Кафедра Компьютерные системы и технологии
НИЯУ МИФИ

Защита информации

Иванов М.А.

Лекция № 9
Рюкзачная криптосистема (Knapsack Cryptosystem)

Темы

- Трудные математические задачи
- Задача об укладке рюкзака
- Knapsack Cryptosystem
- Пример рюкзачной криптосистемы

Москва, 2025

Трудные задачи

Криптосистемы с ОК

Трудные задачи

- Факторизация целых чисел

Криптосистемы с ОК

- Криптосистема RSA

Трудные задачи

- Факторизация целых чисел
- Дискретное логарифмирование

Криптосистемы с ОК

- Криптосистема RSA
- Криптосистема Эль Гамаля (ElGamal Cryptosystem)

Трудные задачи

- Факторизация целых чисел
- Дискретное логарифмирование
- Задача об укладке рюкзака

Криптосистемы с ОК

- Криптосистема RSA
- Криптосистема Эль Гамаля (ElGamal Cryptosystem)
- Рюкзачная криптосистема (Knapsack Cryptosystem)

Трудные задачи

- Факторизация целых чисел
- Дискретное логарифмирование (DLP)
- Задача об укладке рюкзака
- Дискретное логарифмирование на группе точек эллиптической кривой
- …

Криптосистемы с ОК

- Криптосистема RSA
- Криптосистема Эль Гамаля (ElGamal Cryptosystem)
- Рюкзачная криптосистема (Knapsack Cryptosystem)
- Криптосистема, основанная на свойствах эллиптической кривой (Elliptic Curves Cryptosystem)
- …

Трудные задачи

- Факторизация целых чисел
- Дискретное логарифмирование (DLP)
- Задача об укладке рюкзака
- Дискретное логарифмирование на группе точек эллиптической кривой
- Декодирование линейного кода
- …

Криптосистемы с ОК

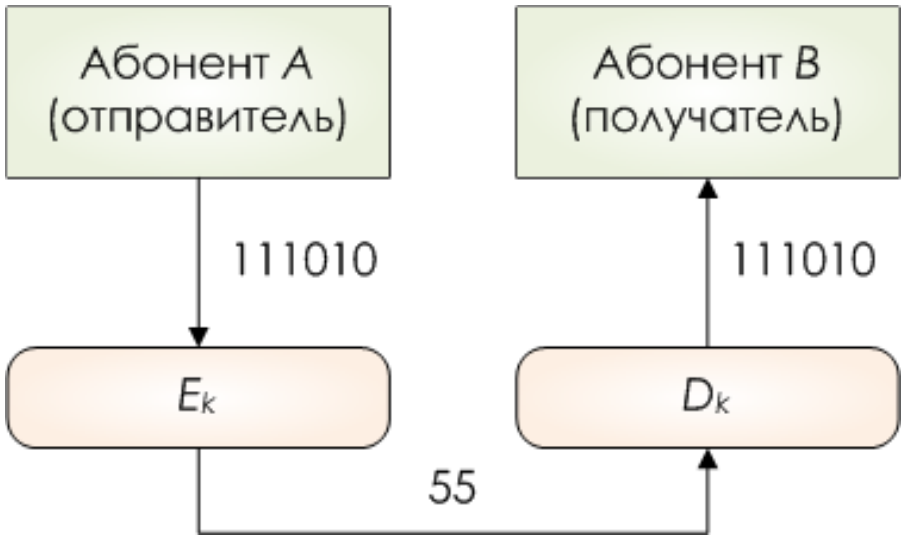
- Криптосистема RSA
- Криптосистема Эль Гамаля (ElGamal Cryptosystem)
- Рюкзачная криптосистема (Knapsack Cryptosystem)
- Криптосистема, основанная на свойствах эллиптической кривой (Elliptic Curves Cryptosystem)
- Криптосистема МакЭлиса (McEliece Cryptosystem)
- …

Простая задача об укладке рюкзака

- Представить число 55 в виде суммы элементов списка чисел {3, 8, 12, 2, 32, 59}
- Ответ: 55 = 3 + 8 + 12 + 32 или 55 <-> (1 1 1 0 1 0)

Простая задача об укладке рюкзака

- Представить число 55 в виде суммы элементов списка чисел {3, 8, 12, 2, 32, 59}
- Ответ: 55 = 3 + 8 + 12 + 32 или 55 <-> (1 1 1 0 1 0)



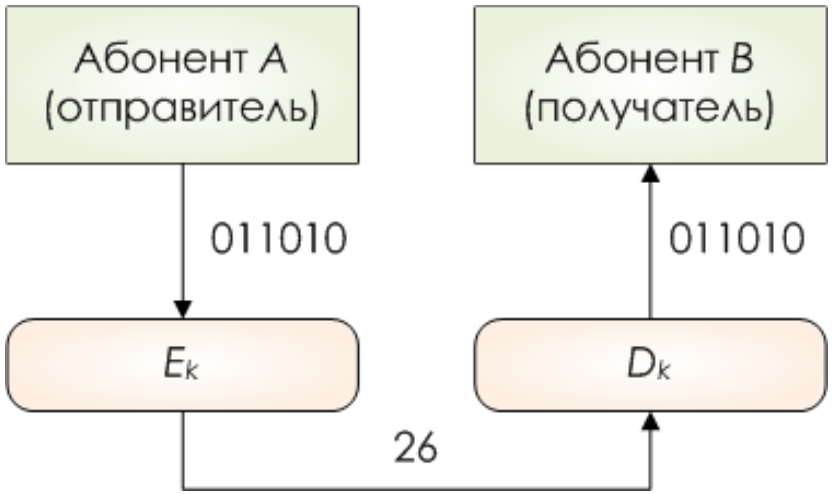
Примитивная система шифрования, в которой отправителю и получателю известен список чисел {3, 8, 12, 2, 32, 59}

Очень простая задача об укладке рюкзака

- Представить число 26 в виде суммы различных чисел из списка {32, 16, 8, 4, 2, 1}
- Ответ: 26 = 16 + 8 + 2 или 26 <-> (0 1 1 0 1 0)

Очень простая задача об укладке рюкзака

- Представить число 26 в виде суммы различных чисел из списка {32, 16, 8, 4, 2, 1}
- Ответ: 26 = 16 + 8 + 2 или 26 <-> (0 1 1 0 1 0)



Примитивная система шифрования, в которой отправителю и получателю известен список чисел {32, 16, 8, 4, 2, 1}

Последовательность построения криптосистемы с открытым ключом

Последовательность построения криптосистемы с открытым ключом

- Составляется трудная задача T, не решаемая за полиномиальное время

Последовательность построения криптосистемы с открытым ключом

- Составляется трудная задача T, не решаемая за полиномиальное время
- Из T выделяется легкая подзадача T_{easy}, имеющая полиномиальный или даже более простой алгоритм решения

Последовательность построения криптосистемы с открытым ключом

- Составляется трудная задача T, не решаемая за полиномиальное время
- Из T выделяется легкая подзадача T_{easy}, имеющая полиномиальный или даже более простой алгоритм решения
- Путем «взбивания» легкая задача T_{easy} превращается в трудно решаемую задачу $T_{shuffle}$, не имеющую никакого сходства с T_{easy}

Последовательность построения криптосистемы с открытым ключом

- Составляется трудная задача T, не решаемая за полиномиальное время
- Из T выделяется легкая подзадача T_{easy}, имеющая полиномиальный или даже более простой алгоритм решения
- Путем «взбивания» легкая задача T_{easy} превращается в трудно решаемую задачу $T_{shuffle}$, не имеющую никакого сходства с T_{easy}
- На основе $T_{shuffle}$ определяется открытая функция зашифрования; процедура получения T_{easy} из $T_{shuffle}$ держится в секрете

Последовательность построения криптосистемы с открытым ключом

- Составляется трудная задача T, не решаемая за полиномиальное время
- Из T выделяется легкая подзадача T_{easy}, имеющая полиномиальный или даже более простой алгоритм решения
- Путем «взбивания» легкая задача T_{easy} превращается в трудно решаемую задачу $T_{shuffle}$, не имеющую никакого сходства с T_{easy}
- На основе $T_{shuffle}$ определяется открытая функция зашифрования; процедура получения T_{easy} из $T_{shuffle}$ держится в секрете
- Криптосистема конструируется таким образом, чтобы для противника процедура дешифрования заключалась в решении $T_{shuffle}$, имеющей вид трудной задачи T, а законный получатель, знающий секрет, решал бы легкую задачу T_{easy}

Трудная задача об укладке рюкзака

- Дан список чисел $\{a_{99} \ldots a_2\ a_1\ a_0\}$, цифры которых выбраны случайным образом, $|a_i| = 40_{10}$, $i = 0, 1, \ldots, 99$
- Представить число c в виде суммы некоторых чисел a_i из списка, $|c| = 42_{10}$

Knapsack Cryptosystems

- КС Меркля-Хеллмана
- КС Грэма-Шамира (****)
- …
- КС Шора-Ривеста (**)

Probabilistic Knapsack Cryptosystem ???

Ранцевая криптосистема Грэма-Шамира

Пример T_{easy}

$$a_0 = 020105$$

$$a_1 = 220209$$

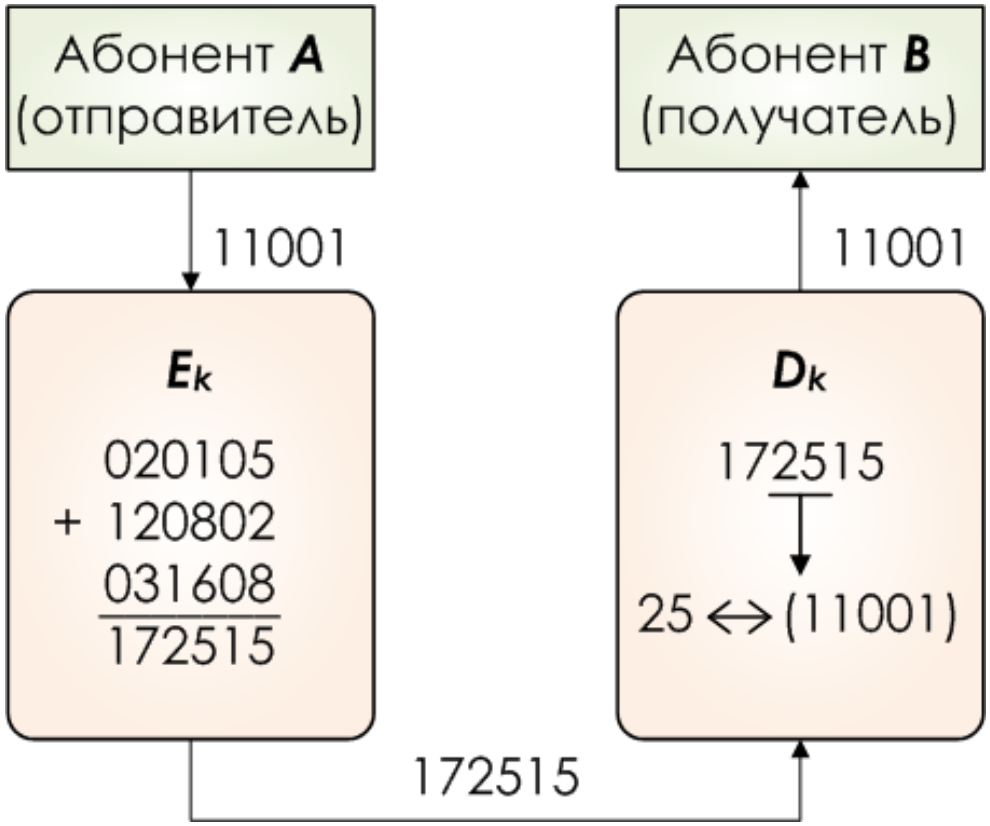
$$a_2 = 260405$$

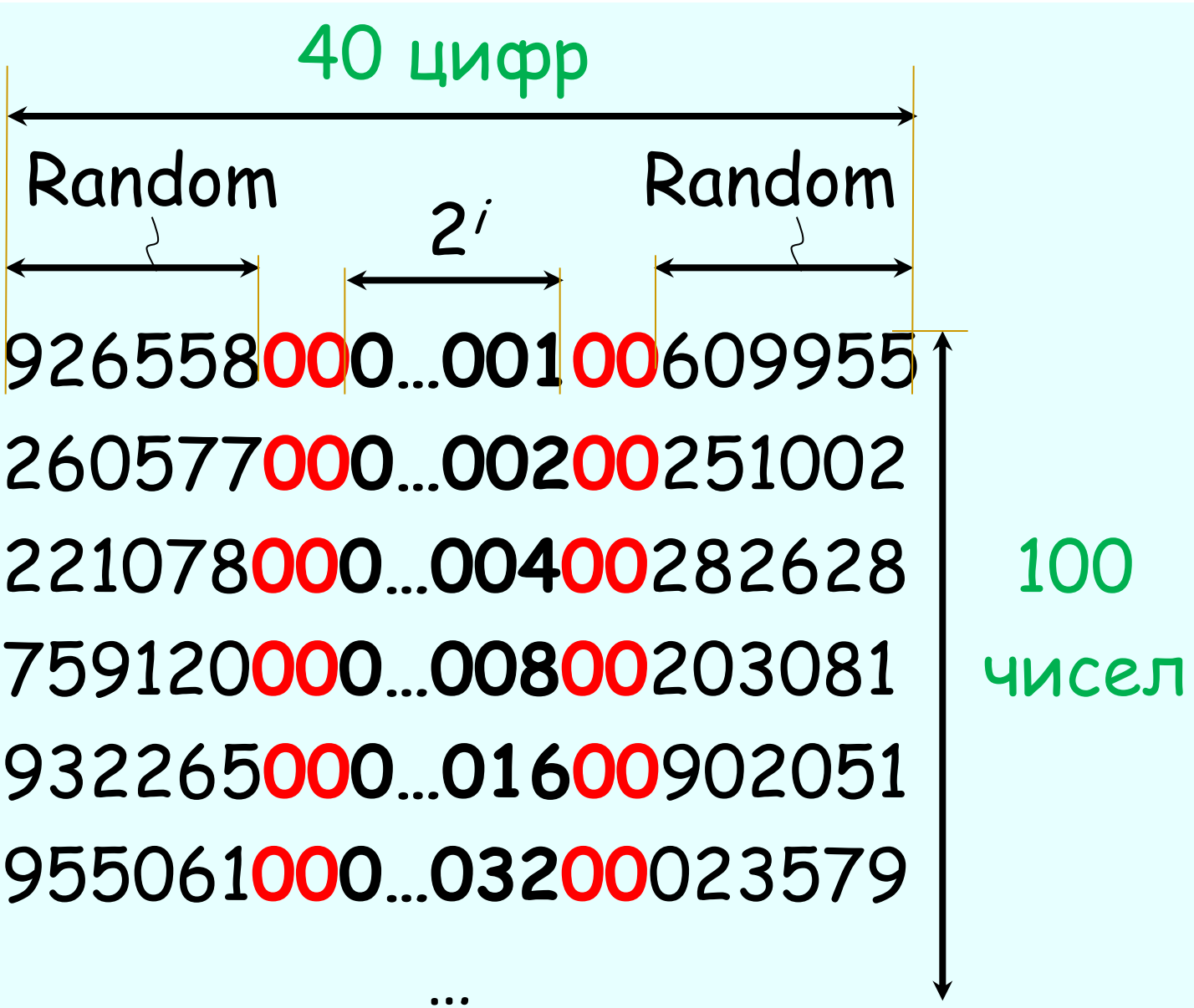
$$a_3 = 120802$$

$$a_4 = 031608$$

Пример T_{easy}

$$a_0 = 020105$$
$$a_1 = 220209$$
$$a_2 = 260405$$
$$a_3 = 120802$$
$$a_4 = 031608$$




40 цифр
Random
2^i
Random
926558000...00100609955
260577000...00200251002
221078000...00400282628
759120000...00800203081
932265000...01600902051
955061000...03200023579
...
100
чисел

«Взбивание» задачи T_{easy} и получение $T_{shuffle}$ (Р. Меркль)

«Взбивание» задачи T_{easy} и получение $T_{shuffle}$ (Р. Меркль)

- Сформируем список $\{a_{n-1} \ldots a_1 \; a_0\}$

«Взбивание» задачи T_{easy} и получение $T_{shuffle}$ (Р. Меркль)

- Сформируем список $\{a_{n-1} \ldots a_1\ a_0\}$
- Выберем два больших взаимно простых числа R и S и найдем такое число T, чтобы выполнялось условие $SR \equiv 1 \bmod T$

«Взбивание» задачи T_{easy} и получение $T_{shuffle}$ (Р. Меркль)

- Сформируем список $\{a_{n-1} \ldots a_1\ a_0\}$
- Выберем два больших взаимно простых числа R и S и найдем такое число T, чтобы выполнялось условие $SR \equiv 1 \bmod T$
- Получим новый список $\{b_{n-1} \ldots b_1\ b_0\}$, каждый элемент которого суть результат умножения соответствующего числа из первоначального списка на S по модулю T:
  $b_i = a_i\ S \bmod T,\ i = 0, 1, \ldots, (n-1)$

«Взбивание» задачи T_{easy} и получение $T_{shuffle}$ (Р. Меркль)

- Сформируем список $\{a_{n-1} \ldots a_1\ a_0\}$
- Выберем два больших взаимно простых числа R и S и найдем такое число T, чтобы выполнялось условие $SR \equiv 1 \bmod T$
- Получим новый список $\{b_{n-1} \ldots b_1\ b_0\}$, каждый элемент которого суть результат умножения соответствующего числа из первоначального списка на S по модулю T: $b_i = a_i\ S \bmod T,\ i = 0, 1, \ldots, (n-1)$
- Уничтожим список $\{a_{n-1} \ldots a_1\ a_0\}$ и число S

«Взбивание» задачи T_{easy} и получение $T_{shuffle}$ (Р. Меркль)

- Сформируем список $\{a_{n-1} \ldots a_1\ a_0\}$
- Выберем два больших взаимно простых числа R и S и найдем такое число T, чтобы выполнялось условие $RS \equiv 1 \bmod T$
- Получим новый список $\{b_{n-1} \ldots b_1\ b_0\}$, каждый элемент которого суть результат умножения соответствующего числа из первоначального списка на S по модулю T: $b_i = a_i\ S \bmod T,\ i = 0, 1, \ldots, (n-1)$
- Уничтожим список $\{a_{n-1} \ldots a_1\ a_0\}$ и число S
- Для всех, не знающих секрета, числа из нового списка будут казаться случайными числами из интервала $[0, (T-1)]$, и все, кто не знает принцип их получения, примут соответствующую задачу за трудную задачу об укладке рюкзака

«Взбивание» задачи T_{easy} и получение $T_{shuffle}$ (Р. Меркль)

- Сформируем список $\{a_{n-1} \ldots a_1\ a_0\}$
- Выберем два больших взаимно простых числа R и S и найдем такое число T, чтобы выполнялось условие $RS \equiv 1 \bmod T$
- Получим новый список $\{b_{n-1} \ldots b_1\ b_0\}$, каждый элемент которого суть результат умножения соответствующего числа из первоначального списка на S по модулю T: $b_i = a_i\ S \bmod T,\ i = 0, 1, \ldots, (n-1)$
- Уничтожим список $\{a_{n-1} \ldots a_1\ a_0\}$ и число S
- Для всех, не знающих секрета, числа из нового списка будут казаться случайными числами из интервала $[0, (T-1)]$, и все, кто не знает принцип их получения, примут соответствующую задачу за трудную задачу об укладке рюкзака
- Список $\{b_{n-1} \ldots b_1\ b_0\}$ объявляется открытым ключом зашифрования

«Взбивание» задачи T_{easy} и получение $T_{shuffle}$ (Р. Меркль)

- Сформируем список $\{a_{n-1} \ldots a_1\ a_0\}$
- Выберем два больших взаимно простых числа R и S и найдем такое число T, чтобы выполнялось условие $SR \equiv 1 \bmod T$
- Получим новый список $\{b_{n-1} \ldots b_1\ b_0\}$, каждый элемент которого суть результат умножения соответствующего числа из первоначального списка на R по модулю T: $b_i = a_i R \bmod T,\ i = 0, 1, \ldots, (n-1)$
- Уничтожим список $\{a_{n-1} \ldots a_1\ a_0\}$ и число R
- Для всех, не знающих секрета, числа из нового списка будут казаться случайными числами из интервала $[0, (T-1)]$, и все, кто не знает принцип их получения, примут соответствующую задачу за трудную задачу об укладке рюкзака
- Список $\{b_{n-1} \ldots b_1\ b_0\}$ объявляется открытым ключом зашифрования
- Числа S и T объявляются секретным ключом расшифрования

Рюкзачная криптосистема (Р. Меркль)

Рюкзачная криптосистема (Р. Меркль)

- **Алгоритм зашифрования** двоичного сообщения $m = m_{n-1} \ldots m_1 m_0$, $m_i \in \{0, 1\}$:

$$c = E(m) = \sum b_i m_i \pmod{T}$$

Рюкзачная криптосистема (Р. Меркль)

- **Алгоритм зашифрования** двоичного сообщения $m = m_{n-1} \ldots m_1 m_0$, $m_i \in \{0, 1\}$:

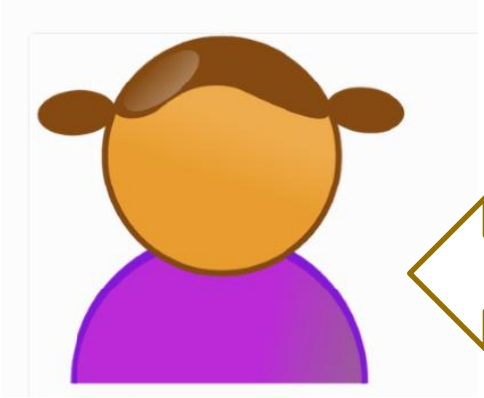
  $$c = E(m) = \sum b_i m_i \pmod{T}$$

- **Алгоритм расшифрования** закрытого сообщения c:

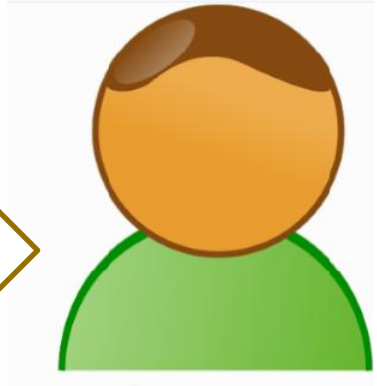
  - составляем произведение

    $$Sc = S \sum b_i m_i \pmod{T} =$$
    $$= \sum a_i SR\, m_i \pmod{T} = \sum a_i m_i \pmod{T}$$

  - решая легкую задачу об укладке рюкзака, находим $m = m_{n-1} \ldots m_1 m_0$



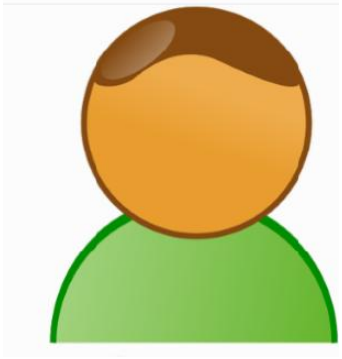
Ненадежный канал связи



Алиса

Боб

Боб хочет получать секретные сообщения



Боб

Боб формирует пару ключей

Находит R, S и T, такие, что RS = 1 mod T:

$41 \cdot 59 = 2419 \rightarrow 41 \cdot 59 = 1 \bmod 2418$

$\rightarrow$ **R = 41, S = 59, T = 2418**

Составляет легкую задачу об укладке рюкзака:

$a_0 = 201$
$a_1 = 502$
$a_2 = 304$
$a_3 = 108$
$a_4 = 016$

$\times$ 41

08241
20582
12464
04428
00656

mod 2418

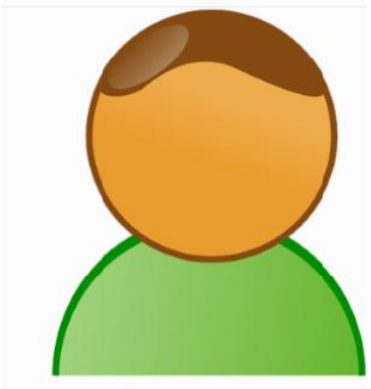
Получает трудную задачу об укладке рюкзака:

$b_0 = 0987$
$b_1 = 1238$
$b_2 = 0374$
$b_3 = 2010$
$b_4 = 0656$

(S, T) = Secret Key

Public Key

Боб хочет получать секретные сообщения



Боб

Боб формирует пару ключей

Находит R, S и T, такие, что RS = 1 mod T:

$41 \cdot 59 = 2419 \rightarrow 41 \cdot 59 = 1 \bmod 2418$

$\rightarrow$ R = 41, S = 59, T = 2418

Составляет легкую задачу об укладке рюкзака:

$a_0 = 201$
$a_1 = 502$
$a_2 = 304$
$a_3 = 108$
$a_4 = 016$

$\times$ 41

08241
20582
12464
04428
00656

mod 2418

Получает трудную задачу об укладке рюкзака:

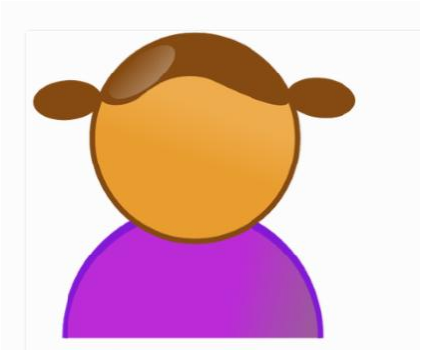
$b_0 = 0987$
$b_1 = 1238$
$b_2 = 0374$
$b_3 = 2010$
$b_4 = 0656$

(S, T) = Secret Key

Public Key

COK

Алиса хочет отправить секретное сообщение M_1 Бобу



Алиса

Читает из справочника открытый ключ Боба, шифрует сообщение M_1 и отправляет криптограмму C_1 Бобу

Исходное сообщение M_1

1
0
0
1
1

Открытый ключ Боба:

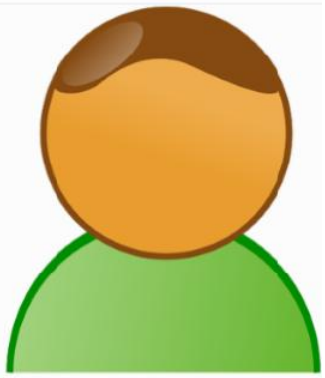
$b_0 = 0987$
$b_1 = 1238$
$b_2 = 0374$
$b_3 = 2010$
$b_4 = 0656$

Шифрование:

$$\begin{array}{r} 0987 \\ + \quad 2010 \\ \hline 0656 \\ \hline 3653 \end{array}$$

Криптограмма $C_1 = 3653$

Боб получает криптограмму C_1 от Алисы



Боб

С помощью своего секретного ключа расшифровывает ее

$$C_1 = 3653$$

$$C_1 \times S \pmod{T} \rightarrow 3653 \times 59 =$$

$$= 215527 = \underline{325} \bmod 2418$$

(S, T) = Secret Key B

$$25 \leftrightarrow (11001)$$

Полученное сообщение $M_1 = 11001$

Чтобы убедиться в правильности сформированного открытого ключа надо рассмотреть еще один пример

Алиса хочет отправить секретное сообщение M_2 Бобу

Алиса

Читает из справочника открытый ключ Боба, шифрует сообщение M_2 и отправляет криптограмму C_2 Бобу

Исходное сообщение M_2

0
1
1
0
1

Открытый ключ Боба:

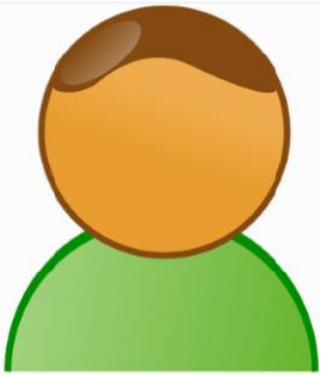
$b_0 = 0987$
$b_1 = 1238$
$b_2 = 0374$
$b_3 = 2010$
$b_4 = 0656$

Шифрование:

$$\begin{array}{r} 1238 \\ +\,0374 \\ 0656 \\ \hline 2268 \end{array}$$

Криптограмма $C_2 = 2268$

Боб получает криптограмму C_2 от Алисы



Боб

С помощью своего секретного ключа расшифровывает ее

$$C_2 = 2268$$

$$C_2 \times S \pmod{T} \rightarrow 2268 \times 59 =$$

$$= 133812 = 822 \bmod 2418$$

$$22 \leftrightarrow (10110)$$

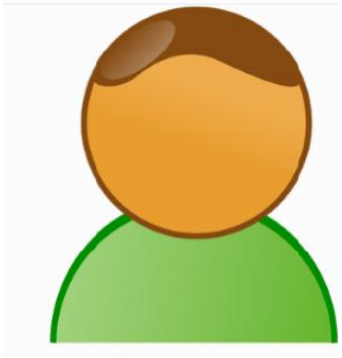
(S, T) = Secret Key B

Полученное сообщение $M_2 = 10110$

Можно использовать кодирование степеней 2, 3, 5, …

Можно использовать супервозрастающую последовательность

Боб хочет получать секретные сообщения



Боб

Боб формирует пару ключей

Находит R, S и T, такие, что RS = 1 mod T:

$83 \cdot 157 = 13031 \rightarrow 83 \cdot 157 = 1 \bmod 13030$

$\rightarrow$ **R = 83, S = 157, T = 13030**

Составляет легкую задачу об укладке рюкзака:

$a_0 = 0109$
$a_1 = 0302$
$a_2 = 0907$
$a_3 = 2708$
$a_4 = 8106$

$\times 83$

009047
025066
075281
224764
672798

mod 13030

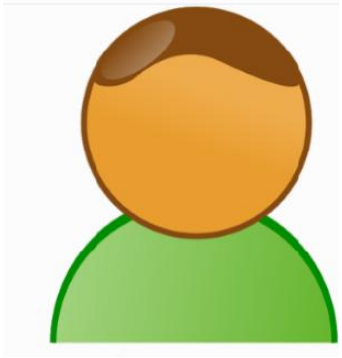
Получает трудную задачу об укладке рюкзака:

$b_0 = 09047$
$b_1 = 12036$
$b_2 = 10131$
$b_3 = 03254$
$b_4 = 08268$

(S, T) = Secret Key

Public Key

Боб хочет получать секретные сообщения



Боб

Боб формирует пару ключей

Находит R, S и T, такие, что RS = 1 mod T:

$83 \cdot 157 = 13031 \rightarrow 83 \cdot 157 = 1 \bmod 13030$

$\rightarrow$ **R = 83, S = 157, T = 13030**

Составляет легкую задачу об укладке рюкзака:

$a_0 = 0109$
$a_1 = 0302$
$a_2 = 0907$
$a_3 = 2708$
$a_4 = 8106$

$\times 83$

009047
025066
075281
224764
672798

mod 13030

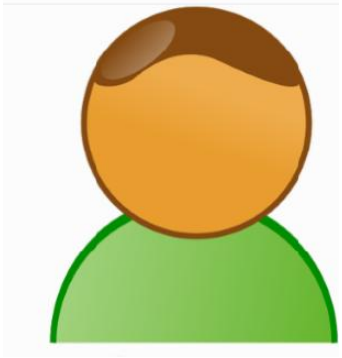
Получает трудную задачу об укладке рюкзака:

$b_0 = 09047$
$b_1 = 12036$
$b_2 = 10131$
$b_3 = 03254$
$b_4 = 08268$

(S, T) = Secret Key

Public Key

Боб хочет получать секретные сообщения



Боб

Боб формирует пару ключей

Находит R, S и T, такие, что RS = 1 mod T:

$83 \cdot 157 = 13031 \rightarrow 83 \cdot 157 = 1 \bmod 13030$

$\rightarrow$ **R = 83, S = 157, T = 13030**

Составляет легкую задачу об укладке рюкзака:

$a_0 = 0109$
$a_1 = 0302$
$a_2 = 0907$
$a_3 = 2708$
$a_4 = 8106$

$\times 83$

009047
025066
075281
224764
672798

mod 13030

Получает трудную задачу об укладке рюкзака:

$b_0 = 09047$
$b_1 = 12036$
$b_2 = 10131$
$b_3 = 03254$
$b_4 = 08268$

(S, T) = Secret Key

Public Key

СОК

Алиса хочет отправить секретное сообщение M Бобу

Алиса

Читает из справочника открытый ключ Боба, шифрует сообщение M_3 и отправляет криптограмму C_3 Бобу

Исходное сообщение M_3

1
0
0
1
1

Открытый ключ Боба:

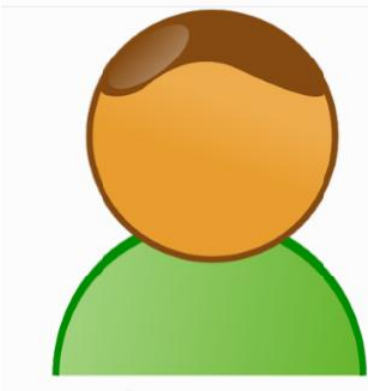
$b_0 = 09047$
$b_1 = 12036$
$b_2 = 10131$
$b_3 = 03254$
$b_4 = 08268$

Шифрование:

09047
+03254
08268
———
20569

Криптограмма $C_3 = 20569$

Боб получает криптограмму C_3 от Алисы



Боб

С помощью своего секретного ключа расшифровывает ее

$$C_3 = 20569$$

$$C_3 \times S \pmod{T} \rightarrow 20569 \times 157 =$$

$$= 3229333 = \underline{10923} \bmod 13030$$

$$109 \leftrightarrow (11001)$$

Полученное сообщение $M_3 = 11001$

$109_{10} = 1 \cdot 81 + 1 \cdot 21 + 0 \cdot 9 + 0 \cdot 3 + 1 \cdot 1 = 11001_3$

Криптосистема Меркля-Хеллмана

Криптосистема Грэма-Шамира

Криптосистема Шора-Ривеста

Бэкдоры для первой и второй КС можно адаптировать для третьей КС

Д.З. Попробуйте придумать скрытую возможность вычисления секретного ключа по открытому ключу, взятому из СОК

The questions are welcome !

КС&Т

Криптографические бэкдоры

Иванов М.А.

Москва,
2025 г.

Криптографические бэкдоры

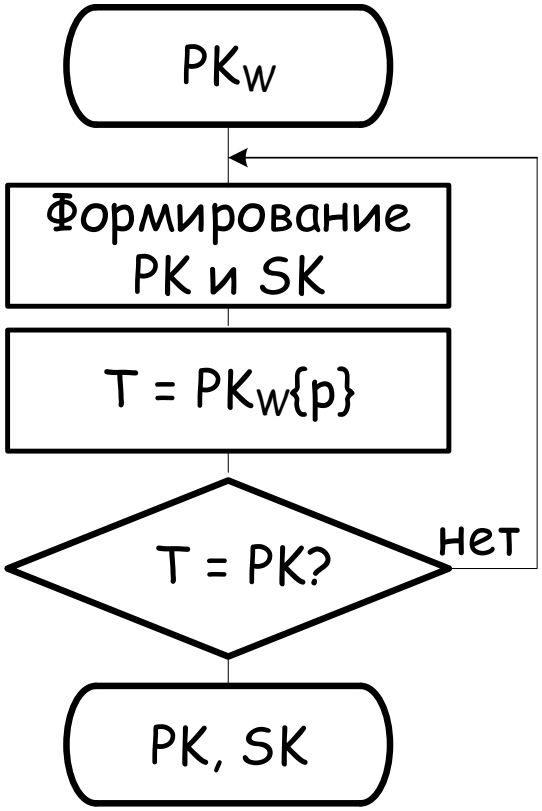
RSA: формирование PK и SK

- → Выбор p и q
- → Вычисление N = pq
- → Вычисление $\varphi(N) = (p - 1)(q - 1)$
- → Выбор e: $(e, \varphi(N)) = 1$
- → Определение d: $ed = 1 \bmod \varphi(N)$

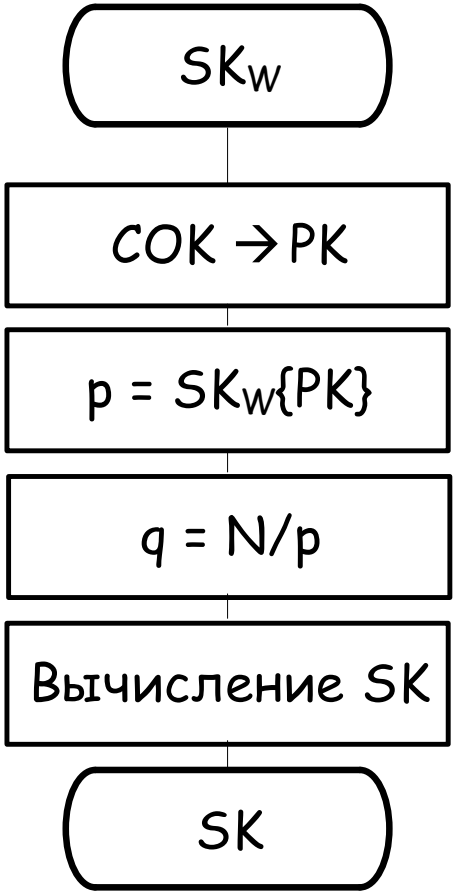
PK = (e, N), SK = d

PK → СОК

PK_W, SK_W - пара ключей

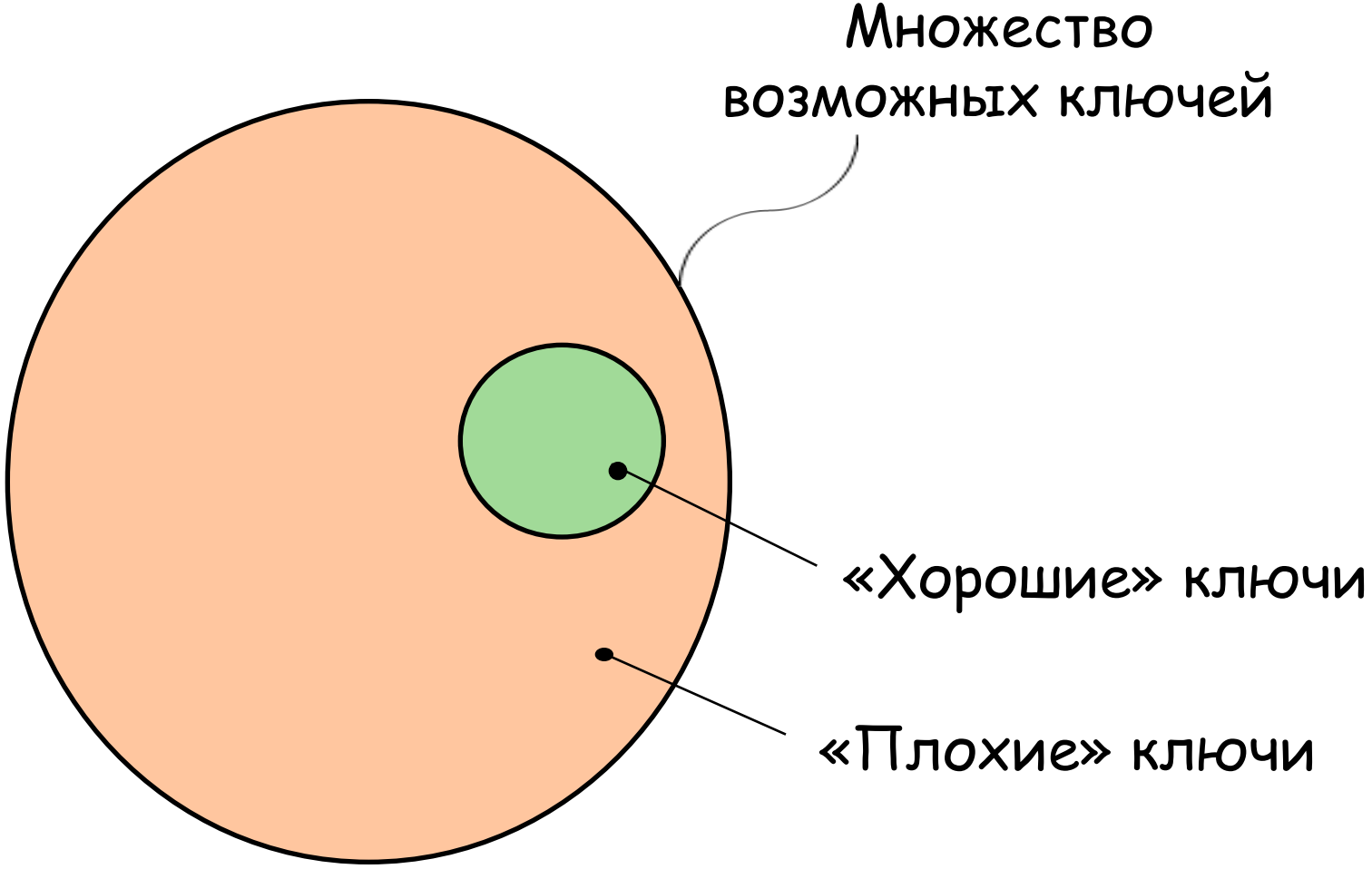


Создание скрытого канала



Атака

Шифр с секретным ключом



Неоднородное ключевое пространство

Скрытый криптографический канал в криптосистеме RSA

Первый криптографический бэкдор в RSA появился только в 1993 г.

Обозначения

$PK = (N, e)$, $SK = d$ – соответственно открытый и закрытый ключи пользователя

$PK_w = (N_w, e_w)$, $SK_w = d_w$ – соответственно открытый и закрытый ключи создателя скрытого канала

Схема алгоритма создания скрытого канала в криптосистеме RSA

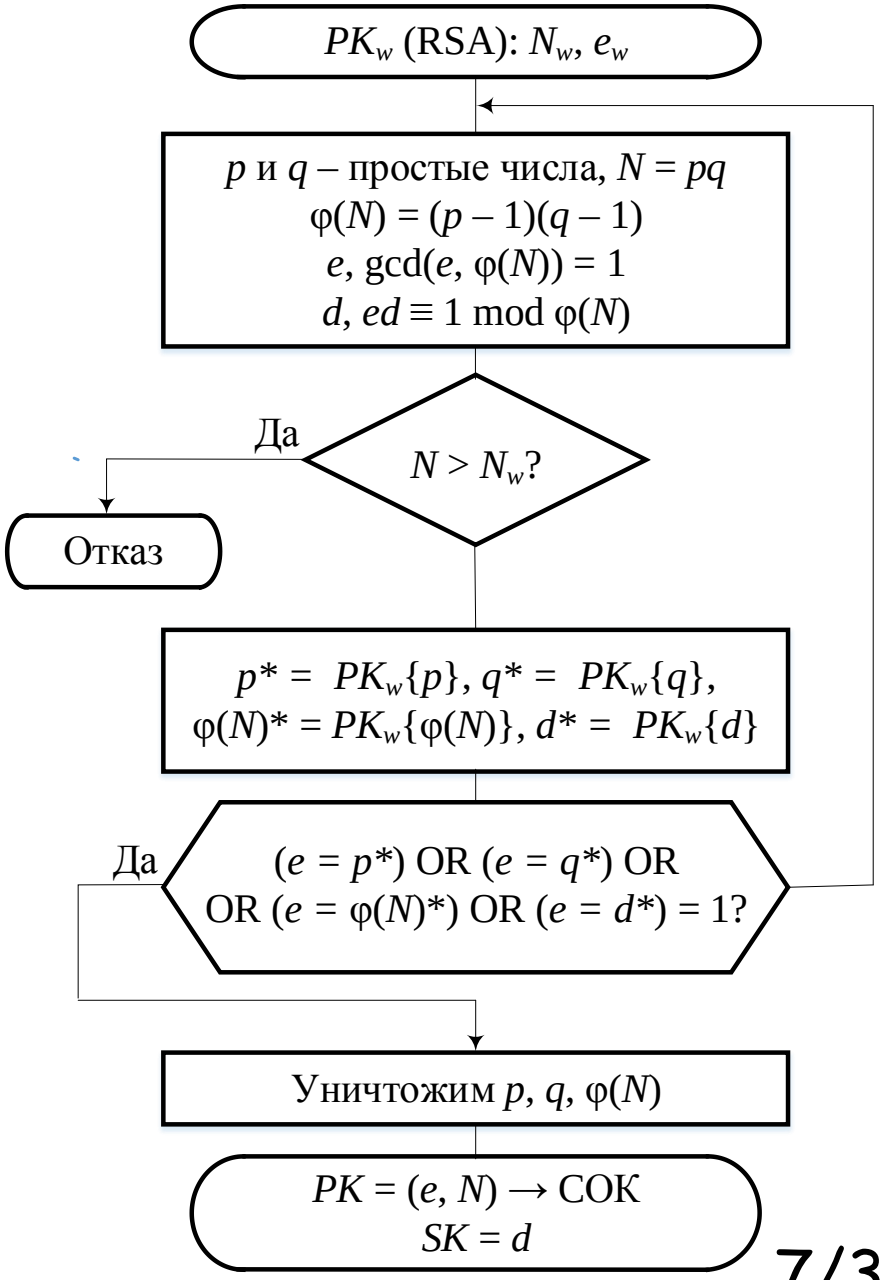


Схема алгоритма создания скрытого канала в криптосистеме RSA

Что в реальном мире будет вместо отказа ?

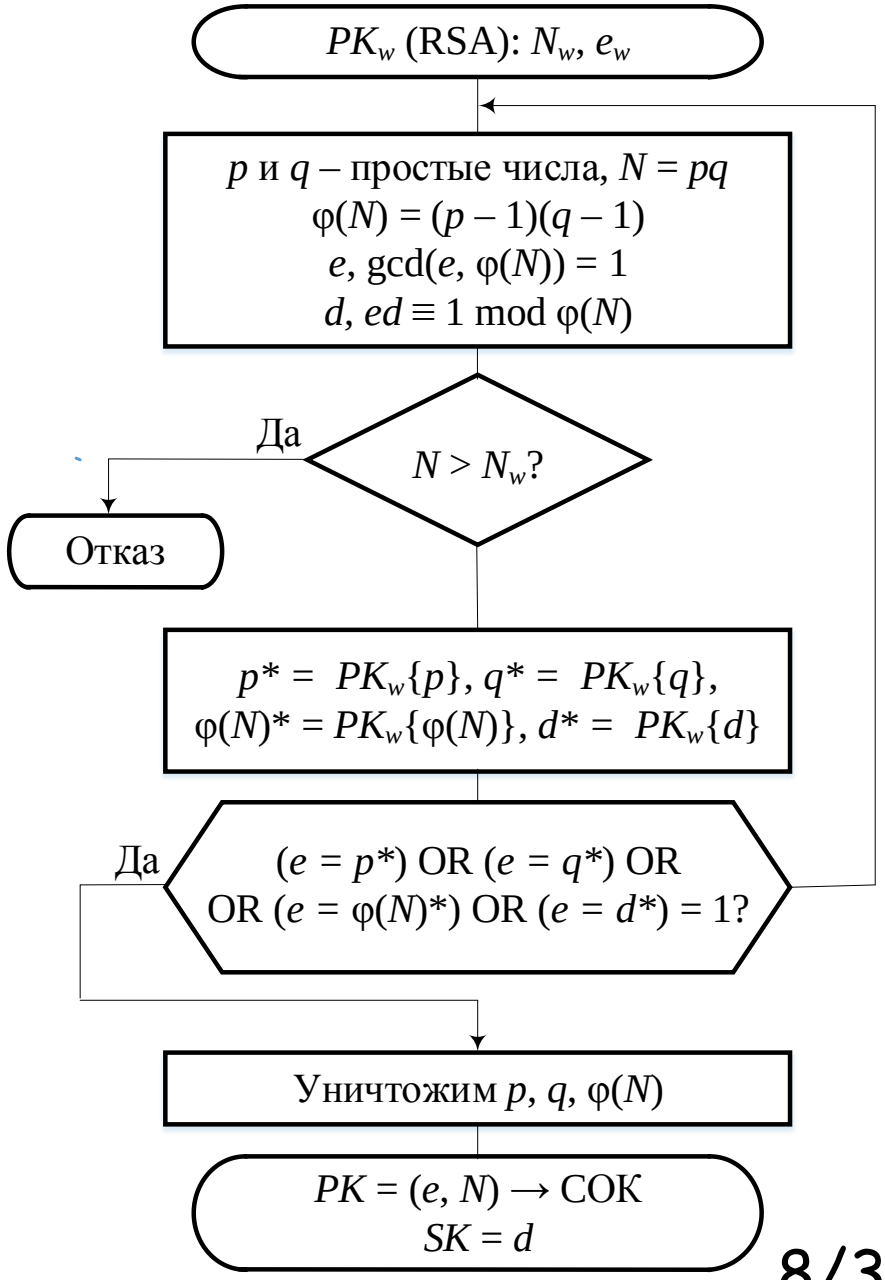
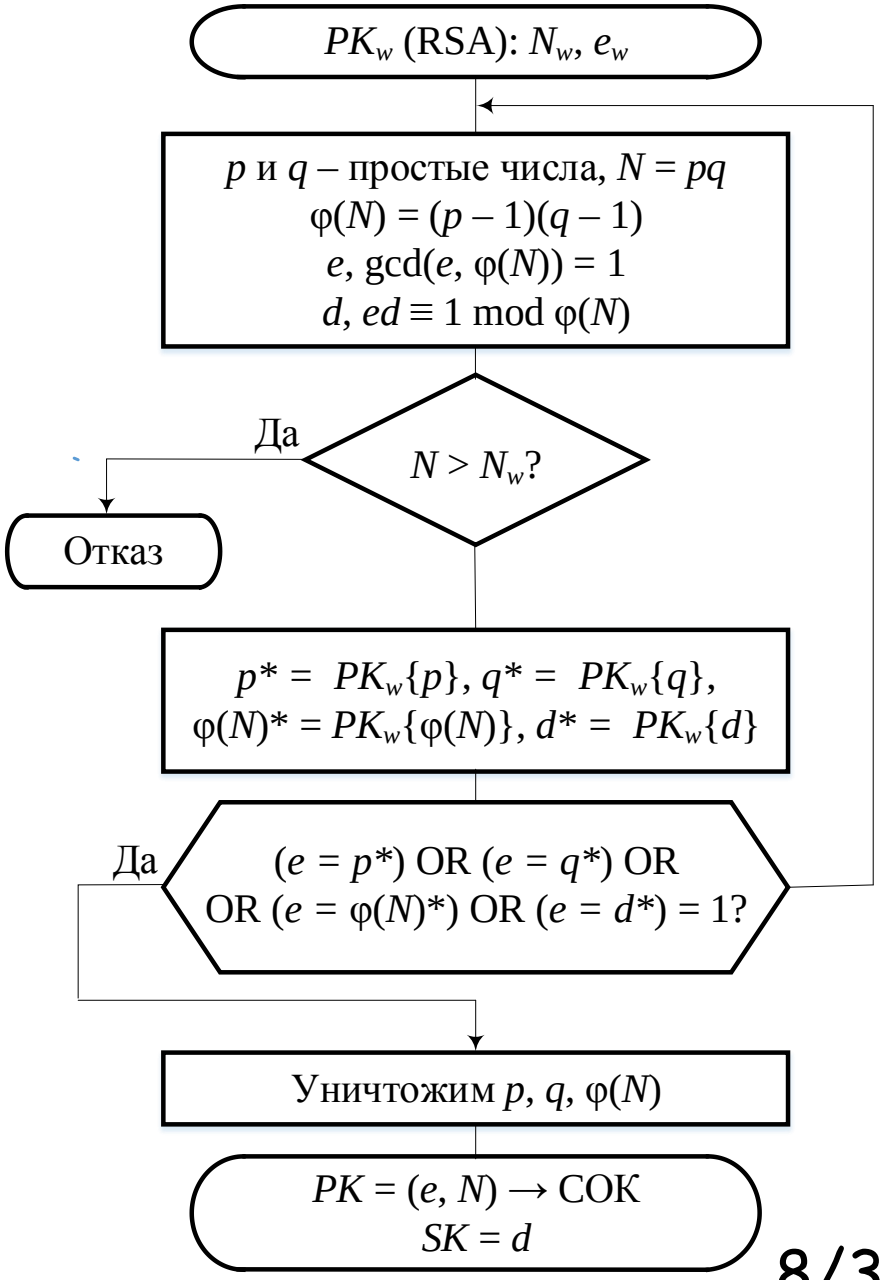


Схема алгоритма создания скрытого канала в криптосистеме RSA



Что в реальном мире будет вместо отказа ?

Модифицируйте алгоритм для случая, когда

$\exists\{PK_{wi}, SK_{wi}\}$

Схема алгоритма использования скрытого канала в криптосистеме RSA

Схема алгоритма использования скрытого канала в криптосистеме RSA

Чего не хватает в этих схемах?

Повторение: криптосистема Грэма-Шамира

1) Составляется легкая задача об укладке рюкзака – список $\{a_i\}$ (в определенных разрядах кодируются элементы супервозрастающей последовательности)
2) Выбираются числа R, S и T, такие что
$$RS \equiv 1 \bmod T,\ T > \Sigma a_i$$
3) Составляется новый список $\{b_i\}$
$$\forall i\ \ b_i = a_i \cdot R \bmod T$$
4) Уничтожаются список $\{a_i\}$ и число R
5) Список $\{b_i\}$ объявляется открытым ключом, пара (S, T) – секретным ключом
6) Шифрование – это сложение элементов списка $\{b_i\}$, которым соответствуют «1» в исходном сообщении M; расшифрование – $C \cdot S \bmod T$ с последующим решением легкой задачи об укладке рюкзака

Идея скрытого канала в ранцевой криптосистеме Грэма-Шамира

1) Программа генерации ключей PK и SK скрывает зашифрованные на ключе PK_w секретные параметры (R и S) в младших разрядах списка $\{b_i\}$ (Public Key);
2) Перехватив криптограмму, злоумышленник W может ее расшифровать:
   - с помощью ключа SK_w он вычисляет R и S;
   - затем по формуле T = RS – 1 находит T;
   - узнав секретный ключ получателя (S, T), W расшифровывает криптограмму.

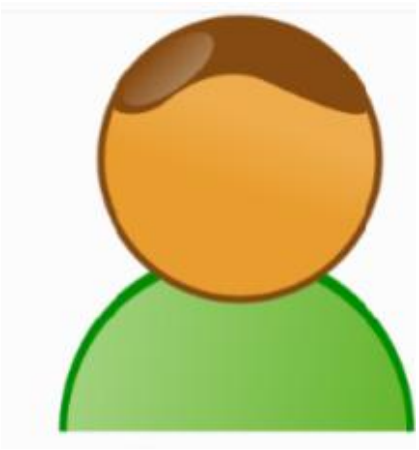
Пример реализации этой идеи

Алиса – отправитель
Боб – получатель
Ева - злоумышленник

1) Используя свой открытый ключ PK_w, Ева создает скрытый криптографический канал, модифицируя программу генерации ключей
2) Боб запускает ее и получает PK ($\{b_i\}$) и SK (S, T)
3) Алиса хочет послать Бобу секретное сообщение M, взяв из СОК открытый ключ Боба, она с его помощью шифрует сообщение M. Полученную криптограмму C Алиса отправляет канал связи
4) Ева перехватывает криптограмму C, с помощью своего секретного ключа SK_w вычисляет R и S, а затем T. Узнав секретный ключ Боба, она читает секретное сообщение.

Численный пример

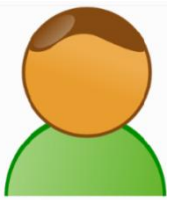
Ева



Алиса

Боб

Боб хочет получать секретные сообщения



Боб

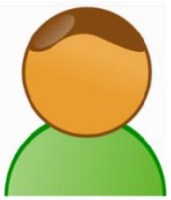
Ева

Ключи Евы

$PK_W = (7, 77)$,
$SK_W = 43$

Ева «заражает» программу генерации PK, SK, которую использует Боб

Боб хочет получать секретные сообщения



Боб

Ева

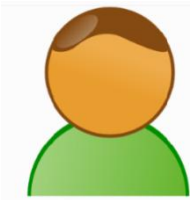
Ключи Евы

$PK_W = (7, 77)$,
$SK_W = 43$

Работает «зараженная» программа генерации ключей

Составляется
легкая задача
об укладке рюкзака:
$a_0 = 0109$
$a_1 = 0202$
$a_2 = 0407$
$a_3 = 0808$
$a_4 = 1605$

Боб хочет получать секретные сообщения



Боб

Находятся R, S и T, такие, что RS = 1 mod T:
$47 \cdot 73 = 3431 \rightarrow 47 \cdot 73 = 1 \bmod 3430$
$\rightarrow$ **R = 47, S = 73, T = 3430**

$47^7 \bmod 77 = 75$
$71^7 \bmod 77 = 36$

Ева

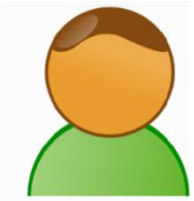
Ключи Евы

$PK_W = (7, 77)$,
$SK_W = 43$

Работает «зараженная» программа генерации ключей

Составляется
легкая задача
об укладке рюкзака:
$a_0 = 0109$
$a_1 = 0202$
$a_2 = 0407$
$a_3 = 0808$
$a_4 = 1605$

Боб хочет получать секретные сообщения



Боб

Находятся R, S и T, такие, что RS = 1 mod T:
$47 \cdot 73 = 3431 \rightarrow 47 \cdot 73 = 1 \bmod 3430$
$\rightarrow$ **R = 47, S = 73, T = 3430**

$47^7 \bmod 77 = 75$
$73^7 \bmod 77 = 17$

Ева

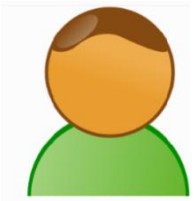
Ключи Евы

$PK_W = (7, 77)$,
$SK_W = 43$

Работает «зараженная» программа генерации ключей

Составляется
легкая задача
об укладке рюкзака:
$a_0 = 0109$
$a_1 = 0202$
$a_2 = 0407$
$a_3 = 0808$
$a_4 = 1605$

Боб хочет получать секретные сообщения



Боб

Находятся R, S и T, такие, что RS = 1 mod T:
$47 \cdot 73 = 3431 \rightarrow 47 \cdot 73 = 1 \bmod 3430$
$\rightarrow$ **R = 47, S = 73, T = 3430**

$47^7 \bmod 77 = 75$
$73^7 \bmod 77 = 17$

Ева

Ключи Евы

$PK_W = (7, 77)$,
$SK_W = 43$

Работает «зараженная» программа генерации ключей

Составляется
легкая задача
об укладке рюкзака:
$a_0 = 0109$
$a_1 = 0202$
$a_2 = 0407$
$a_3 = 0808$
$a_4 = 1605$

0100
0200
0400
0800
1605

0105
0201
0401
0803
1605

$\times 47$
$\bmod 3430$

Получается
трудная задача
об укладке рюкзака:
xxx5
xxx7
xxx7
xxx1
xxxx

$b_0 = 1505$
$b_1 = 2587$
$b_2 = 1697$
$b_3 = 0011$
$b_4 = 3405$

Алиса хочет отправить секретное сообщение M Бобу

Алиса

Читает из справочника открытый ключ Боба, шифрует сообщение M и отправляет криптограмму C Бобу

Исходное сообщение M

1
0
0
1
1

Открытый ключ Боба:

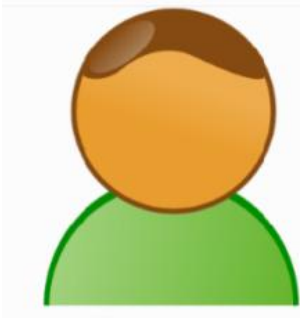
$b_0 = 1505$
$b_1 = 2587$
$b_2 = 1697$
$b_3 = 0011$
$b_4 = 3405$

Шифрование:

$$\begin{array}{r} 1505 \\ + \quad 0011 \\ \hline 3405 \\ \hline\hline 4921 \end{array}$$

Криптограмма $C = 4921$

Боб получает криптограмму, полученную из канала связи, и с помощью своего секретного ключа читает секретное сообщение



Боб

Закрытый ключ Боба:
S = 73, T = 3430

$C = 4921$

$C \times S \pmod{T} \rightarrow 4921 \times 73 =$

$= 359233 = \underline{25}13 \bmod 3430$

$25 \leftrightarrow (11001)$

Полученное сообщение
M = 11001

Ева вычисляет секретный ключ Боба по его открытому ключу, взятому из справочника, и читает секретное сообщение Алисы

Ева

Открытый ключ Боба:
$b_0 = 1505$
$b_1 = 2587$
$b_2 = 1697$
$b_3 = 0011$
$b_4 = 3405$

$$75^{43} \bmod 77 = 2^{42} \cdot 75 = 64^7 \cdot 75 = 169^3 \cdot 13 \cdot 2 =$$
$$= 15^3 \cdot 13 \cdot 2 = (-169) \cdot 2 = -338 = 385 - 338 = 47$$
$$17^{43} \bmod 77 = 17^{42} \cdot 17 = 58^{21} \cdot 17 = 19^{20} \cdot 58 \cdot 17 =$$
$$= 24^{10} \cdot 58 \cdot 17 = 37^5 \cdot 58 \cdot 17 = 40^5 \cdot 19 \cdot 17 =$$
$$= 58 \cdot 40 \cdot 19 \cdot 17 = 73$$

$$S = 73 \rightarrow T = RS - 1 = 47 \cdot 73 - 1 = 3430$$

$C = 4921$

$C \times S \pmod T \rightarrow 4921 \times 73 =$
$= 359233 = \underline{25}13 \bmod 3430$

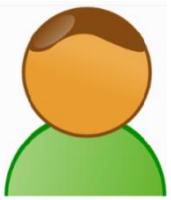
$25 \leftrightarrow (11001)$

Полученное сообщение
M = 11001

В рассмотренном примере модификация списка $\{a_i\}$ осуществляется элементарно, так как T[0] = 0

В общем случае все чуть сложнее

Боб хочет получать секретные сообщения



Боб

Находятся R, S и T, такие, что RS = 1 mod T:
$47 \cdot 73 = 3431 \rightarrow 47 \cdot 73 = 1 \bmod 3430$
$\rightarrow$ **R = 47, S = 71, T = 3336**

$47^7 \bmod 77 = 75$
$71^7 \bmod 77 = 36$

Ева

Ключи Евы

$PK_W = (7, 77)$,
$SK_W = 43$

Работает «зараженная» программа генерации ключей

Составляется легкая задача об укладке рюкзака:
$a_0 = 0109$
$a_1 = 0202$
$a_2 = 0407$
$a_3 = 0808$
$a_4 = 1605$

0100
0200
0400
0800
1605

0103
0207
0408
0807
1605

$\times 47 \bmod 3336$

Получается трудная задача об укладке рюкзака:
xxx5 $b_0 = 1505$
xxx7 $b_1 = 3057$
xxx6 $b_2 = 2496$
xxx3 $b_3 = 1233$
xxxx $b_4 = 2043$

1364->1411->1458->1505, 2728->2775->2822->2869->2916->2963->3010->
->3057, 2120->2167->2214->2261->2308->2355->2402->2449->2496,
904->951->998->1045->1092->1139->1186->1233

Алиса хочет отправить секретное сообщение M Бобу

Алиса

Читает из справочника открытый ключ Боба, шифрует сообщение M и отправляет криптограмму C Бобу

Исходное сообщение M

1
0
0
1
1

Открытый ключ Боба:

$b_0 = 1505$
$b_1 = 3057$
$b_2 = 2496$
$b_3 = 1233$
$b_4 = 2043$

Шифрование:

$$\begin{array}{r} 1505 \\ + \quad 1233 \\ \quad 2043 \\ \hline 4781 \end{array}$$

Криптограмма $C = 4781$

Ева вычисляет секретный ключ Боба по его открытому ключу, взятому из справочника, и читает секретное сообщение Алисы

Ева

Открытый ключ Боба:
$b_0 = 1505$
$b_1 = 3057$
$b_2 = 2496$
$b_3 = 1233$
$b_4 = 2043$

$$75^{43} \bmod 77 = 2^{42} \cdot 75 = 64^7 \cdot 75 = 169^3 \cdot 13 \cdot 2 =$$
$$= 15^3 \cdot 13 \cdot 2 = (-169) \cdot 2 = -338 = 385 - 338 = 47$$
$$36^{43} \bmod 77 = (36^2)^{21} \cdot 36 = 64^{21} \cdot 36 = 169^{10} \cdot 64 \cdot 36 =$$
$$= 71^5 \cdot 13 \cdot 41 = 64 \cdot 71 \cdot 13 \cdot 41 =$$
$$= 13 \cdot 6 \cdot 13 \cdot 41 = 71$$

$R = 47, S = 71 \rightarrow T = RS - 1 = 47 \cdot 71 - 1 = 3336$

$C = 4781$
$C \times S \pmod T \rightarrow 4781 \times 71 =$
$= 339451 = 2515 \bmod 3336$

$25 \leftrightarrow (11001)$

Полученное сообщение
M = 11001

Обозначения

$PK_w = (N_w, e_w)$, $SK_w = d_w$ –
соответственно открытый и закрытый
ключи создателя скрытого канала
$PK = \{b_i\}$, $SK = (S, T)$ –
соответственно открытый и закрытый
ключи пользователя
k – разрядность N_w
n – число элементов списка $\{a_i\}$
R^* – зашифрованное число R
S^* – зашифрованное число S
$X[0]$ – младший разряд числа X

Схема алгоритма создания скрытого канала в ранцевой криптосистеме

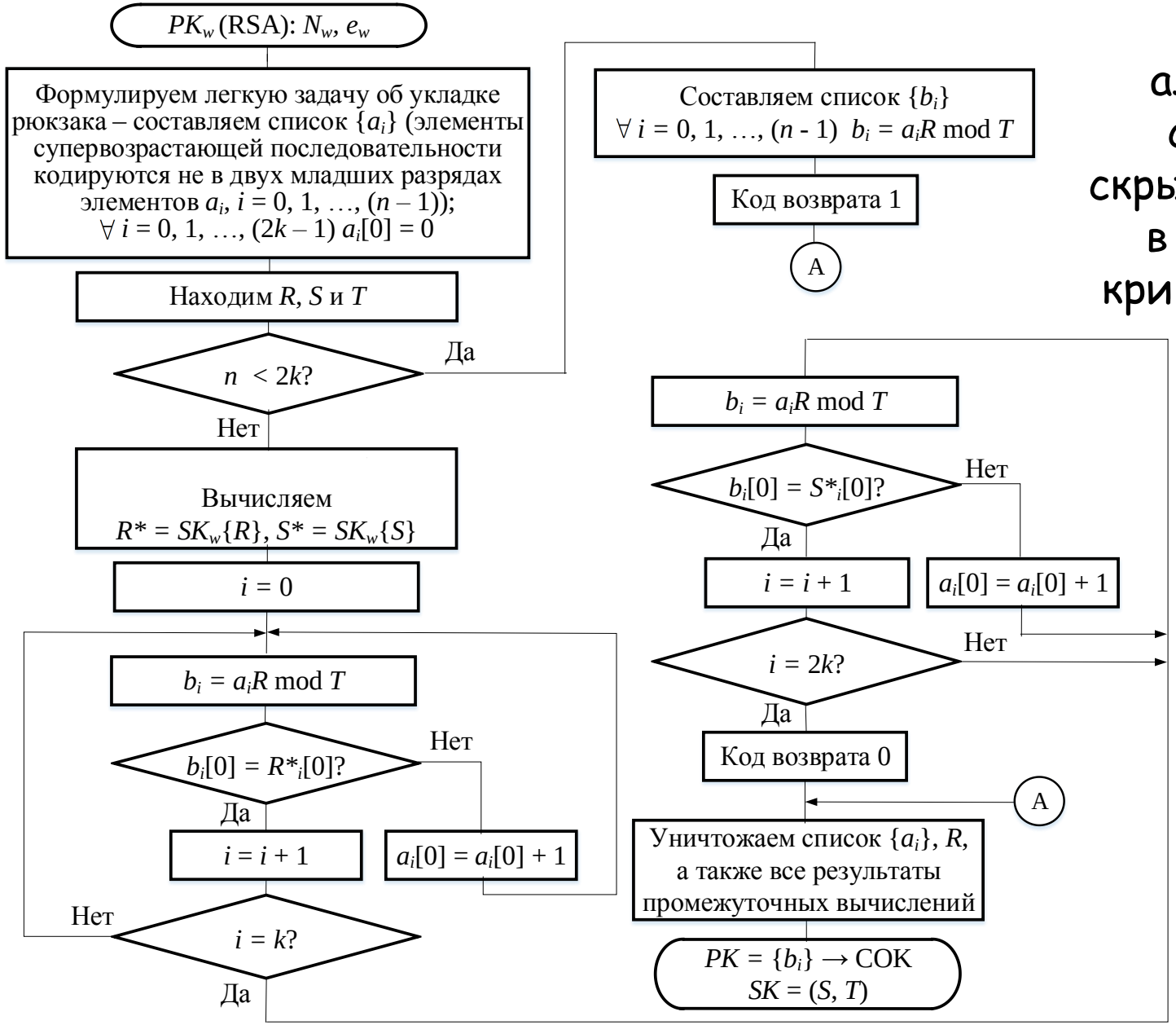
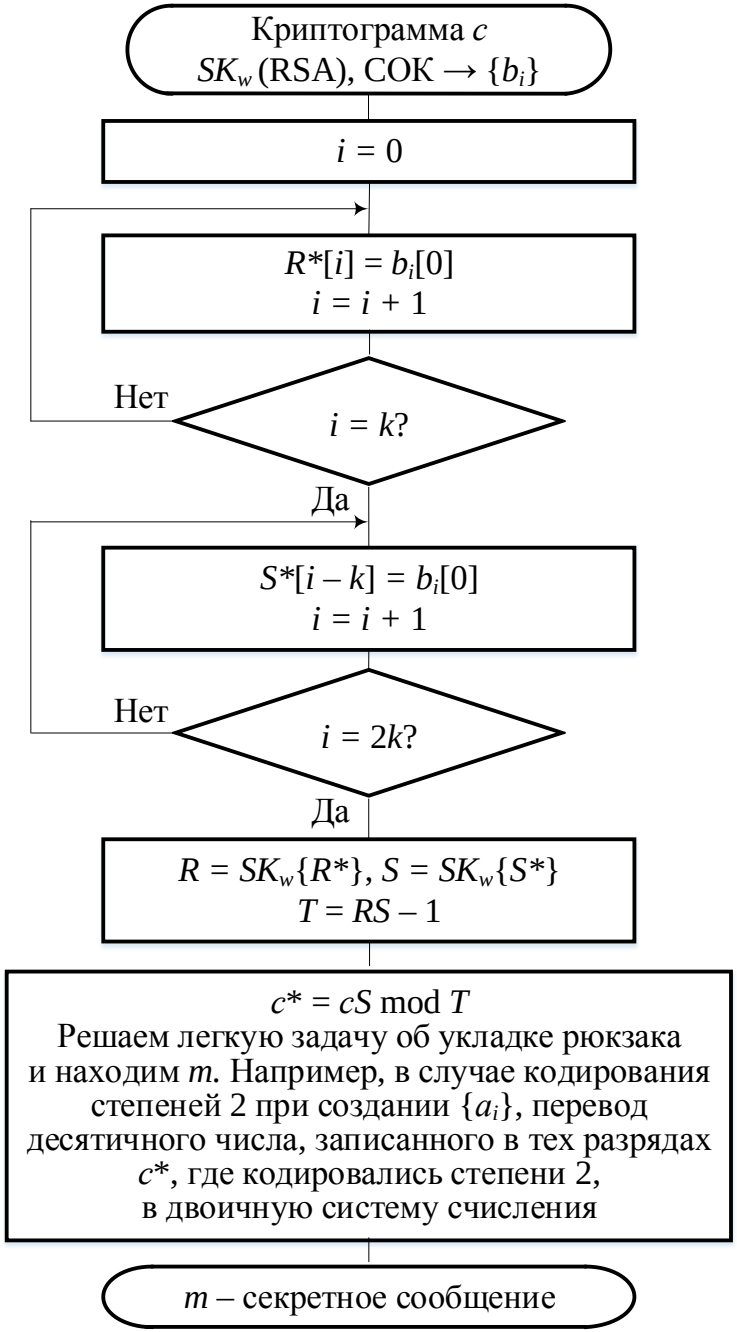


Схема алгоритма использования скрытого канала в ранцевой криптосистеме



Что вы можете сделать на КР?

1) Модифицируете мои алгоритмы создания скрытого канала в КС RSA и его использования для вычисления секретного ключа
2) Находите описание какого-либо бэкдора RSA и составляете численный пример его работы
3) Исправляете в моих алгоритмах создания и использования скрытого канала в ранцевой КС неточности и составляете численный пример
4) Модифицируете мой алгоритм создания скрытого канала в ранцевой КС в лучшую сторону и составляете численный пример
5) Составляете численный пример скрытого канала для ранцевой криптосистемы, отличной от КС Грэма-Шамира
6) Пишете код зараженной программы генерации ключей
7) Пишете код программы, которая по открытому ключу вычисляет секретный
8) Реализуете пп. 6 и 7

Варианты – кодирование 2, 3, 5, супервозрастающая последовательность

Последняя КР будет по бэкдорам. $T[0] \neq 0$!!!

The questions are welcome !