
Криптоанализ
RSA

Пути вскрытия RSA

Полиномиально эквиваленты

1

Дано: $n, e,$

$M^e \bmod n$

Найти: M

Задача RSA

2

Факторизация модуля

n

3

Вычисление функции

$\varphi(n)$

4

Расчет закрытой экспоненты

$d = e^{-1} \bmod \varphi(n)$

Пути вскрытия RSA :

факторизация n ~ вычисление $\varphi(n)$

Как зная p и q, найти $\varphi(n)$

$n = pq$ → $\varphi(n) = (p-1)(q-1)$ →

$$\begin{cases} pq = n, \\ \varphi(n) = (p-1)(q-1) = pq - (p+q) + 1. \end{cases}$$

$$\begin{cases} pq = n, \\ p+q = n - \varphi(n) + 1, \end{cases}$$

$$x^2 - (n - \varphi(n) + 1)x + n = 0.$$

L-нотация для обозначения сложности алгоритмов факторизации чисел

$$L_N(\varepsilon, c) = e^{(c+O(1))(\log_2 N)^{\varepsilon}(\log_2 \log_2 N)^{1-\varepsilon}}$$

$\varepsilon = 0$ — **ПОЛИНОМИАЛЬНЫЙ**

Эффективны

$\varepsilon = 1$ — **ЭКСПОНЕНЦИАЛЬНЫЙ**

Не эффективны

$0 < \varepsilon < 1$ — **СУБЭКСПОНЕНЦИАЛЬНЫЙ**

Чем ближе ε к 0, тем алгоритм более эффективен

Наиболее эффективные алгоритмы факторизации

Квадратичное решето	$L_N(\frac{1}{2},1) = e^{(1+O(1))(\log_2 N \cdot \log_2 \log_2 N)^{1/2}}$
Факторизация на эллиптических кривых	$L_N(\frac{1}{2},\sqrt{2}) = e^{(1+O(1))(2\log_2 p \cdot \log_2 \log_2 p)^{1/2}}$ p – наименьший множитель числа N
Общий метод решета числового поля	$L_N(\frac{1}{3},\sqrt[3]{\frac{64}{9}}) = e^{(1{,}92+O(1))(\log_2 N^{1/3} \cdot \log_2 \log_2 N)^{2/3}}$

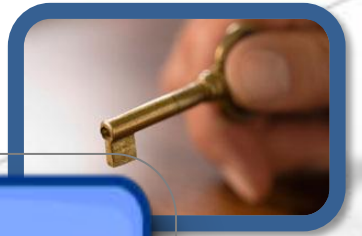
Последние результаты факторизации больших чисел

Factorization of a 768-bit RSA modulus

version 1.4, February 18, 2010

решето числового поля

Thorsten Kleinjung ,
Kazumaro Aoki , Jens Franke , Arjen K. Lenstra , Emmanuel Thomé ,
Joppe W. Bos , Pierrick Gaudry , Alexander Kruppa , Peter L. Montgomery,
Dag Arne Osvik , Herman te Riele, Andrey Timofeev, and Paul Zimmermann

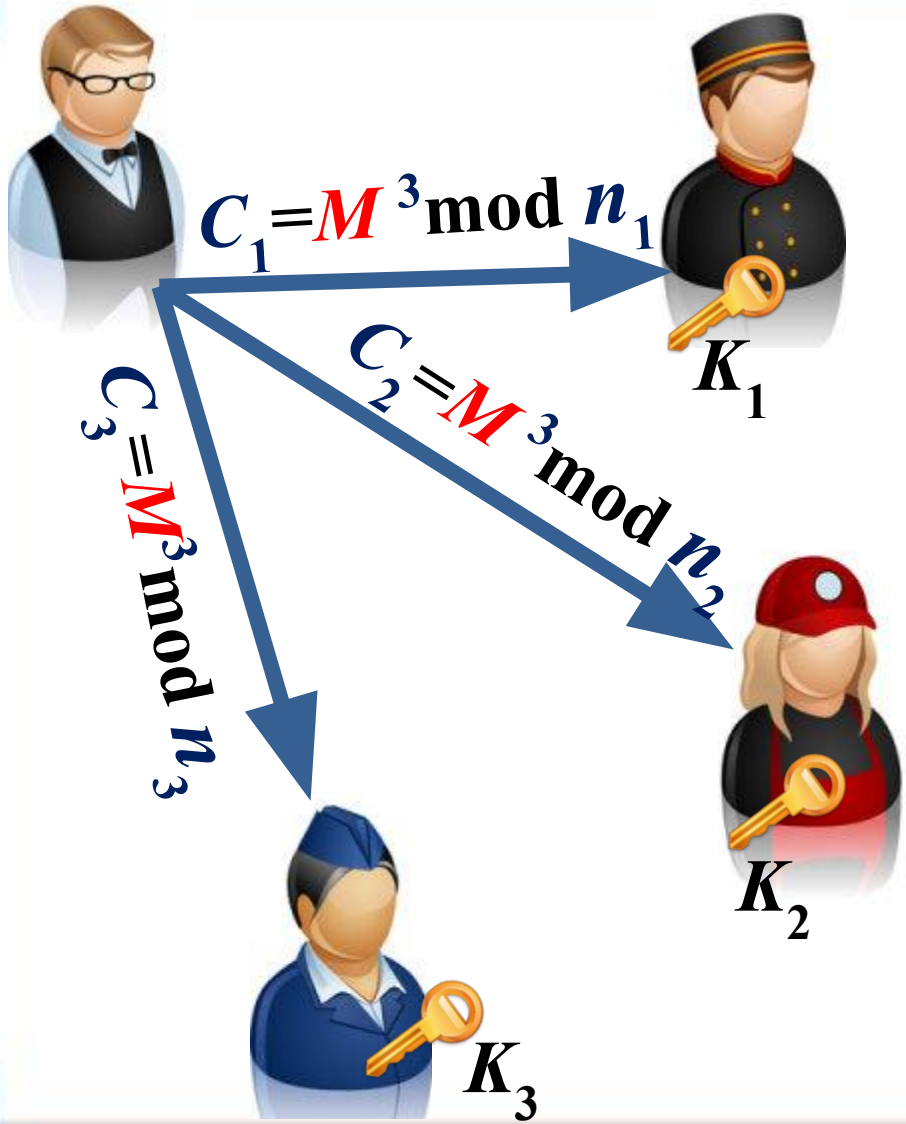


Числовое поле быстрее для очень больших чисел

Для RSA квадратичное решето лучше, чем эллиптические кривые

Квадратичное решето работает для чисел не больше 10^{110} с простым делителем, меньшим $\sqrt{n}$

Атака на RSA на основе общей экспоненты



Если модули – взаимно простые, то по китайской тереме от остатках можно комбинировать

$$\begin{cases} C_1 = M^3 \bmod n_1 \\ C_2 = M^3 \bmod n_2 \\ C_3 = M^3 \bmod n_3 \end{cases}$$

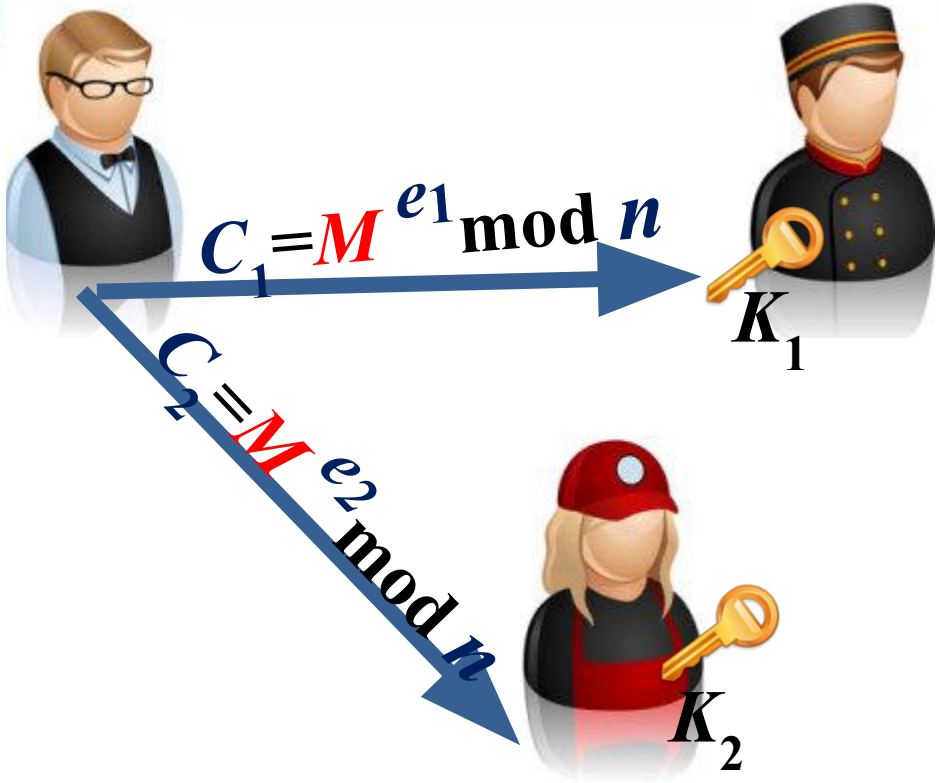
и отсюда найти

$$C = M^3 \bmod n_1 n_2 n_3$$

Т.к. $M^3 < n_1 n_2 n_3$ ⇨

$$M = \sqrt[3]{C}$$

Атака на RSA на основе общего модуля



$t_1 = e_1^{-1} \bmod e_2$

$t_1 e_1 = t_2 e_2 + 1, \quad t_2 \in Z$

$t_2 = (t_1 e_1 - 1)/e_2$

$M = C_1^{t_1} C_2^{-t_2} \bmod n$

Почему?

$$t_1 e_1 \equiv 1 (\bmod e_2) \Rightarrow t_1 e_1 = 1 + e_2 t_2 \Rightarrow t_2 = \frac{t_1 e_1 - 1}{e_2} \Rightarrow$$

$$C_1^{t_1} C_2^{-t_2} (\bmod n) = (M^{e_1})^{t_1} (M^{e_2})^{-t_2} = M^{e_1 t_1} M^{-e_2 t_2} = M^{1+e_2 t_2} M^{-e_2 t_2} = M$$

Атака на RSA : «встреча посередине»

Мультипликативность:

$$C_1 \equiv M_1^{\,e} \bmod n$$

$$C_2 \equiv M_2^{\,e} \bmod n$$

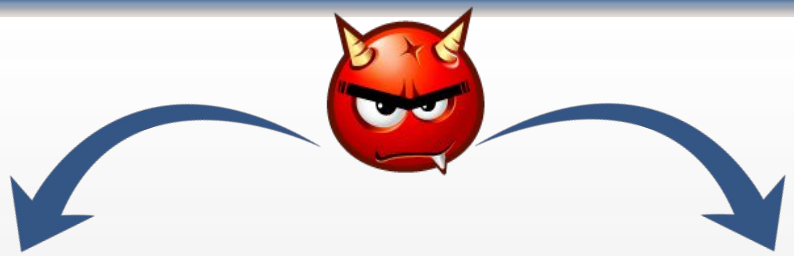
Каким будет шифротекст открытого текста $M = M_1 M_2$?

$$C \equiv (M_1 M_2)^e = M_1^{\,e} M_2^{\,e} \bmod n = C_1 C_2$$

$$C \cdot M_1^{\,-e} = M_2^{\,e} \bmod n \quad \Rightarrow$$ можно построить атаку

Пусть известно, что $M = M_1 M_2 < 2^{L/2}$

Атака на RSA : «встреча посередине»



$C \cdot (1^{-e}) \bmod n$

$C \cdot (2^{-e}) \bmod n$

$C \cdot (3^{-e}) \bmod n$

$\dots$

$\dots$

$C \cdot (2^{L/2})^{-e}$

$C \cdot i^{-e} \bmod n \equiv j^{e} \bmod n$

$M = i \cdot j$

$1^{e} \bmod n$

$2^{e} \bmod n$

$3^{e} \bmod n$

$\dots$

$\dots$

$(2^{L/2})^{e} \bmod n$

Циклическая атака на RSA (бесключевое чтение)

$$C^e \equiv C_1 \bmod n$$

$$C_1^e \equiv C_2 \bmod n$$

$$C_2^e \equiv C_3 \bmod n$$

$$\dots$$

$$C_{k-2}^e \equiv C_{k-1} \bmod n$$

$$C_{k-1}^e \equiv C_k \bmod n \equiv C$$

Атака успешна, если порядок k открытой експоненты e мал (k – наименьшее число, для которого $e^k \equiv 1 (\bmod \varphi(n))$; НОД$(e, \varphi(n))=1$)

$$\Rightarrow \quad M = C_{k-1}$$

Атака Винера: математическое вступление

ЦЕПНЫЕ (НЕПРЕРЫВНЫЕ) ДРОБИ

Любое действительное число x можно представить цепной дробью

$$x = [a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

$$a_0 \in Z; \quad a_1, a_2, \ldots \in N$$

Атака Винера: математическое вступление

Как найти элементы цепной дроби для числа x ?

$$x_0 = x - a_0 \ ;$$

$$a_1 = \left\lfloor \frac{1}{x_0} \right\rfloor ; \qquad x_1 = \frac{1}{x_0} - a_1 \ ;$$

$$a_2 = \left\lfloor \frac{1}{x_1} \right\rfloor ; \qquad x_2 = \frac{1}{x_1} - a_2 \ ;$$

$$\dots$$

$$a_i = \left\lfloor \frac{1}{x_{i-1}} \right\rfloor ; \qquad x_i = \frac{1}{x_{i-1}} - a_i \ ;$$

$\lfloor x \rfloor$ -целая часть числа x

Атака Винера: математическое вступление

Пример. Найти разложение в цепную дробь числа $x = \frac{34}{99}$

Решение. $a_0 = \left\lfloor x_0 \right\rfloor = \left\lfloor \frac{34}{99} \right\rfloor = 0$; $x_0 = x - a_0 = \frac{34}{99}$

$a_1 = \left\lfloor \frac{1}{x_0} \right\rfloor = \left\lfloor \frac{99}{34} \right\rfloor = 2$; $x_1 = \frac{1}{x_0} - a_1 = \frac{99}{34} - 2 = \frac{31}{34}$

$a_2 = \left\lfloor \frac{1}{x_1} \right\rfloor = \left\lfloor \frac{34}{31} \right\rfloor = 1$; $x_2 = \frac{1}{x_1} - a_2 = \frac{34}{31} - 1 = \frac{3}{31}$

$a_3 = \left\lfloor \frac{1}{x_2} \right\rfloor = \left\lfloor \frac{31}{3} \right\rfloor = 10$; $x_3 = \frac{1}{x_2} - a_3 = \frac{31}{3} - 10 = \frac{1}{3}$

$a_4 = \left\lfloor \frac{1}{x_3} \right\rfloor = \left\lfloor \frac{3}{1} \right\rfloor = 3$

Атака Винера: математическое вступление

$$x = \frac{34}{99} = [0;\ 2,\ 1,\ 10,\ 3] = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{10 + \cfrac{1}{3}}}}$$

Атака Винера: математическое вступление

***i*-ой подходящей дробью** $\frac{p_i}{q_i}$ **для цепной дроби**

$$x = [a_0; a_1, a_2, \ldots]$$

называют конечную цепную дробь $\frac{p_i}{q_i} = [a_0; a_1, a_2, \ldots, a_i]$

Рекуррентные формулы для вычисления подходящих дробей для цепной дроби $\frac{p_i}{q_i} = [a_0; a_1, a_2, \ldots, a_i]$ **:**

$$p_{-1} = 1; \quad q_{-1} = 0;$$

$$p_0 = a_0; \quad q_0 = 1$$

$$\frac{p_i}{q_i} = \frac{a_i p_{i-1} + p_{i-2}}{a_i q_{i-1} + q_{i-2}}; \quad i = 1,2,\ldots$$

Атака Винера: математическое вступление

Пример. Найти подходящие дроби для цепной дроби

$$\frac{34}{99} = [0; 2, 1, 10, 3]$$

Решение. $[0;\ 2,\ 1,\ 10,\ 3]$

$a_0\ \ a_1\ \ a_2\ \ a_3\ \ a_4$

$$p_{-1} = 1; \quad p_0 = 0; \quad q_{-1} = 0; \quad q_0 = 1$$

$$\frac{p_1}{q_1} = \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}} = \frac{2\cdot 0+1}{2\cdot 1+0} = \frac{1}{2}; \quad p_1 = 1; \quad q_1 = 2;$$

$$\frac{p_2}{q_2} = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0} = \frac{1\cdot 1+0}{1\cdot 2+1} = \frac{1}{3}; \quad p_2 = 1; \quad q_2 = 3;$$

Атака Винера: математическое вступление

$$\frac{p_3}{q_3} = \frac{a_3 p_2 + p_1}{a_3 q_2 + q_1} = \frac{10 \cdot 1 + 1}{10 \cdot 3 + 2} = \frac{11}{32}; \quad p_3 = 11; \; q_3 = 32;$$

$$\frac{p_4}{q_4} = \frac{a_4 p_3 + p_2}{a_4 q_3 + q_2} = \frac{3 \cdot 11 + 1}{3 \cdot 32 + 2} = \frac{34}{99}; \quad p_4 = 34; \; q_4 = 99$$

Подходящие дроби:

$$\frac{p_1}{q_1} = \frac{1}{2}; \quad \frac{p_2}{q_2} = \frac{1}{3}; \quad \frac{p_3}{q_3} = \frac{11}{32}; \quad \frac{p_4}{q_4} = \frac{34}{99};$$

Атака Винера: математическое вступление

Если несократимая дробь $\frac{p}{q}$ удовлетворяет неравенству:

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{2q^2}$$

то дробь $\frac{p}{q}$ – одна из подходящих дробей в разложении числа x в цепную дробь.

Атака Винера

М. Винер показал, что когда секретная экспонента

$d < \frac{1}{3}\sqrt[4]{n}$, **то дробь** $\frac{e}{n}$ **удовдетворяет неравенству**

$$\left| \frac{e}{n} - \frac{k}{d} \right| \leq \frac{1}{2d^2}$$

- **это классическая аппроксимация с помощью цепных дробей;**

- **число дробей** $\frac{k}{d}$, **где** $d < n$, **не больше** $\log n$

- **для некоторого** k **выполнится** $\frac{k}{d} = \frac{p}{q}$. **Тогда так как НОД** $(k, d) = 1$, **то** $p = k, q = d$

Атака Винера: сценарий

Разложить дробь $\frac{e}{n}$ в цепную дробь

Найти все подходящие дроби для дроби $\frac{e}{n}$

Среди подходящих дробей p/q найти ту, для которой eq-1 делится нацело на p. Тогда $p=k$, $q=d$.

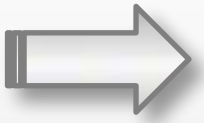
Атака Винера: противодействие

Для противодействия атаке надо, чтобы секретная экспонента была не меньше, чем

$$n^{0,292}$$

Например, если модуль имеет размер 1024 бит, необходимо чтобы длина секретной экспоненты была не менее 256 бит.

Использование китайской теоремы об остатках для ускорения расшифрования

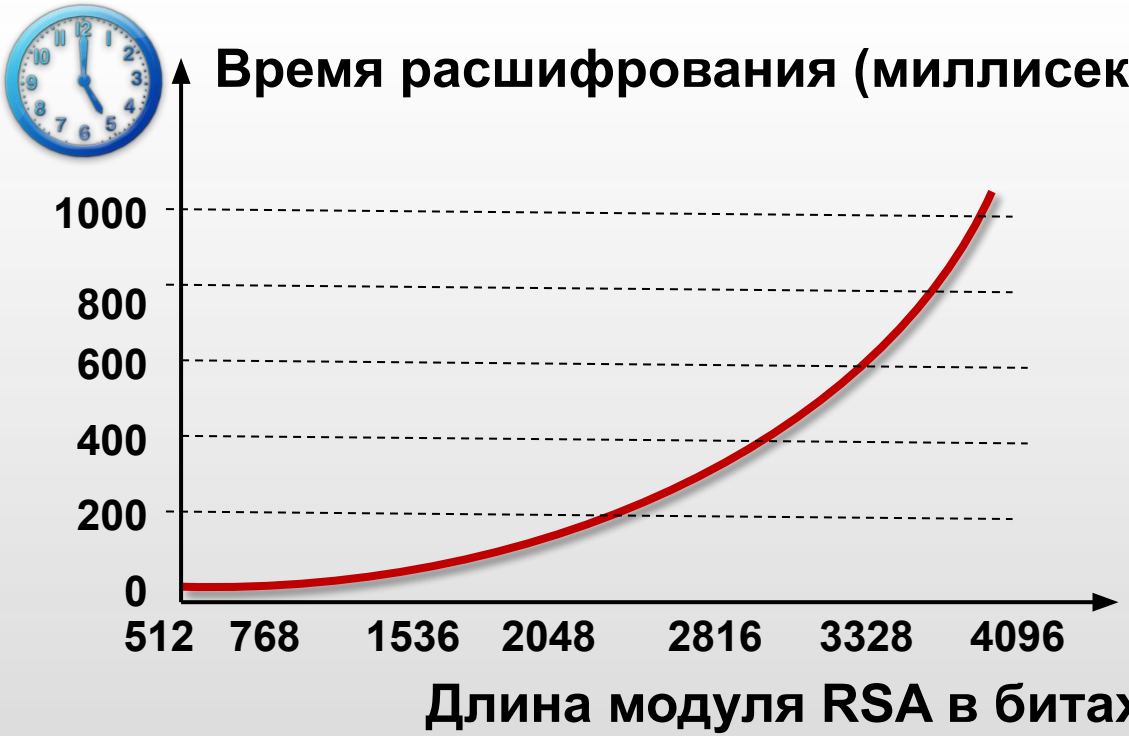


$$M = C^{d} \bmod n$$

Секретный ключ – экспонента d

Если длина модуля $|n|=1024$ бит, то длина секретной экспоненты $|d| \sim 1024$ бит

Зависимость времени вычисления значения $y = x^e \pmod n$ от длины модуля



http://security.stackexchange.com/questions/1833/encryption-decryption-time

Каждое удвоение длины ключа RSA увеличивает время расшифрования в 6 – 7 раз

Нужен алгоритм расшифрования с минимальным числом операций

Использование китайской теоремы об остатках для ускорения расшифрования

Владелец секретного ключа знает p и q

1

$$M_p \equiv C^d \bmod p \equiv C^{d \bmod p-1} \bmod p$$

$$M_q \equiv C^d \bmod q \equiv C^{d \bmod q-1} \bmod q$$

2

По китайской теореме об остатках

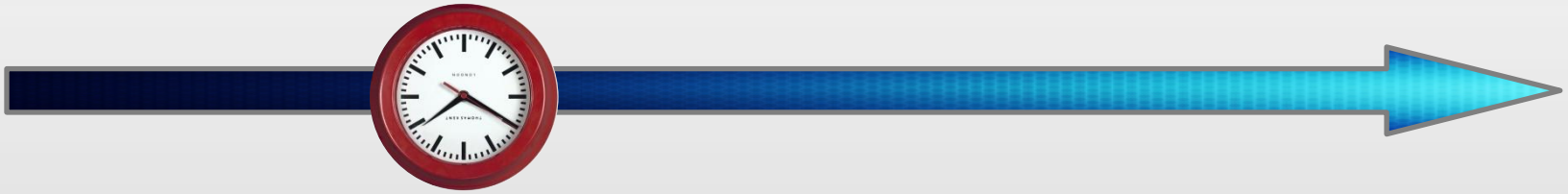
$$\begin{cases} M \equiv M_p \bmod p \\ M \equiv M_q \bmod q \end{cases}$$

Если длина модуля $|n|=1024$ бит, то длины множителей $|p|=|q|=512$ бит

Использование китайской теоремы об остатках для ускорения расшифрования

Два возведения в степень по mod дл. 512 бит с показателем 512 бит

t



Одно возведение в степень по mod дл. 1024 бит с показателем 1024 бит

t

Симметричные против асимметричных криптосистем

Стойкие, работают очень быстро. Им не нужны большие вычислительные ресурсы.

Асимметричные алгоритмы очень медленные

При передаче ключа он может быть перехвачен мошенником

Распространяют открытые ключи открыто. Перехват открытых ключей – бесполезен.

Гибридные криптосистемы

Гибридные криптосистемы

Совмещают преимущества криптосистем с открытым ключом и производительность симметричных шифров:

- **данные шифруются с помощью симметричного шифра;**
- **асимметричный алгоритм шифрует только ключ симметричного шифра**

Инкапсуляция ключа

Инкапсуляция сообщения

Числовая упаковка сообщения

C_k – RSA, $E_{\text{откр.}}(k)$

C_m – AES, $E_k(m)$

Гибридные криптосистемы