.
- В 1998 году была представлена работоспособная машина ($210 000) для взлома DES. Она способна в среднем расшифровывать один ключ DES каждые 4,5 дня.

Advanced Encryption Standard (AES)

Новый стандарт

- **лучшее сочетание безопасности и скорости, чем у DES**
- **128-разрядные ключи, может поддерживать 192- и 256-разрядные ключи (vs 56 DES).**
- **за каждый цикл кодирует блок 128 бит (vs 64 DES)**
- **получит статус федерального стандарта по обработке информации летом 2001 года**

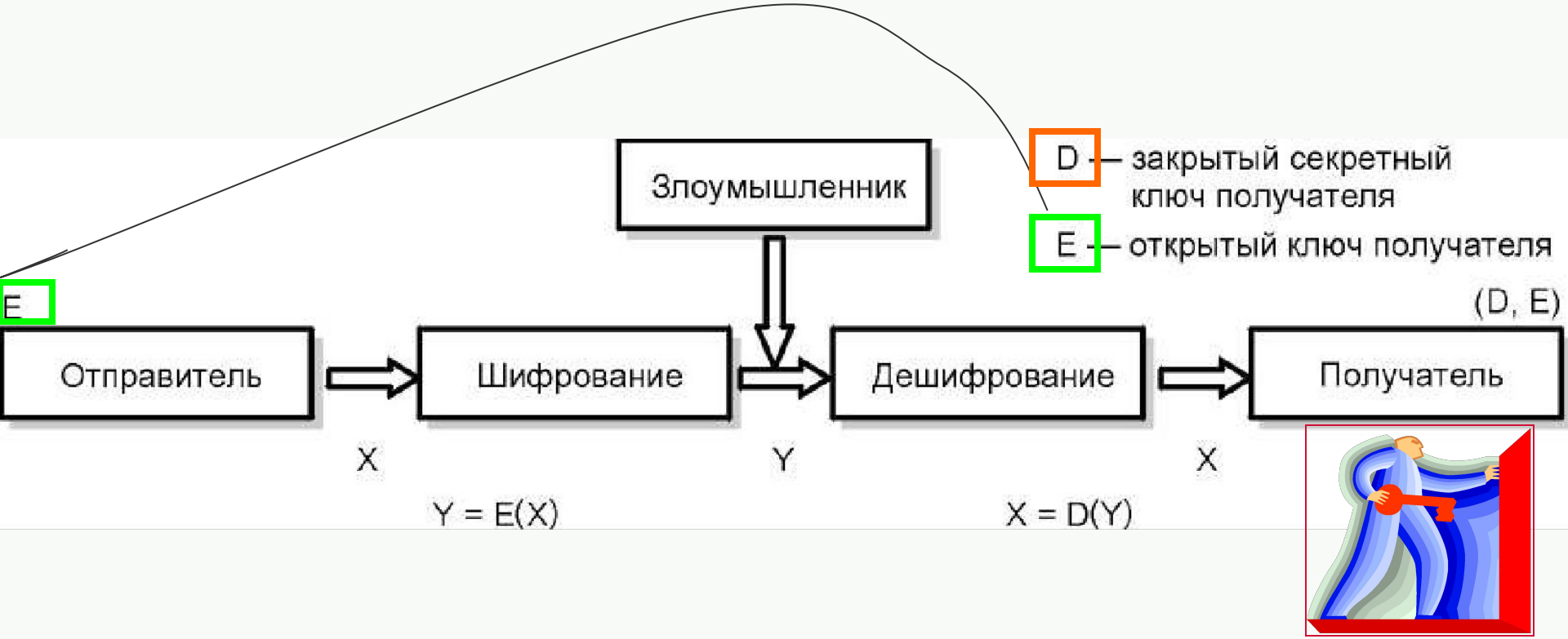
Процесс перехода:

(1) прост для настраиваемых продуктов

(2) проблемы с унаследованными алгоритмами шифрования (в браузерах – RC4, в электронной почте PGP – IEDA)

Несимметричное шифрование

В середине 70-х—Диффи и Хеллман



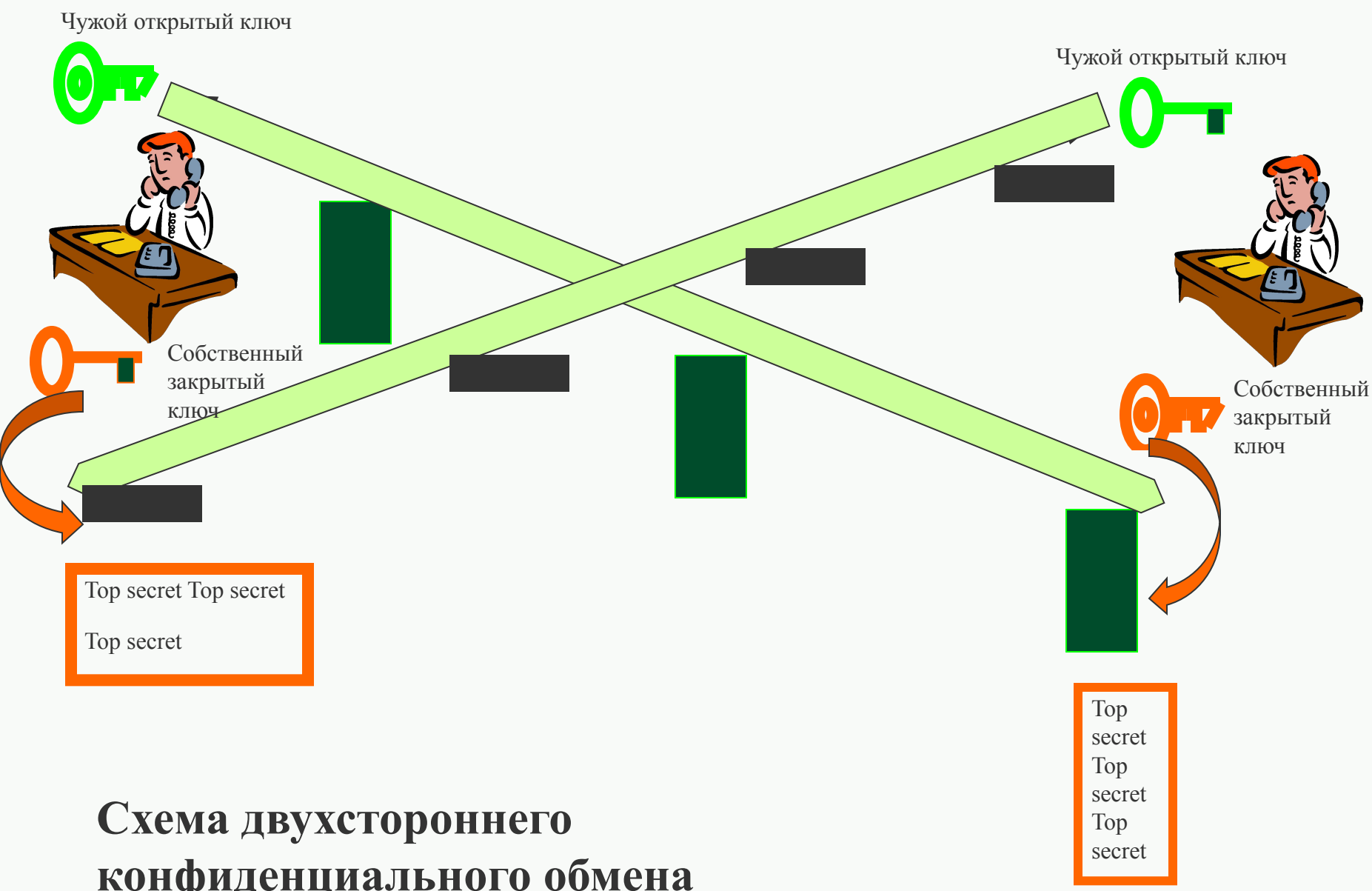


Схема двухстороннего конфиденциального обмена

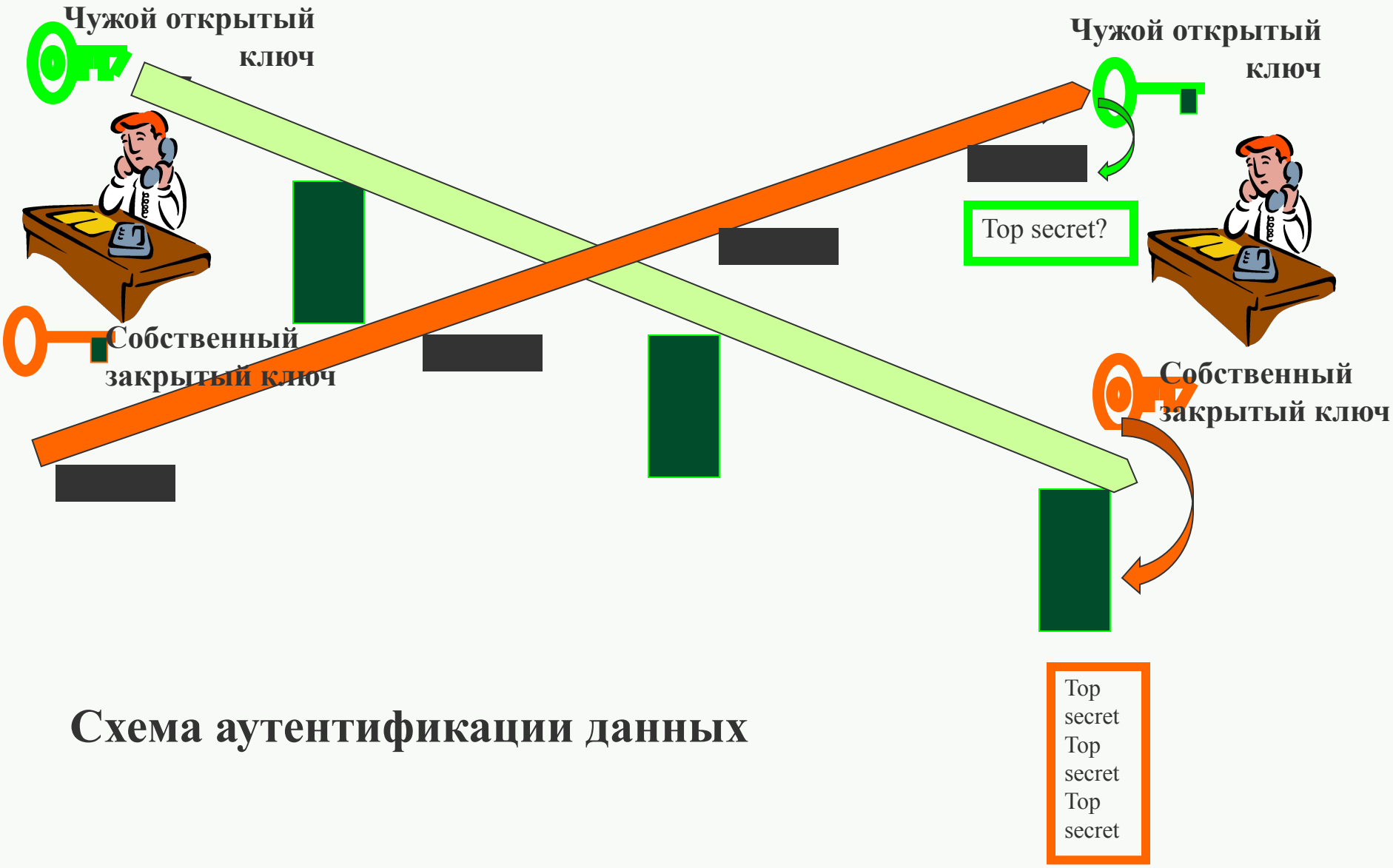
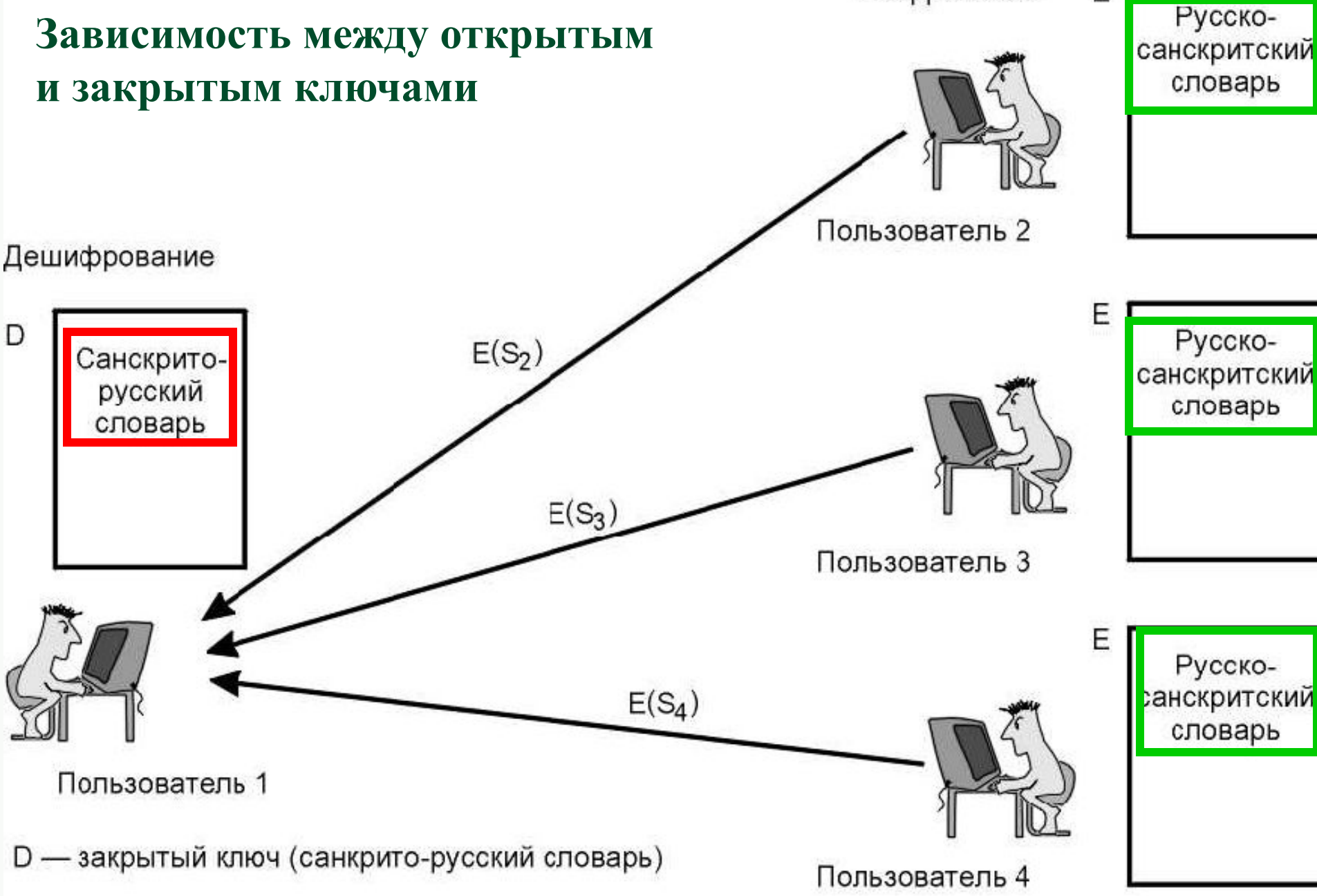


Схема аутентификации данных

Аутентификация сообщения (электронная подпись)

Односторонний конфиденциальный обмен сообщениями

Зависимость между открытым и закрытым ключами



а

Криптоалгоритм RSA

В 1978 г. Rivest, Shamir, Adleman (RSA) разработали метод на основе принципов Диффи-Хеллмана

1. случайно выбираются два очень больших простых числа p и q
2. вычисляются два произведения $n=p \cdot q$ и $m=(p-1) \cdot (q-1)$
3. выбирается случайное число E, не имеющее общих сомножителей с m 
4. находится D такое, что $DE=1$ по модулю m 
5. исходный текст, X, разбивается на блоки $0<X<n$
6. Для шифрования сообщения вычисляется $C=X^E$ по модулю n
7. Для дешифрирования вычисляется $X= C^D$ по модулю n

Для того,
чтобы найти разложение
200-
значного десятичного числа
понадобится
4
миллиарда лет работы
компьютера с быстродействием
1

Недостатки асимметричного подхода

- Более медленная генерация ключей и более длительное шифрование
- Проблема подмены открытых ключей

Достоинства

Более масштабируемый – количество ключей зависит **линейно** от числа пользователей – 2n

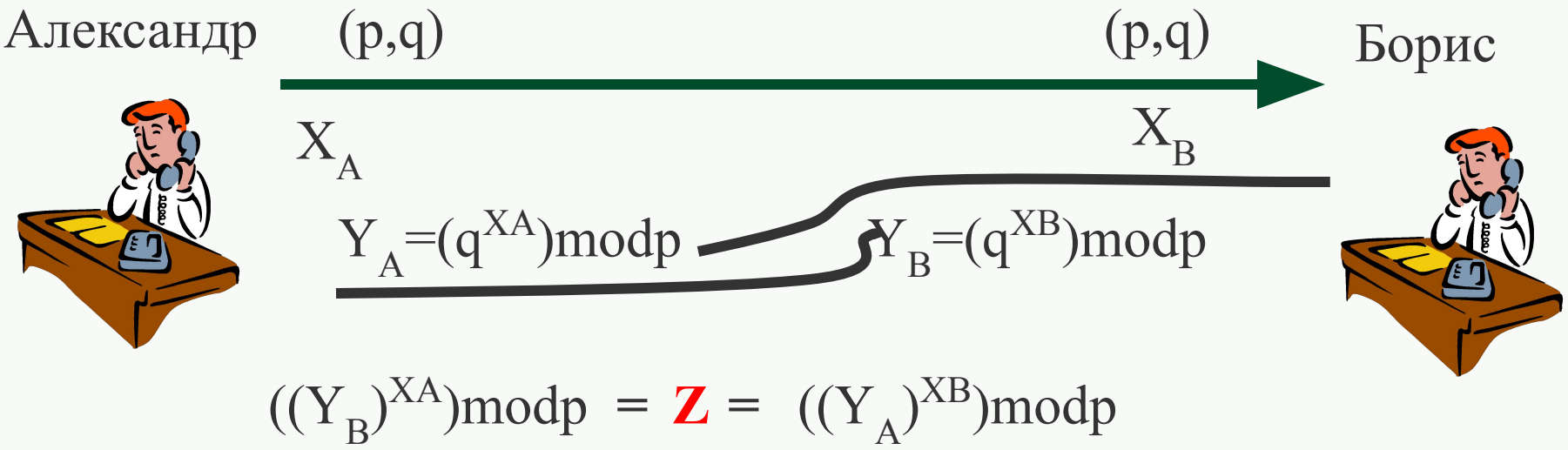
Сравнительные характеристики криптоалгоритмов DES и RSA

Характеристика	DES	RSA
Скорость шифрования	высокая	низкая
Используемая функция при шифрации	перестановка и подстановка	возведение в степень
Длина ключа	56 бит	более 500 бит
Наименее затратный криптоанализ	перебор по всему ключевому пространству	разложение числа на простые множители
Время генерации ключа	миллисекунды	минуты
Тип ключа	симметричный	асимметричный

Комбинированное использование симметричного и асимметричного шифрования

Протокол SKIP (Simple Key management for Internet Protocol)

- IP-пакеты шифруются на основе симметричного алгоритма
- Ключи для шифрования вычисляются с использованием асимметричного алгоритма



$$((Y_B)^{XA})\text{mod}p = \mathbf{Z} = ((Y_A)^{XB})\text{mod}p$$

1. Александр генерирует два больших числа p и q, отвечающие некоторым математическим критериям и посылает их Борису.

2. Независимо друг от друга Александр и Борис выбирают по большому числу XA и XB соответственно

3. Каждый на своей стороне вычисляет значения YA и YB.

4. Александр и Борис обмениваются значениями YA и YB

5. Каждый вычисляет **разделяемый секрет Z**

$Y_1=q^{X1} \bmod p$

1 X_1,

$Y_2=q^{X2} \bmod p$

2 X_2,

p, q -

разделяемые
всеми узлами
открытые
параметры

$Y_3=q^{X3} \bmod p$

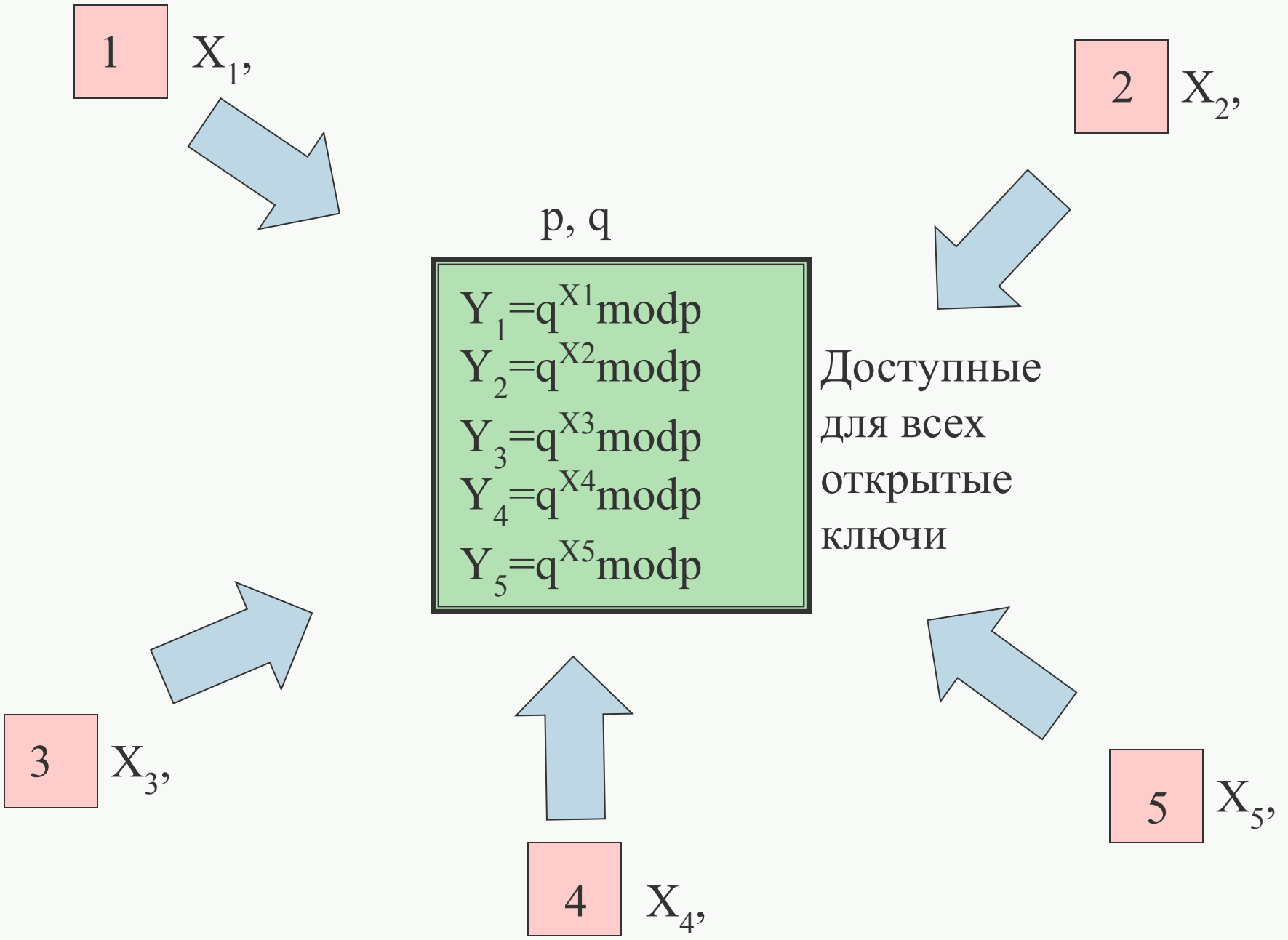
3 X_3,

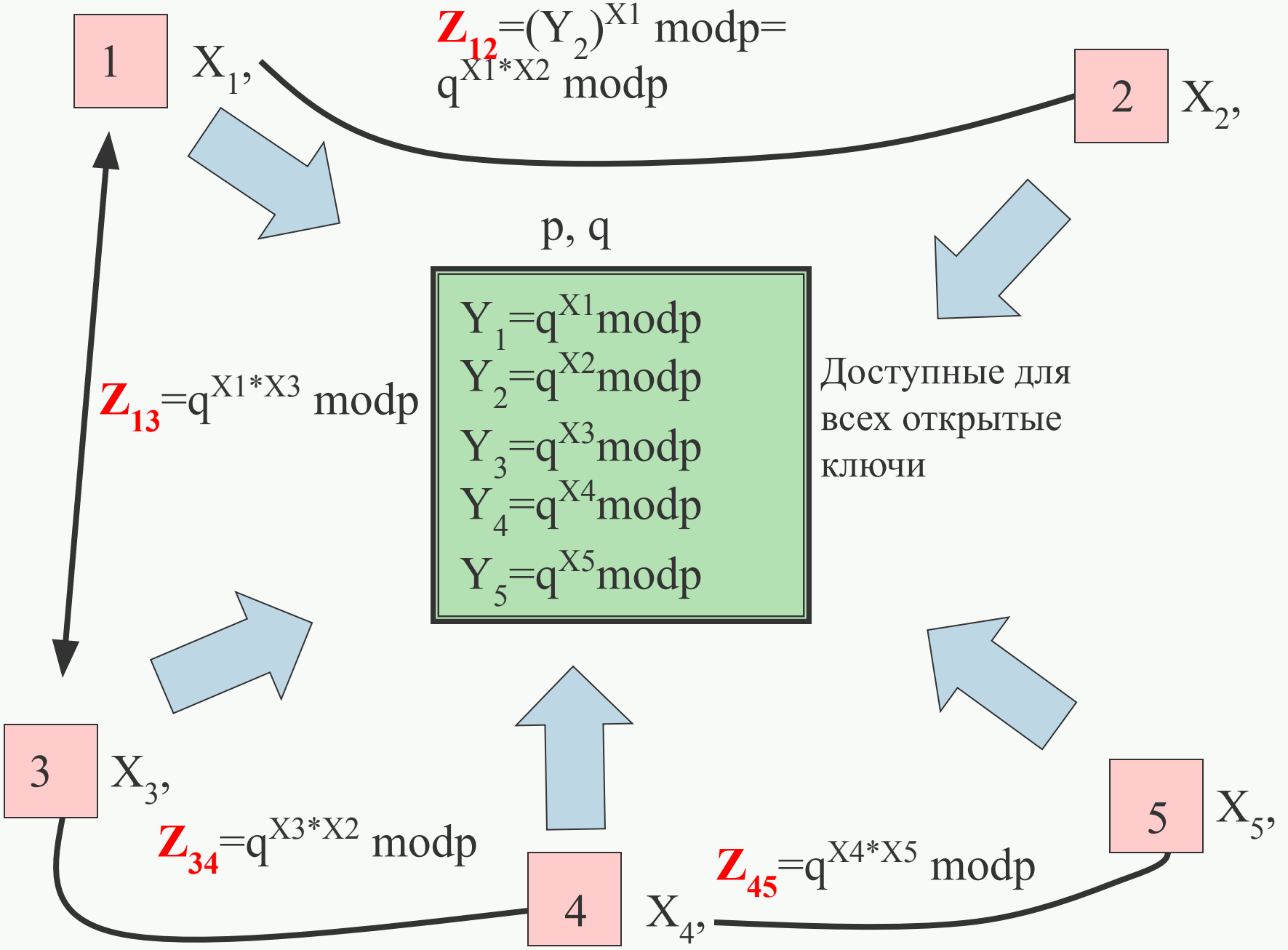
$Y_4=q^{X4} \bmod p$

4 X_4,

$Y_5=q^{X5} \bmod p$

5 X_5,


1
X_1,
2
X_2,
p, q
$Y_1=q^{X1}\text{mod}p$
$Y_2=q^{X2}\text{mod}p$
$Y_3=q^{X3}\text{mod}p$
$Y_4=q^{X4}\text{mod}p$
$Y_5=q^{X5}\text{mod}p$
Доступные для всех открытые ключи
3
X_3,
4
X_4,
5
X_5,

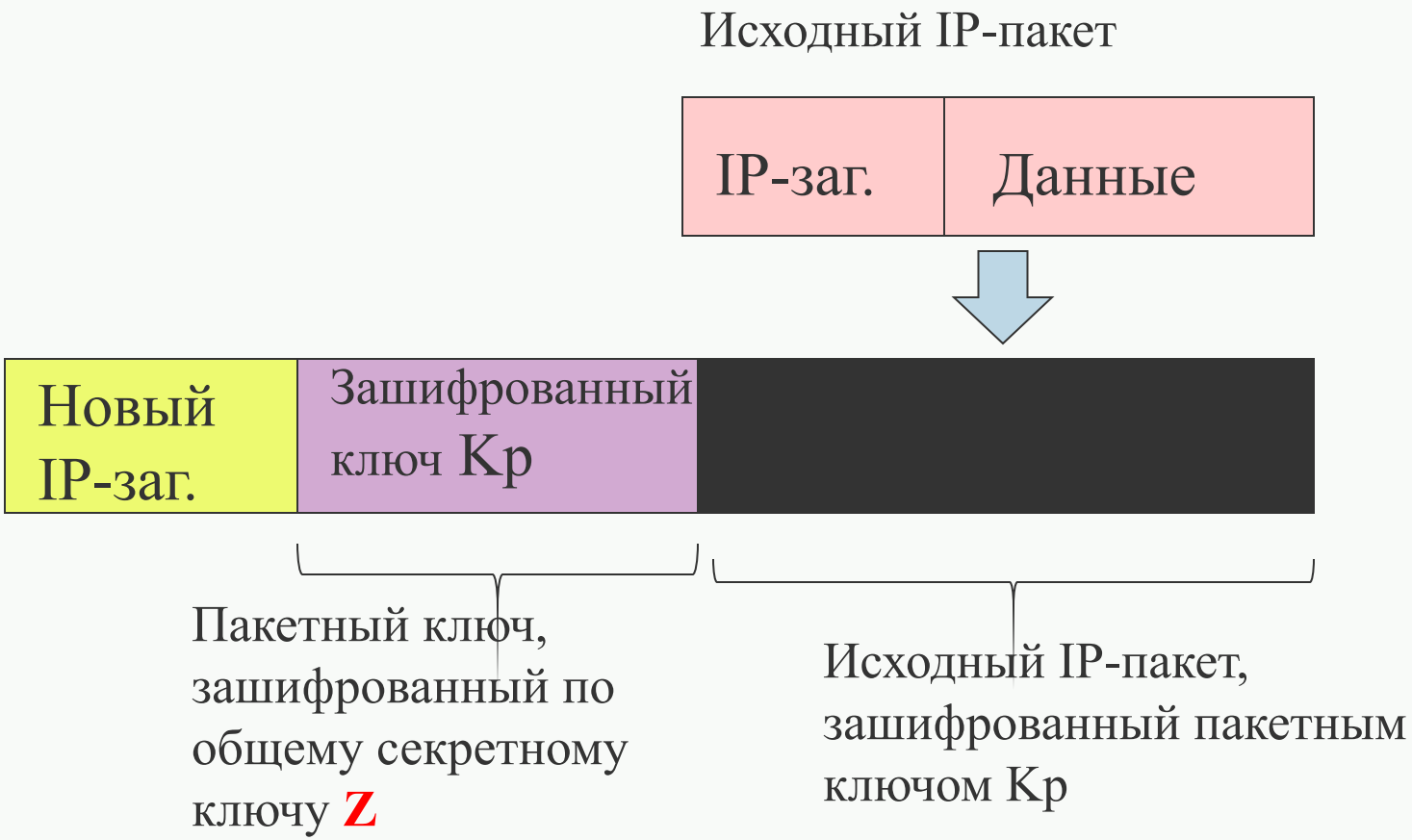

1
X_1,
$Z_{12}=(Y_2)^{X1}$ modp=
q^{X1*X2} modp
2
X_2,
p, q
$Y_1=q^{X1}$modp
$Y_2=q^{X2}$modp
$Y_3=q^{X3}$modp
$Y_4=q^{X4}$modp
$Y_5=q^{X5}$modp
Доступные для всех открытые ключи
$Z_{13}=q^{X1*X3}$ modp
3
X_3,
$Z_{34}=q^{X3*X2}$ modp
4
X_4,
$Z_{45}=q^{X4*X5}$ modp
5
X_5,

Комбинированное использование симметричного и асимметричного шифрования

Протокол SKIP (Simple Key management for Internet Protocol)

- IP-пакеты шифруются на основе симметричного алгоритма
- Ключи для шифрования вычисляются с использованием асимметричного алгоритма

Формат пакета SKIP

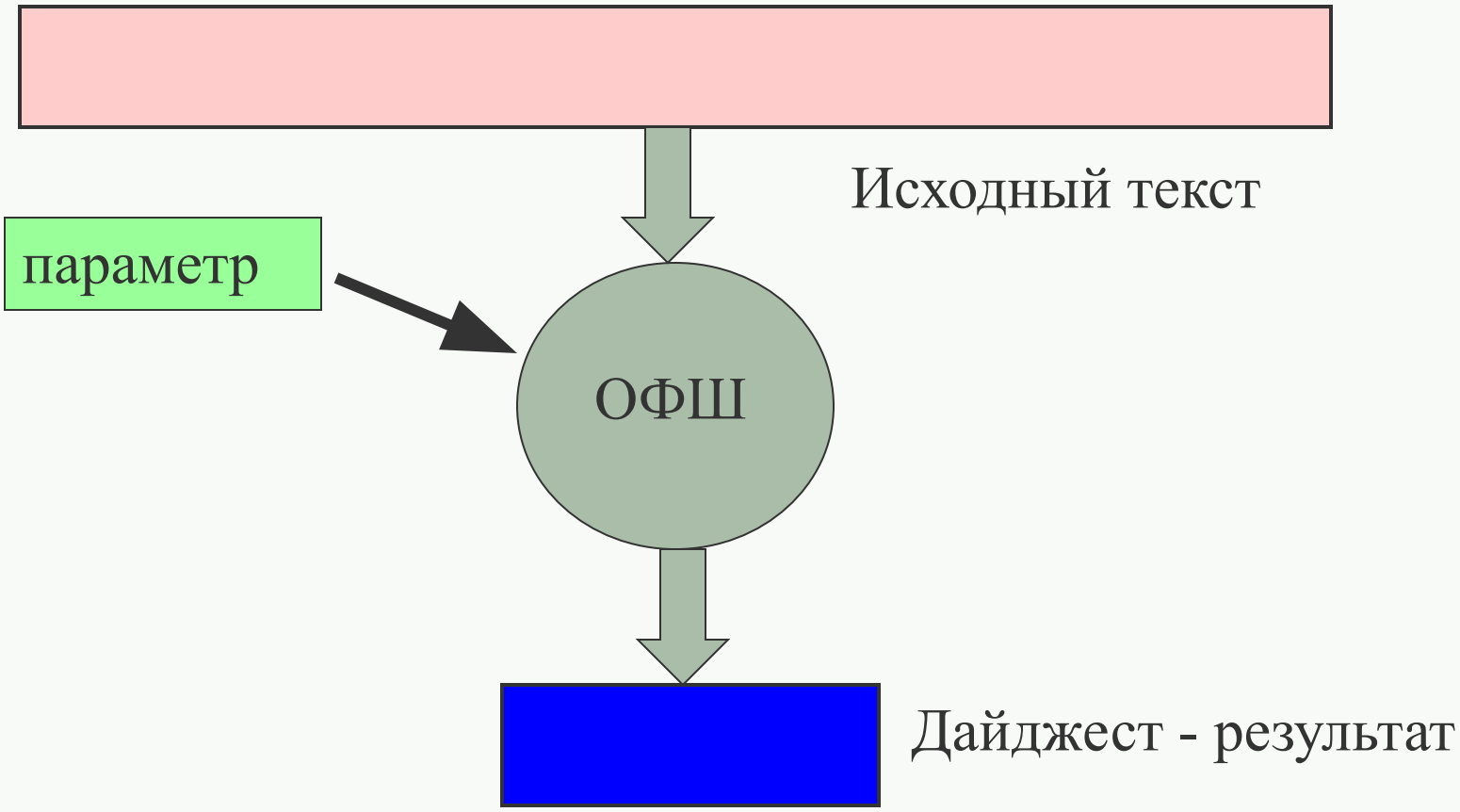


Односторонние функции шифрования

(ОФШ) (one-way function)

хэш-функции (hash function)

дайджест-функции (digest function)



Требование к односторонним функциям:

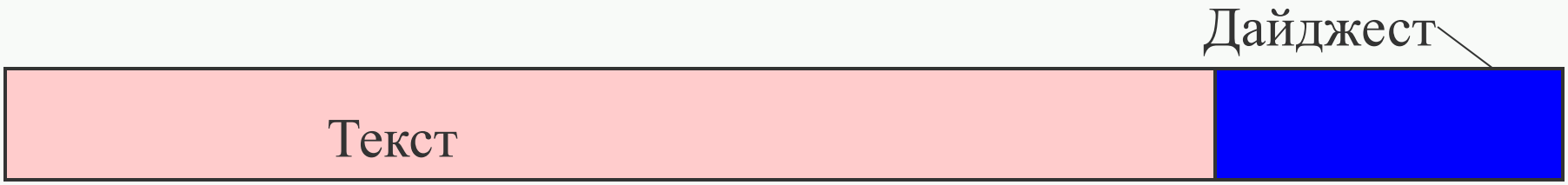
- по дайджесту, вычисленному с помощью данной функции, невозможно каким-либо образом вычислить исходное сообщение

Наиболее популярные хэш-функции:

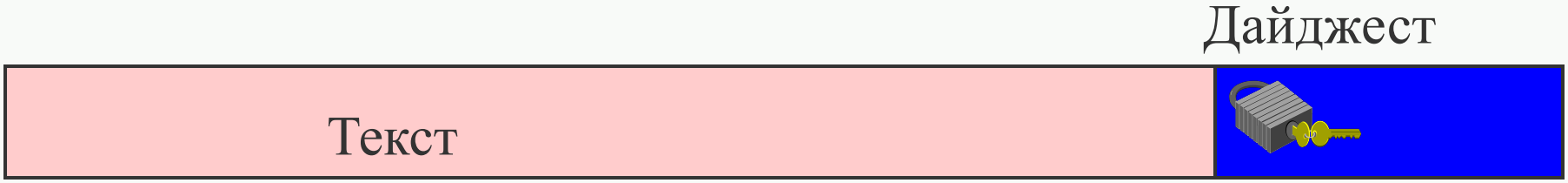
- **MD2, MD4, MD5** - дайджесты фиксированной длины 16 байт
- **SHA** - американский стандарт, адаптированный вариант MD4, длина дайджеста 20 байт
- **MDC2 MDC4** - IBM

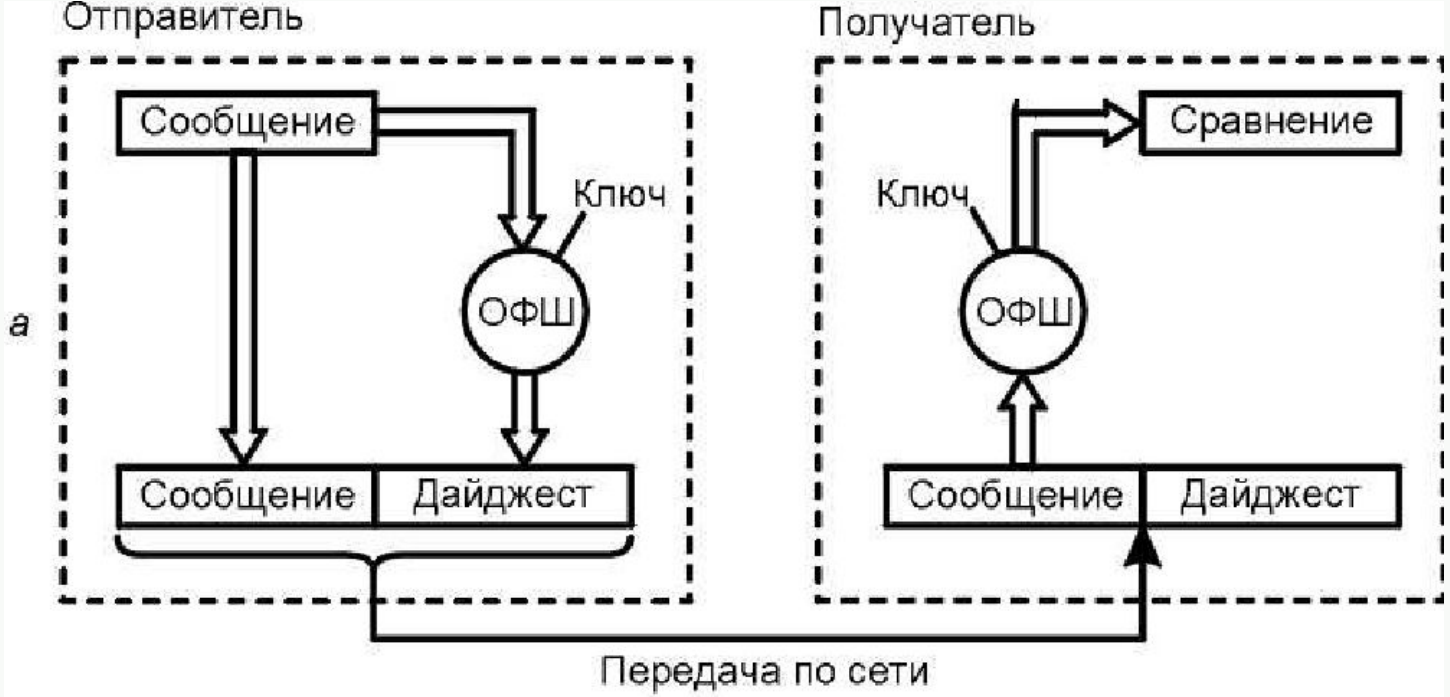
Назначение односторонних функций шифрации

(1) контроль целостности

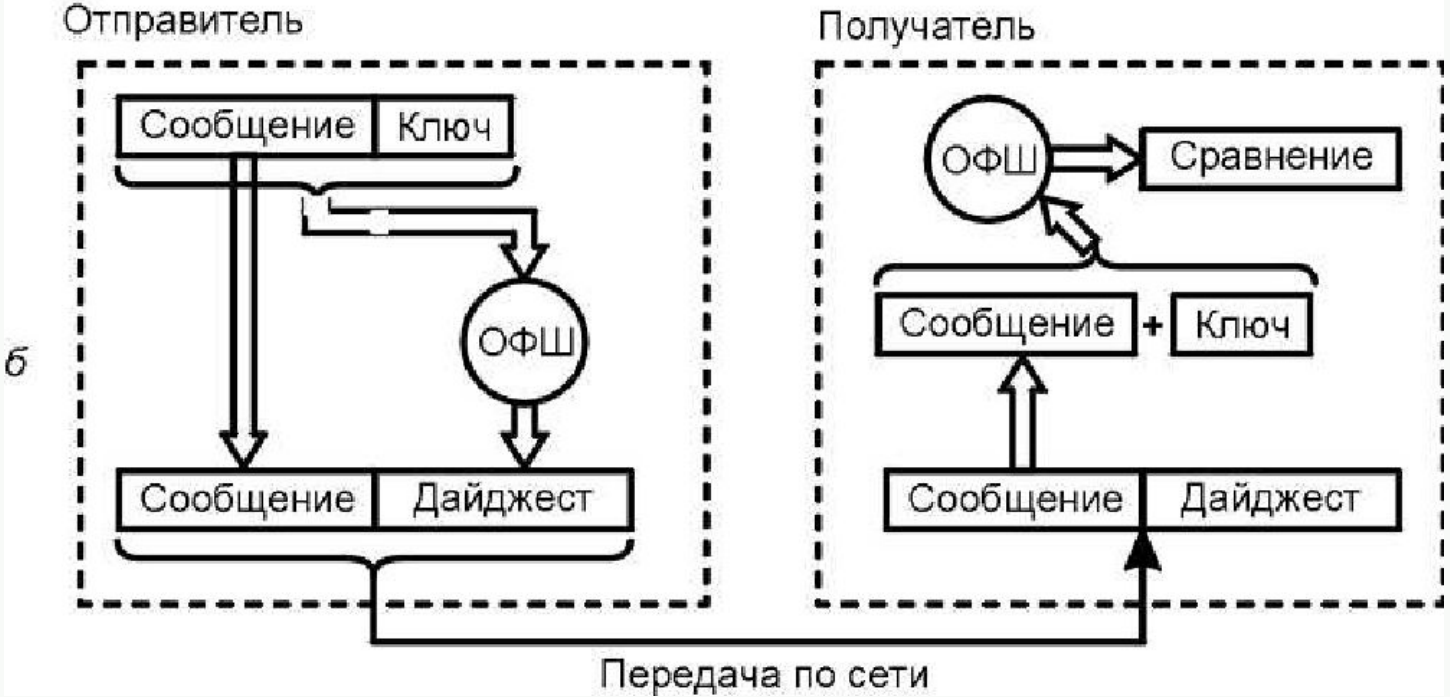


(2) контроль аутентичности




Отправитель
Получатель
Сообщение
Ключ
ОФШ
Сообщение
Дайджест
Ключ
Сравнение
ОФШ
Сообщение
Дайджест
Передача по сети

а


Отправитель
Получатель
Сообщение
Ключ
ОФШ
Сообщение
Дайджест
ОФШ
Сравнение
Сообщение
+
Ключ
Сообщение
Дайджест
Передача по сети

б