

А. П. Кирпичников, И. А. Кутепова

СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ КРИПТОСИСТЕМЫ RSA

Ключевые слова: Криптосистема, симметричная криптосистема, шифрование, расшифрование.

В данной работе рассматриваются принципы систем шифрования с открытыми ключами (асимметрических криптосистем). В частности будет разобран алгоритм поиска открытых и закрытых ключей криптосистемы RSA с целью выработки нового, более удобного алгоритма построения списка открытых и закрытых ключей, который будет работать быстрее стандартного.

Keywords: cryptosystem, symmetric cryptosystem, encryption, decryption.

This paper presents the principles of public-key cryptography systems (asymmetric cryptography systems). In particular algorithm for finding RSA cryptosystem's public and private keys will be analyzed to develop a new, more convenient algorithm for constructing a list of public and private keys that will work faster than the standard.

С давних времен человечество волновали проблемы защиты информации. Необходимость защищать информацию возникла из потребностей тайной передачи сообщений, как военных, так и дипломатических. Например, у китайцев простая запись сообщения с помощью иероглифов делала его тайным для чужестранцев [1].

Греки нашли другое необычное решение для обеспечения тайны переписки: они брили наголо голову раба и выцарапывали на ней свое послание. Когда волосы на голове раба отрастали вновь, его посылали доставить сообщение. Получатель брил голову раба и прочитывал текст. Ясно, что способ этот очень ненадежен и вдобавок неэффективен. Всякий осведомленный о таком способе связи мог схватить раба, побрить ему голову и прочесть послание. Более того, на отправку сообщения и получение ответа таким способом уходило несколько недель [2].

Юрий Цезарь придумал способ получше. Каждую букву сообщения он заменял на другую, которая в латинском алфавите отстояла от исходной на три позиции дальше. Цезарь вошел в историю, а «шифр Юлия Цезаря», как его до сих пор называют, служит примером одной из первых систем шифрования [2].

Для обозначения всей области тайной (секретной) связи используется термин «криптология», который происходит от греческого «cryptos» - тайный и «logos» - сообщение [1].

Существует два вида шифрования информации – симметричное шифрование и асимметричное относительно преобразования расшифрования. Поэтому можно выделить два класса криптосистем:

- симметричные (одноключевые) криптосистемы;
- асимметричные (двухключевые) криптосистемы (с открытым ключом).

Системы шифрования с открытыми ключами применяются для организации конфиденциальной связи между пользователями в сети. Они являются эффективными системами криптографической защиты данных.

Для шифрования и расшифрования передаваемых данных используются два разных ключа, их называют открытым и секретным (или закрытым)

ключами. Именно поэтому системы носят название асимметричные.

Открытый ключ может использовать любой пользователь (отправитель информации), который занимается шифрованием информации. Но с помощью этого ключа обратное расшифрование данных осуществить невозможно.

Для расшифровывания информации используется второй ключ – секретный и им владеет только получатель зашифрованной информации. Секретный ключ невозможно определить исходя из знания открытого ключа. Схема асимметричной криптосистемы с открытым ключом представлена на рисунке 1.

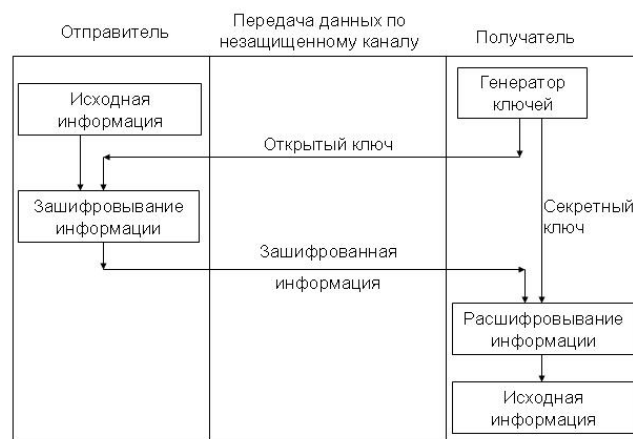


Рис. 1 – Схема асимметричной криптосистемы с открытым ключом

Особенности асимметрических криптосистем:

- Открытый ключ и зашифрованная информация (криптограмма) могут отправляться по незащищенному каналу, т.е. могут быть известны противнику.
- Алгоритмы шифрования и расшифрования являются открытыми.
- Защита информации производится за счет секретности закрытого ключа.

В 1978 году три автора: Р.Райвест (Rivest), А.Шамир (Shamir) и А.Адлеман (Adleman) предложили алгоритм шифрования данных RSA, который

был назван по первым буквам фамилий его автора. Это первая серьезная система шифрования с открытым ключом, которая используется и сегодня. Основанием криптосистемы RSA является то, что большие числа сложно разложить на множители [3].

В криптосистеме RSA открытый и закрытый ключи, исходное сообщение и зашифрованное сообщение принадлежат множеству целых чисел

$$Z_n = \{ 0, 1, 2, \dots, N-1 \}, \text{ где } N - \text{модуль:} \\ N = P * Q.$$

P и Q – случайные большие простые числа. Они хранятся в секрете для обеспечения наибольшей безопасности.

Множество Z_n с операциями сложения и умножения по модулю N образуют арифметику по модулю N .

Далее выбирается случайный открытый ключ, удовлетворяющий условиям:

- $1 < \text{секретный ключ} < \phi(N)$;
- НОД (открытый ключ, $\phi(N)$) = 1, т.е. открытый ключ и $\phi(N)$ должны быть взаимно простыми.

$\phi(N)$ - функция Эйлера, которая указывает количество положительных чисел в интервале от 1 до N .

$$\phi(N) = (P-1) * (Q-1)$$

Потом вычисляется секретный ключ (по расширенному алгоритму Евклида):

$$k_{\text{секретный}} = k_{\text{открытый}}^{-1} \pmod{\phi(N)}$$

Открытый ключ используется для шифрования данных, а секретный – для их расшифрования.

Для более детального изучения рассмотрим зависимость открытых ключей от закрытых в криптосистеме RSA на примере:

$$P = 5; \quad Q = 11; \\ N = P * Q = 55; \quad \phi(N) = (P-1) * (Q-1) = 40.$$

Для вычисления всех возможных открытых ключей необходимо найти все числа с учетом выполнения двух условий:

- $1 < \text{секретный ключ} < \phi(N)$;
- НОД (открытый ключ, $\phi(N)$) = 1;

Для получения искомого списка открытых ключей будет идти перебор всех возможных чисел, удовлетворяющих условиям [4]:

- $1 < \text{секретный ключ} < 40$;
- НОД (открытый ключ, 40) = 1.

Вспользуемся алгоритмом Евклида 39 раз для вычисления наибольших общих делителей.

Пример:

$$\begin{aligned} \text{НОД}(33, 40) &= 1 \\ 40 &= 1 * 33 + 7 \\ 33 &= 4 * 7 + 5 \\ 7 &= 1 * 5 + 2 \\ 5 &= 2 * 2 + 1 \\ 2 &= 2 * 1 + 0 \Rightarrow \end{aligned}$$

33 – открытый ключ;

Получаем следующий список открытых ключей:

Открытые ключи	1	3	7	9	11	13	17	19
----------------	---	---	---	---	----	----	----	----

Открытые ключи	21	23	27	29	31	33	37	39
----------------	----	----	----	----	----	----	----	----

Для нахождения закрытых ключей воспользуемся расширенным алгоритмом Евклида 16 раз (по числу найденных открытых ключей):

Пример:

Открытый ключ = 33

q	u ₁	u ₂	u ₃	v ₁	v ₂	v ₃
-	0	1	40	1	0	33
1	1	0	33	-1	1	7
4	-1	1	7	5	-4	5
1	5	-4	5	-6	5	2
2	-6	5	2	17	-14	1

Закрытый ключ = 17

Получаем следующие списки открытых и соответствующих им закрытых ключей:

Открытые ключи	1	3	7	9	11	13	17	19
Закрытые ключи	1	-13	-17	9	11	-3	-7	19

Открытые ключи	21	23	27	29	31	33	37	39
Закрытые ключи	-19	7	3	-11	-9	17	13	-1

Для удобства можно пересчитать все отрицательные значения по модулю 40.

$$-13 \equiv 27 \pmod{40}$$

$$-17 \equiv 23 \pmod{40}$$

$$\begin{aligned}
 -3 &\equiv 37 \pmod{40} \\
 -7 &\equiv 33 \pmod{40} \\
 -19 &\equiv 21 \pmod{40} \\
 -11 &\equiv 29 \pmod{40} \\
 -9 &\equiv 31 \pmod{40} \\
 -1 &\equiv 39 \pmod{40}
 \end{aligned}$$

Списки открытых и соответствующих им закрытых ключей будут выглядеть так [5]:

Открытые ключи	1	3	7	9	11	13	17	19
Закрытые ключи	1	-13	-17	9	11	-3	-7	19
Закрытые ключи	1	27	23	9	11	37	33	19

Открытые ключи	21	23	27	29	31	33	37	39
Закрытые ключи	-19	7	3	-11	-9	17	13	-1
Закрытые ключи	21	7	3	29	31	17	13	39

Для того чтобы проиллюстрировать полученные результаты, построим графики зависимости закрытого ключа от открытого (Рисунок 2):

При построении данного графика была обнаружена симметричность расположения точек относительно двух осей (Рисунок 2):

- $y = x$;
- $y = -x + 40$.

Построим еще несколько графиков зависимости закрытого ключа от открытого для различных P и Q (рис. 3-6).

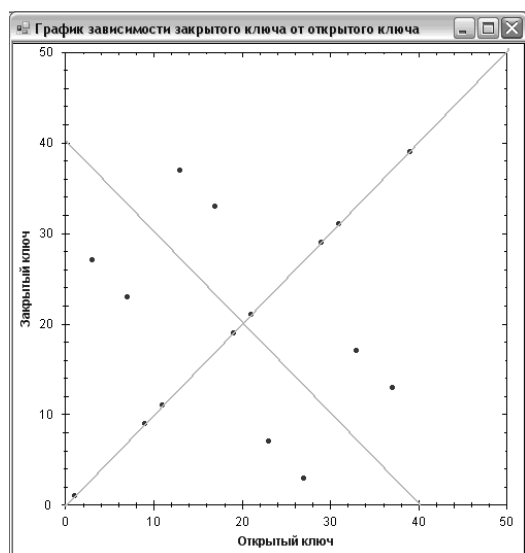


Рис. 2 – График зависимости закрытого ключа от открытого

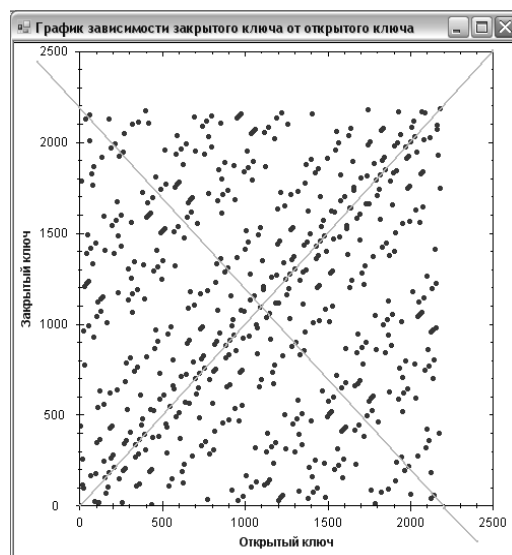


Рис. 3 - $P=29, Q=79$

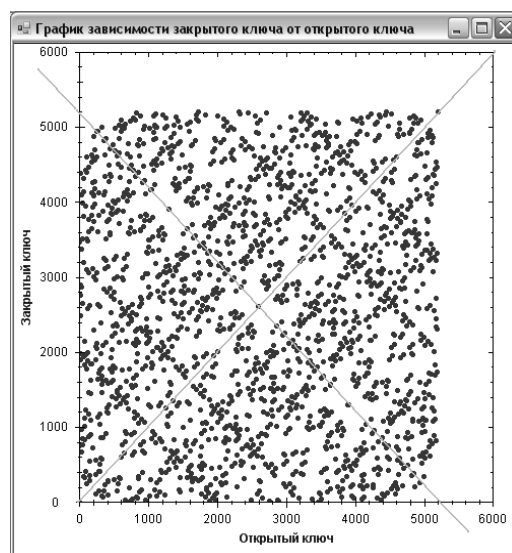


Рис. 4 - $P=53, Q=101$

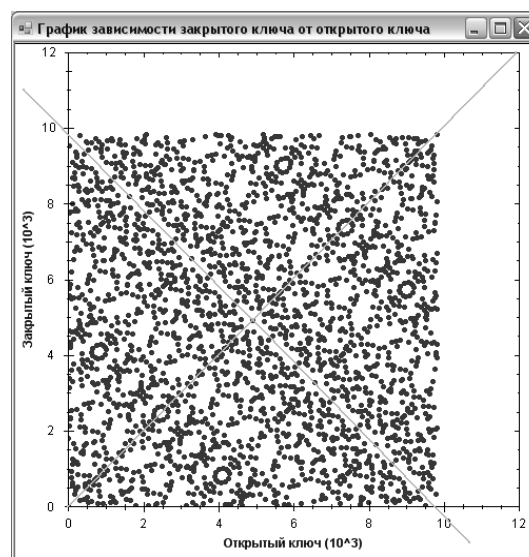


Рис. 5 - $P=79, Q=127$

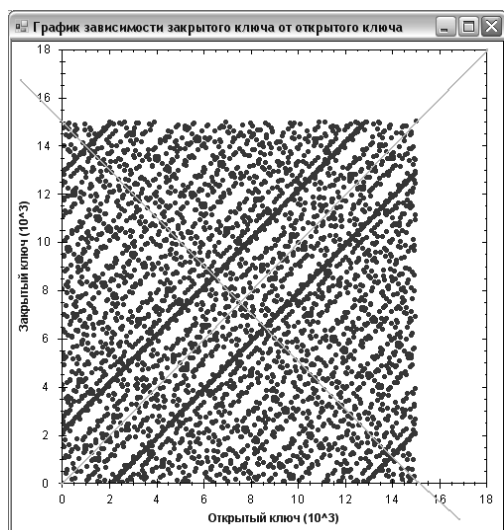


Рис. 6 - P=101, Q=151

На этих графиках тоже наблюдается симметрия, относительно двух осей.

- Для P=29, Q=79: $\phi(N) = 2184$
Оси симметрии: $y = x$;
 $y = -x + 2184$
- Для P=53, Q=101: $\phi(N) = 5200$
Оси симметрии: $y = x$;
 $y = -x + 5200$
- Для P=79, Q=127: $\phi(N) = 9828$
Оси симметрии: $y = x$;
 $y = -x + 9828$
- Для P=101, Q=151: $\phi(N) = 15000$
Оси симметрии: $y = x$;
 $y = -x + 15000$

Из вышеизложенного можно обобщить, что графики зависимости закрытых ключей от открытых в криптосистеме RSA симметричны относительно двух осей:

- $y = x$;
- $y = -x + \phi(N)$

Данную симметричность расположения точек на графике можно использовать при нахождении закрытых ключей, соответствующих найденным открытым ключам.

При вычислении каждого закрытого ключа, целесообразно находить ещё и все симметричные ему значения, что поможет ускорить вычисления. Если точка с координатами (открытый ключ, закрытый ключ) принадлежит оси симметрии, то ей будет соответствовать еще одна точка с симметричными координатами, в противном случае ей будет соответствовать еще 3 точки.

Рассмотрим принцип работы этого алгоритма на предыдущем примере, где

$$P = 5; \quad Q = 11.$$

Имеем следующий список открытых ключей:

Открытые ключи	1	2	7	9	11	13	17	19
Открытые ключи	21	23	27	29	31	33	37	39

Для нахождения закрытых ключей все так же будем использовать расширенный алгоритм Евклида:

- Открытый ключ = 1, закрытый ключ = 1
Точка с координатами (1,1)
принадлежит оси симметрии $y = x \Rightarrow$
Можно найти еще 1 точку: (39,39).
- Открытый ключ = 3, закрытый ключ = 27
Точка с координатами (3,27)
не принадлежит осям симметрии $\Rightarrow$
Можно найти еще 3 точки: (13,37), (27,3), (37,13).
- Открытый ключ = 7, закрытый ключ = 23
Точка с координатами (7,23)
не принадлежит осям симметрии $\Rightarrow$
Можно найти еще 3 точки: (17,33), (23,7), (33,17).
- Открытый ключ = 9, по закрытый ключ = 9
Точка с координатами (9,9)
принадлежит оси симметрии $y = x \Rightarrow$
Можно найти еще 1 точку: (31,31)
- Открытый ключ = 11, закрытый ключ = 11
Точка с координатами (11,11)
принадлежит оси симметрии $y = x \Rightarrow$
Можно найти еще 1 точку: (29,29)
- Открытый ключ = 19, закрытый ключ = 19
Точка с координатами (19,19)
принадлежит оси симметрии $y = x \Rightarrow$
Можно найти еще 1 точку: (21,21)

При нахождении закрытых ключей алгоритм Евклида использовался 16 раз, а с использованием осей симметрии – всего 6 раз. То есть с использованием нового алгоритма производительность можно значительно увеличить.

В данной статье были рассмотрены принципы систем шифрования с открытыми ключами (асимметрических криптосистем). В частности был разобран алгоритм поиска открытых и закрытых ключей криптосистемы RSA. Была обнаружена симметрия на графиках зависимости закрытых ключей от открытых, что позволило выработать новый алгоритм их построения, который будет работать быстрее стандартного.

Литература

1. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин, *Защита информации в компьютерных системах и сетях*. М., Радио и связь, 2001. 376 с.
2. Р. Черчауз, *Коды и шифры. Юлий Цезарь, «Энигма» и Интернет*. М., Весь мир, 2009. 320 с.
3. Нил Коблиц, *Курс теории чисел и криптографии*. М., Научное изд-во ТВП, 2001. 254 с.
4. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич, *Математические и компьютерные основы криптологии*. Минск, Новое знание, 2003. 382 с.
5. А.П. Алфёров, А.Ю. Зубов, А.С. Жидков, А.В. Черёмушкин, *Основы криптографии*. М., Гелиос АНВ, 2005. 480 с.

© **А. П. Кирпичников** – д-р физ.-мат. наук, зав. каф. интеллектуальных систем и управления информационными ресурсами КНИТУ, kirpichnikov@kstu.ru; **И. А. Кутепова** – инженер каф. интеллектуальных систем и управления информационными ресурсами КНИТУ, kutepovaira@mail.ru.