

# Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

# Раздел 13 - Асимметричные криптосистемы

Общий вид

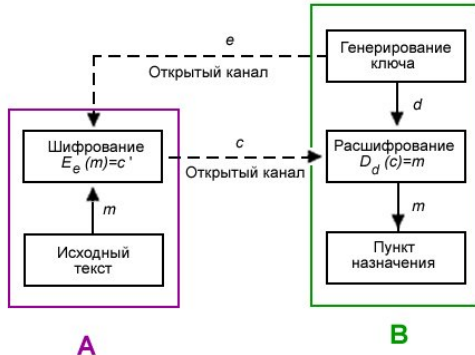
Перестановка RSA

Атаки на RSA

PKCS 1

Шифр Эль-Гамаль

## Общий вид криптосистемы с открытым ключом.



Замеч.: в таком виде уязвима к атаке Man-in-the-Middle, если зл-к встраивается в канал на этапе передачи открытого ключа, и открытый ключ нельзя проверить в обход зл-ка. (Hash, ЭЦП.)

Т.е. есть проблема - управление откp. ключами. (public key management)

Опр.

Асимм.  $\kappa/c$  - это тройка алгоритмов  $G, E, D$ :

$G(\cdot)$  - рандомизированный генератор пары ключей (открытый ключ, закрытый ключ - public key, secret key). Принимает *seed* - начальное значение.

$E(\cdot, \cdot)$  - рандомизир. алгоритм шифрования.  $c = E(pk, m)$

$D(\cdot, \cdot)$  - детерм. алгоритм расшифрования.  $m = D(sk, c)$

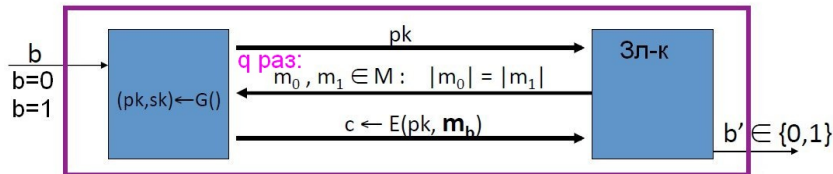
Для пары  $(pk, sk)$ , созданной  $G()$ , верно  $D(sk, E(pk, m)) = m$

Односторонняя функция (one-way function, OWF).

Односторонняя функция с секретом.

Существование односторонних функций до сих пор не доказано. Существует несколько функций, для которых не известно эффективного алгоритма вычисления обратной функции. (Но для большинства - не доказано, что их нет!)  
На них основываются методы асимметричной криптографии.

## Стойкость против подслушивания



Зл-к возвращает значение  $b'$ , пытается угадать значение  $b$ .

Опр.

$S = (G, E, D)$  семантически стойкая к атаке с выбранным открытым текстом (semantic security), если для  $\forall A \in \mathcal{PP}$

$$Adv_{CPA}(A, S) := |P(b' = 1 | b = 0) - P(b' = 1 | b = 1)| < \varepsilon(n)$$

## Сравнение с симм. к/с.

В симм. к/с зл-к не знал ключ и не мог сам строить ш/т по открытому тексту.

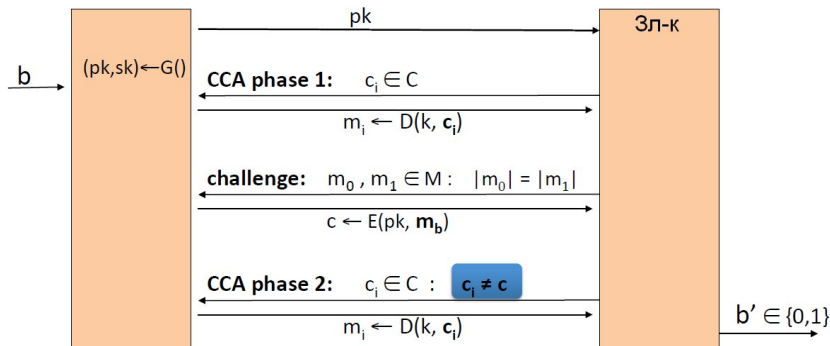
В асимм. к/с зл-к знает открытый ключ и может созд. любое кол-во ш/т для любых исходных текстов, даже если ключ “одноразовый”.

Поэтому для асимм. к/с не различаем случаи с одноразовым ключом и многоразовым ключом.

Из стойкости для однораз. ключа  $\Rightarrow$  стойкость для многораз. ключа.

Асимм. шифрование обязано быть рандомизированным.

## Стойкость против активных атак



Опр.

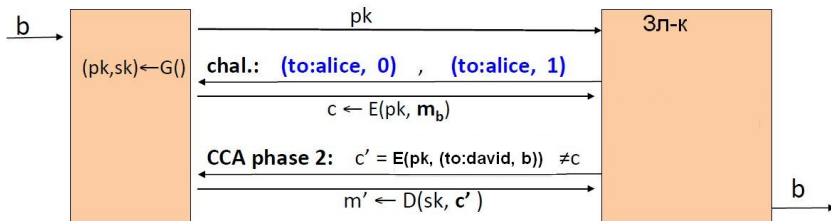
$S = (G, E, D)$  семантически стойкая к атаке с выбранным шифротекстом, если  $\forall A \in PP$

$$Adv_{CCA}(A, S) = |P(b' = 1 | b = 0) - P(b' = 1 | b = 1)| < \varepsilon(n)$$



## Пример

Пусть мы можем воздействовать на шифротекст:  
контролируемо подменять часть сообщения. Тогда не будет  
стойк. к атаке с выбр. шифротекстом: зл-к узнает, чему равно  
 $b$ .



## Активные атаки: сравнение с симм. к/с.

Симм. к/с:

стойкий шифр - заверенное шифрование

(стойкость к атаке с выбранным открытым текстом и целостность ш/т).

Т.е. зл-к не может создавать новые шифротексты, которые будут приняты.

Асимм. к/с:

Зл-к может создавать новые ш/т, которые будут приняты.

Поэтому непосредственно требуем стойкость к атаке с выбранным ш/т.

## Перестановка с секретом

Опр.

Три алгоритма  $(G(), F(\cdot, \cdot), F'(\cdot, \cdot))$  определяют перестановку с секретом, если

$G()$  выдает пары  $pk, sk$  - открытый ключ, закрытый ключ.

$F(pk, \cdot) : X \rightarrow X$ .

$F'(sk, y)$  - функция  $F^{-1}(pk, \cdot)$ :  
если  $y = F(pk, x)$ , то  $F'(sk, y) = x$ .

Опр.

Если ф-ция  $F(pk, \cdot) : X \rightarrow X$  - односторонняя ф-ция при неизв.  $sk$ ,

то  $(G(), F(\cdot, \cdot), F'(\cdot, \cdot))$  определяет *стойкую перестановку с секретом* (secure trapdoor permutation).

# Раздел 13 - Асимметричные криптосистемы

Общий вид

Перестановка RSA

Атаки на RSA

PKCS 1

Шифр Эль-Гамаль

## Перестановка RSA - “RSA из учебника”.

1977, Rivest, Shamir, Adleman.

Основана на выч-но трудной задаче: разл. на мн-ли.

### Генерация ключей

1) Выбир. любые  $p, q$  - большие простые числа, например, 128-битовые. Держим их в секрете.

2)  $N := pq$

3)  $\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$  - невозм. быстро вычислить, не зная  $p, q$

4) Выбир.  $\forall e > 1 : \text{НОД}(e, \varphi(N)) = 1$ . Число  $e$  - “небольшое” и с малым числом единичных битов (это ускоряет вычисления - можно польз. сдвигами). Например,  $e = 0x100001$  или  $e = 2^{16} + 1$  - простые числа.

5)  $d = e^{-1} \bmod(\varphi(N))$  с пом. *ExtGCD*.

Число  $N$  наз. "модулем"

Число  $e$  - открытая экспонента,  $d$  - закрытая экспонента

Пара  $(N, e)$  - откp. ключ (public key),  $(N, d)$  - закрытый ключ (private key).

Числа  $p, q$  больше не нужны, но они секретные.

## Шифрование

Сообщение - на части, часть  $\leftrightarrow$  число  $m$ ,  $0 < m < N$ .

$$c := m^e \bmod N$$

## Расшифрование

$$c^d = m^{ed} \bmod N = m^{k\varphi(n)+1} \bmod N \stackrel{(*)}{=} m \bmod N \text{ (т. Эйлера)}$$

( $*$ ): с вероятностью порядка

$1 - 2/\min(p, q) \approx 1 - 2^{-\text{len}(\min(p, q))}$ , число  $m$  не кратно  $p$  или  $q$ .

Если  $m$  не вз. простое с  $N$ ? Вер-ть этого  $\approx 2^{-\text{len}(\min(p, q))}$  - никогда не случится. Это будет замечено, можно попросить изменить  $m$  и переслать.

## Пример

$p = 11$ ,  $q = 17$ ,  $N = 187$ .  $e$  не должно иметь общих дел-й с  $10 * 16 = 160$ . Пусть  $e = 9$ .

Тогда  $d = 9^{-1} \bmod 160 = 89$  (*ExtGCD*)

Пусть  $m = 688232$ .  $m_1 = 68$ ,  $m_2 = 82$ ,  $m_3 = 32$ .

Зашифрование:  $c_1 = 68^9 \bmod 187 = 17$ .

Расшифрование:  $17^{89} \bmod 187 = 68 = m_1$ .



Уязвимость перестановки RSA:

- не обесп. семантическую стойкость шифрования к атаке с выбранным открытым текстом (детерминированное шифр-е);

Является ли перестановка RSA,  $m \rightarrow m^e \bmod N$ ,  
односторонней функцией?

Пусть  $d$  не изв.; известно  $c = x^e$ ;  
требуется найти  $x = c^{1/e}$  в  $\mathbb{Z}_N$ , вычислив корень степени  $e$ .

Лучший известный сейчас алгоритм вычисл. корней степени  $e$   
в  $\mathbb{Z}_N$ : два шага,

- 1) разложить  $N$  на множители (сложно, субэкспоненциальный алгоритм),  $N = pq$
- 2) вычисл. корни степ.  $e$  по модулю простых  $p$  и  $q$  (полин. алгоритм).

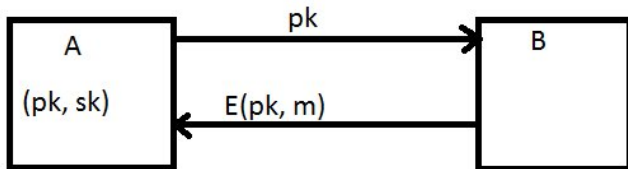
Можно ли проще? Не известно.

Субэкспоненциальная сложность взлома, поэтому асимм. к/с при той же стойкости имеет более длинный ключ и медленнее, чем симм. к/с.

Использование асимм. к/с:

1) инициализация сессии, создание общего ключа для симм. шифра

2) односторонняя коммуникация, напр. e-mail.



# Раздел 13 - Асимметричные криптосистемы

Общий вид

Перестановка RSA

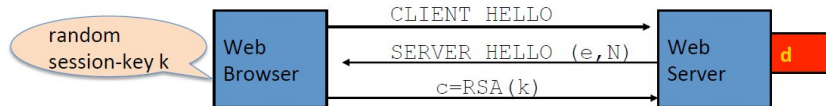
Атаки на RSA

PKCS 1

Шифр Эль-Гамаль

## Атака 1 на перестановку RSA - а-ля “встреча посередине”.

Типично: асимметричное шифрование исп. для создания общего ключа для сессии, в которой будет исп. симметричное шифрование.



Длина ключа  $k$  для симм. шифра небольшая. Пусть это 64 бита. Зл-к видит  $c = k^e \in \mathbb{Z}_N$ .

Если  $k$  можно предст. в виде  $k = k_1 \cdot k_2$ ,  $0 < k_1, k_2 < 2^{34}$  (это произойдет с вер-ю ок. 0.35 для  $k$  длины 64 бита), то  $c/(k_1)^e = (k_2)^e$ .

## Атака:

1) постр. таблицу:  $c/1^e$ ,  $c/2^e$ ,  $c/3^e$ , ...  $c/(2^{34})^e$  - треб. время пропорц.  $2^{34}$  и память  $2^{34} \cdot 34$ .

2) для  $k_2 = 0, \dots, 2^{34}$  попробовать найти  $(k_2)^e$  в таблице - треб.  $2^{34}$  операций поиска, т.е. время пропорц.  $2^{34} \cdot \log_2(2^{34})$ .

Если нашли, то выдать пару  $(k_1, k_2)$ ;  $k := k_1 \cdot k_2$ . Найден ключ  $k$ , который будет исп. в симметричном шифре.

Общее время  $\approx 2^{40} \ll 2^{64}$ .

## Атака 2 на перестановку RSA с малым $d$

Большое  $d$  - долго расшифровывать. Уменьшим его?

Атака Wiener'a:  $d < N^{0.25} \Rightarrow$  можно найти  $d$  по  $(N, e)$ .

RSA: малая публичная экспонента - быстрое шифрование. Рек.  
 $e = 2^{16} + 1$  - простое. Шифр-е - 17 умножений по модулю.

### Атака 3 при одинаковой публичной экспоненте $e = 3$

$e = 3$ .

3 получателя:  $(N_1, e), (N_2, e), (N_3, e)$ .  $m \rightarrow c_1, c_2, c_3$ .

$N := N_1 N_2 N_3$ ,  $N_i$  вз. простые.

Обозн.  $c = m^3 < N$ .

$\Rightarrow \exists! c \in \mathbb{Z}_N : c = c_i \bmod N_i$

$\Rightarrow m = c^{1/3}$  - как числа, не по модулю.

Защита:

а) для атаки нужно  $e$  получателей:  $c < N$ . Не исп.  $e = 3$ .

б) рандомизация шифрования (см. напр. PKCS 1)



**Атака 4 на RSA с общим модулем**  
( $N, e_i, d_i$ ). Пусть  $e_i$  вз. простые.

$$c_1 = m^{e_1} \bmod n$$

$$c_2 = m^{e_2} \bmod n$$

$\text{НОД}(e_1, e_2) = 1$ , поэтому  $\text{ExtGCD} \Rightarrow e'_1, e'_2 : e_1 e'_1 + e_2 e'_2 = 1$ .

Очев, одно из  $e'_1, e'_2$  отрицательное. Пусть это  $e'_1$ .  
Тогда выч.  $c_1^{-1} \bmod n$  ( $\text{ExtGCD}$ ).

$$(c_1^{-1})^{-e'_1} * c_2^{e'_2} = m^{e_1 e'_1 + e_2 e'_2} = m \bmod n$$

Защита: не использовать общий модуль.

## Атака 5: проблема малой энтропии

```
prng.seed(seed)
p = prng.generate_random_prime()
prng.add_randomness(bits)
q = prng.generate_random_prime()
N = p*q
```

Малая начальная энтропия  $\Rightarrow$  одинаковые  $p$ .

Тогда  $\text{НОД}(N_1, N_2) = p$ .

Так факторизуется 0.4% от взятых в сети публичных ключей!

## Атака 6 по побочным каналам

- время или график мощности при вычислении  $c^d \bmod N$ .
- ЭМИ  $\Rightarrow$  ошибка при вычислении  $c^d \bmod N$ .

Любое из них позволит узнать  $d$ .

# Раздел 13 - Асимметричные криптосистемы

Общий вид

Перестановка RSA

Атаки на RSA

PKCS 1

Шифр Эль-Гамаль

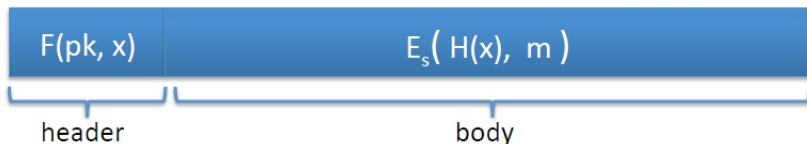
## Первая стойкая к атакам асимм. к/с

- $(G, F, F^{-1})$  - односторонняя функция с секретом,  $X \rightarrow Y$ .
- $H : X \rightarrow K$  - криптографическая х/ф
- $(E_s, D_s)$  - симметрический шифр: заверенное шифрование

Защита:  $|X|^{1/2}$  достаточно велико.

$H(x)$ : нужный размер результата и запутывание.

$E(pk, m):$ $x \xleftarrow{R} X, y := F(pk, x)$ $c := E_s(H(x), m)$ $(y, c)$	$D(sk, (y, c)):$ $x := F^{-1}(sk, y)$ $m := D_s(H(x), c)$ $m$
---	--



## Теорема 1

Если  $(G, F, F')$  - односторонняя функция с секретом,  
 $(E_S, D_S)$  обесп. заверенное шифрование

$H : X \rightarrow K$  - “случайный оракул”,

то асимм. к/с  $(G, E, D)$  стойкая к атаке с изв. шифротекстом  
(в модели со случ. оракулом).

Без док-ва.

В жизни нет “случайных оракулов”, но иначе доказать не удастся.

## Public-Key Cryptography Standard 1 (RSA) (\*)

v1.5: шифрование:  $c := \text{RSA}(pk, (02 || \text{randompad} || FF || m))$

Зачем *randompad*?

Расшифрование: расшифровать ш/т и проверить, что первые 2 байта равны 0x00 0x02. Если не равны, отправить ошибку “неверный протокол”.

Т.е. зл-к может проверять, что первые два байта после расшифровки равны 02.

Как м.б. исправить?

а) Не шифровать 02? - Примем все ш/т!

б) Не отвечать “неверный протокол” и обеспечить равное время работы.

## “The million message attack” (Bleichenbacher) (\*)

Атака с выбранным шифротекстом.

$$s \xleftarrow{R} M$$

послать  $c' = cs^e \bmod n = (ms)^e \bmod n$

если  $c'$  не отвегнут, то  $msb(ms) = 02$ .

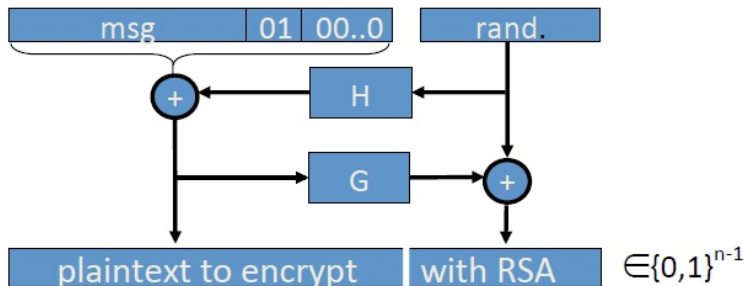
Так собираем инф-ю об  $m$ . Чтобы полностью узнать  $m$ , нужно неск. миллионов сообщений.



## PKCS1 v2.0: OAEP (\*)

Optimal Asymmetric Encryption Padding

$n := \text{len}(N)$ ;  $r \xleftarrow{R} R$ . Шифрование:  $c = \text{RSA}(f(m||pad, r))$



$G, H$  - хэш функции.

При расшифровке проверить  $pad$ . Отвергнуть ш/т, если не правильный.

(Пояснить рисунок.)

(\*)

## Теорема 2

Если RSA - односторонняя перестановка с секретом и  $G, H$  - случайные оракулы, то RSA-OAEP стойкая к атакам с выбранным шифротекстом.

Реализация расшифрования:

Так, чтобы избежать атаку по возвращаемому ответу и по времени обработки.

(Вторая стойкая к атакам асимметричная к/с)

**Сравнение длин ключей симм. и асимм. при один.  
стойкости**  
(по данным NIST)

Симм. шифр	размер модуля RSA	Порядок гр. эллипт. кривой
64	512	
80	1024	160
128	3072	256
256 (AES)	15360	512

Поэтому постеп. переход к к/с на эллипт. кривых.

# Раздел 13 - Асимметричные криптосистемы

Общий вид

Перестановка RSA

Атаки на RSA

PKCS 1

Шифр Эль-Гамаль

## Протокол шифрования Эль-Гамаль (El Gamal)

Осн. на сложности проблемы дискр. логарифмирования: по известным  $p, g, y$  найти  $x$ :  $y = g^x \bmod p$ . Субэксп. сложность.

### 1. Генерация ключей:

- выбир. группу  $G$  порядка  $q$ . Обычно  $G$  - циклическая подгруппа нек. группы  $\mathbb{Z}_p^*$  (см. далее).
- $g$  - генератор  $G$ .
- выбир. случ.  $x$ :  $1 < x < q - 1$
- выч.  $y := g^x$
- о.к. -  $(G, q, g, y)$ ; з.к. -  $x$

## 2. Шифрование. Все операции в группе $G$ .

- $m \in G$ .
- выбир. случ.  $k$ ,  $1 < k < q - 1$ . Это аналог IV, но  $k$  не передается.
- $c_1 := g^k$
- $c_2 := y^k m$
- $(c_1, c_2)$  - шифротекст, в 2 раза длиннее  $m$ .

## 3. Расшифрование:

- $m := c_2 \cdot c_1^{-x}$ .

## 4. Корректность:

- $c_2 * c_1^{-x} = y^k m \cdot c_1^{-x} = g^{kx} m g^{-kx} = m$

## Утверждение

Если в группе  $G$  дискретный логарифм - сложная задача и алгоритм шифрования не разглашает информацию об  $m$ , то шифр Эль Гамалья семантически стойкий к атаке с выбором открытого текста.

Без док-ва.

Подходит, напр., группа вычетов  $\mathbb{Z}_p^*$  по модулю надежного простого числа  $p = 2q + 1$  ( $p, q$  - простые) и выбор  $g$  из **подгруппы квадратичных вычетов** порядка  $q$ , так что  $\left(\frac{g}{p}\right) = 1$  и ограничение множества сообщений:  $\left(\frac{m}{p}\right) = 1$ .

## Утверждение

Произвольные  $\mathbb{Z}_p^*$  и  $g$  не подходят: раскрывается 1 бит инф-и об  $m$ .

## Док-во

Пусть  $g$  - генератор  $\mathbb{Z}_p^*$ . След-но  $g$  - не кв. вычет,  $\left(\frac{g}{p}\right) = -1$ .

Символ Лежандра вычисляется эффективно. Вычислим

$\left(\frac{c_1}{p}\right) = \left(\frac{g^k}{p}\right) = \left(\frac{g}{p}\right)^k$  - узнаем четность  $k$ .

Публичный ключ  $y = g^x$  - узнаем четность  $x$ .

$c_2 = g^{kx} m$ , вычислим  $l_1 = \left(\frac{c_2}{p}\right)$ .

Из предыдущих, знаем  $l_2 = \left(\frac{g^{kx}}{p}\right)$ .

Тогда узнаем  $\left(\frac{m}{p}\right) = l_1/l_2$ .

Ч.т.д.



## Литература к лекции

1. Boneh, Joux, Nguyen. "Why Textbook ElGamal and RSA Encryption Are Insecure". Параграфы 1 и 3.1.

<http://www.ssi.gouv.fr/archive/fr/sciences/fichiers/lcr/bojong00.pdf>

2\*. PKCS 1 v2.2: RSA Cryptography Standard,

<http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf>