THE REVIEW TO QUESTION OF RSA ALGORITHM FOR ENCIPHERING OF INFORMATION

Baltabaev J.E. (Republic of Uzbekistan) Email: Baltabaev57@scientifictext.ru

Baltabaev Jahangir Eliwbaevich – Master,
DEPARTMENT OF APPLIED MATHEMATICS,
KARAKALPAK STATE UNIVERSITY, NUKUS, REPUBLIC OF UZBEKISTAN

Abstract: *in article problem definition information security and for their decision RSA algorithm is considered. In the last two decades, thanking first of all to inquiries of cryptography and wide circulation of the COMPUTER, researches on algorithmic questions of the theory of numbers endure the period of rough and very fruitful development. It is provided the full theoretical review of the RSA method and a short example. Results are received in the program C ++.*
Keywords: *asymmetric cryptography, the RSA system, enciphering, interpretation, an open key, the closed key.*

ОБЗОР К ВОПРОСУ АЛГОРИТМА RSA ДЛЯ ШИФРОВАНИЯ ИНФОРМАЦИИ

Балтабаев Ж.Е. (Республика Узбекистан)

Балтабаев Жахангир Елиубаевич – магистрант,
кафедра прикладной математики,
Каракалпакский государственный университет, г. Нукус, Республика Узбекистан

Аннотация: *в статье рассматривается постановка задачи защиты информации и для их решения алгоритм RSA. В последние два десятилетия, благодаря, в первую очередь, запросам криптографии и широкому распространению ЭВМ, исследования по алгоритмическим вопросам теории чисел переживают период бурного и весьма плодотворного развития. Приведен полный теоретический обзор метода RSA и короткий пример. Результаты получены в программе C++.*
Ключевые слова: *асимметричная криптография, система RSA, шифрования, расшифровка, открытый ключ, закрытый ключ.*

В середине 70-х годов произошел настоящий прорыв в современной криптографии - появление асимметричных криптосистем, которые не требовали передачи секретного ключа между сторонами. Здесь отправной точкой принято считать работу, опубликованную Уитфилдом Диффи и Мартином Хеллманом в 1976 году под названием «Новые направления в современной криптографии». В ней впервые сформулированы принципы обмена шифрованной информацией без обмена секретным ключом. Независимо к идее асимметричных криптосистем подошел Ральф Меркли. Несколькими годами позже Рон Ривест, Ади Шамир и Леонард Адлеман открыли систему RSA, первую практическую асимметричную криптосистему, стойкость которой была основана на проблеме факторизации больших простых чисел. Асимметричная криптография открыла сразу несколько новых прикладных направлений, в частности системы электронной цифровой подписи (ЭЦП) и электронных денег.

В 80-90-е годы появились совершенно новые направления криптографии: вероятностное шифрование, квантовая криптография и другие. Осознание их практической ценности еще впереди. Актуальной остается и задача совершенствования симметричных криптосистем. В 80-90-х годах были разработаны нефейстеловские шифры (SAFER, RC6 и др.), а в 2000 году после открытого международного конкурса был принят новый национальный стандарт шифрования США - AES.

1. ПОСТАНОВКА ЗАДАЧИ

Безопасность передачи данных по каналам связи является актуальной. Современные компьютерные сети не исключение. К сожалению, в сетевых операционных системах (Windows NT/XP, Novell и т.д.) иностранного производства, как следствие, из-за экспортных соображений уровень алгоритмов шифрования заметно снижен.

Задача: исследовать современные методы шифрования и их приложимость к шифрованию потоков данных. Разработать собственную библиотеку алгоритмов шифрования и программный продукт, демонстрирующий работу этих алгоритмов при передаче данных в сети.

2. АЛГОРИТМ RSA

Труды Евклида и Диофанта, Ферма и Эйлера, Гаусса, Чебышева и Эрмита содержат остроумные и весьма эффективные алгоритмы решения диофантовых уравнений, выяснения разрешимости сравнений, построения больших по тем временам простых чисел, нахождения наилучших приближений и т.д.

Возможности ЭВМ имеют определённые границы. Приходится разбивать длинную цифровую последовательность на блоки ограниченной длины и шифровать каждый такой блок отдельно [1]. Мы будем считать в дальнейшем, что все шифруемые целые числа неотрицательны и по величине меньше

некоторого заданного (скажем, техническими ограничениями) числа m. Таким же условиям будут удовлетворять и числа, получаемые в процессе шифрования. Это позволяет считать и те, и другие числа элементами кольца вычетов Z/mZ. Шифрующая функция при этом может рассматриваться как взаимно однозначное отображение колец вычетов

$$f : Z/mZ \to Z/mZ$$

а число $f(x)$ представляет собой сообщение x в зашифрованном виде.

Простейший шифр такого рода - шифр замены, соответствует отображению $f : x \to x + k \pmod m$ при некотором фиксированном целом k. Подобный шифр использовал еще Юлий Цезарь. Конечно, не каждое отображение f подходит для целей надежного сокрытия информации.

В 1978 г. американцы Р. Ривест, А. Шамир и Л. Адлеман (R.L.Rivest. A.Shamir. L.Adleman) предложили пример функции f, обладающей рядом замечательных достоинств. На её основе была построена реально используемая система шифрования, получившая название по первым буквам имен авторов -система RSA. Эта функция такова, что

1) существует достаточно быстрый алгоритм вычисления значений $f(x)$;

2) существует достаточно быстрый алгоритм вычисления значений обратной функции $f^{-1}(x)$;

3) функция $f(x)$ обладает некоторым «секретом», знание которого позволяет быстро вычислять значения $f^{-1}(x)$; в противном же случае вычисление $f^{-1}(x)$ становится трудно разрешимой в вычислительном отношении задачей, требующей для своего решения столь много времени, что по его прошествии зашифрованная информация перестает представлять интерес для лиц, использующих отображение f в качестве шифра.

3 . СИСТЕМА ШИФРОВАНИЯ RSA

Пусть m и e натуральные числа. Функция f реализующая схему RSA, устроена следующим образом

$$f : x \to x^e \pmod m. \qquad (1)$$

Для расшифровки сообщения $a = f(x)$ достаточно решить сравнение

$$x^e = a \pmod m. \qquad (2)$$

При некоторых условиях на m и e это сравнение имеет единственное решение x.

Для того чтобы описать эти условия и объяснить, как можно найти решение, нам потребуется одна теоретико-числовая функция, так называемая функция Эйлера. Эта функция натурального аргумента m обозначается $\varphi(m)$ и равняется количеству целых чисел на отрезке от 1 до m, взаимно простых с m. Так $\varphi(1) = 1$ и $\varphi(p^r) = p^{r-1}(p-1)$ для любого простого числа p и натурального r. Кроме того, $\varphi(ab) = \varphi(a)\varphi(b)$ для любых натуральных взаимно простых a и b. Эти свойства позволяют легко вычислить значение $\varphi(m)$, если известно разложение числа m на простые сомножители.

Если показатель степени e в сравнении (2) взаимно прост с $\varphi(m)$, то сравнение (2) имеет единственное решение. Для того, чтобы найти его, определим целое число d, удовлетворяющее условиям

$$de \equiv 1 \pmod{\varphi(m)}, \quad 1 \le d < \varphi(m). \qquad (3)$$

Такое число существует, поскольку $(e, \varphi(m)) = 1$, и притом единственно. Здесь и далее символом (a, b) будет обозначаться наибольший общий делитель чисел a и b. Классическая теорема Эйлера, утверждает, что для каждого числа x, взаимно простого с m, выполняется сравнение $x^{\varphi(m)} \equiv 1 \pmod m$ и, следовательно.

$$a^d \equiv x^{de} \equiv x \pmod{m}. \qquad (4)$$

Таким образом, в предположении $(a, m) = 1$, единственное решение сравнения (2) может быть найдено в виде

$$x \equiv a^d \pmod{m}. \qquad (5)$$

Если дополнительно предположить, что число m состоит из различных простых сомножителей, то сравнение (5) будет выполняться и без предположения $(a, m) = 1$. Действительно, обозначим $r = (a, m)$ и $s = m/r$. Тогда $\varphi(m)$ делится на $\varphi(s)$, а из (2) следует, что $(x, s) = 1$. Подобно (4), теперь легко находим $x \equiv a^d \pmod{s}$. А кроме того, имеем $x \equiv 0 \equiv a^d \pmod{r}$. Получившиеся сравнения в силу $(r, s) = 1$ дают нам (5).

Функция (1), принятая в системе RSA, может быть вычислена достаточно быстро. Обратная к $f(x)$ функция $f^{-1} : x \to x^d \pmod{m}$ вычисляется по тем же правилам, что и $f(x)$, лишь с заменой показателя степени e на d. Таким образом, для функции (1) будут выполнены указанные выше свойства 1) и 2).

Для вычисления функции (1) достаточно знать лишь числа e и m. Именно они составляют открытый ключ для шифрования. А вот для вычисления обратной функции требуется знать число d. оно и является «секретом», о котором речь идёт в пункте в). Казалось бы, ничего не стоит, зная число m разложить его на простые сомножители, вычислить затем с помощью известных правил значение $\varphi(m)$ и, наконец, с помощью (3) определить нужное число d. Все шаги этого вычисления могут быть реализованы достаточно быстро, за исключением первого. Именно разложение числа m на простые множители и составляет наиболее трудоемкую часть вычислений. В теории чисел несмотря на многолетнюю её историю и на очень интенсивные поиски в течение последних 20 лет, эффективный алгоритм разложения натуральных чисел на множители так и не найден [2]. Конечно, можно, перебирая все простые числа до $\sqrt{m}$, и деля на них m, найти требуемое разложение. Но, учитывая, что количество простых в этом промежутке, асимптотически равно $2\sqrt{m} \cdot (\ln m)^{-1}$, находим, что при m, записываемом 100 десятичными цифрами, найдётся не менее $4 \cdot 10^{42}$ простых чисел, на которые придётся делить m при разложении его на множители. Очень грубые прикидки показывают, что компьютеру, выполняющему миллион делений в секунду, для разложения числа $m > 10^{99}$ таким способом на простые сомножители потребуется не менее, чем 10^{35} лет. Известны и более эффективные способы разложения целых чисел на множители, чем простой перебор простых делителей, но и они работают очень медленно.

Авторы схемы RSA предложили выбирать число m в виде произведения двух простых множителей p и q, примерно одинаковых по величине. Так как

$$\varphi(m) = \varphi(pq) = (p-1)(q-1), \qquad (6)$$

то единственное условие на выбор показателя степени e в отображении (1) есть

$$(e, p-1) = (e, q-1) = 1. \qquad (7)$$

Итак, лицо, заинтересованное в организации шифрованной переписки с помощью схемы RSA, выбирает два достаточно больших простых числа p и q. Перемножая их, оно находит число $m = pq$. Затем выбирается число e, удовлетворяющее условиям (7), вычисляется с помощью (6) число $\varphi(m)$ и с помощью (3) - число d. Числа m и e публикуются, число d остается секретным. Теперь любой может отправлять зашифрованные с помощью (1) сообщения организатору этой системы, а организатор легко сможет расшифровывать их с помощью (5).

4. ПРИМЕР: ШИФРОВАНИЕ СООБЩЕНИЯ

Для наглядности вычисления, будем использовать небольшие числа. Но на практике используют очень большие числа (длиной 200-300 десятичных разрядов).

Действия объекта B:

- Берет P $= 3, Q = 11$.
- Берет модуль $N = P \times Q = 3 \times 11 = 33$.
- Берет значение функции Эйлера для $N = 33$: $\varphi(N) = (P-1) \times (Q-1) = 2 \times 10 = 20$.
- Берет в качестве открытого ключа Kв произвольное число с учетом условия: $1 < K_{\text{в}} \leq \varphi(N), mod\ (K_{\text{в}}, \varphi(N)) = 1$, допустим $K_{\text{в}} = 7$.
- Решаем значение секретного ключа $\kappa_{\text{в}}$ используя алгоритм Евклида: $\kappa_{\text{в}} \equiv = 3$.
- объект B передает объекту A пару чисел $(N = 33, K_{\text{в}} = 7)$.

Действия объекта A:

- Показывает шифруемое сообщение как последовательность целых чисел в диапазоне 0…32. Допустим буква A представляется как число 1, буква B это 2 и C $= 3$. Припустим что сообщение C A B можно показать как последовательность числе 321, то есть $M1 = 3, M2 = 1, M3 = 2$.
- Шифрует сообщение, M используя ключ $K_{\text{в}} = 7$ и $N = 33$ по формуле: $C_i = M_i K_{\text{в}}\ (mod\ N) = M_i 7 (mod\ 3)$.
- Получаем:
  - $C_i = 3^7 (mod\ 33) = 2187\ (mod\ 33) = 9$
  - $C_i = 1^7\ (mod\ 33) = 1\ (mod\ 33) = 1$
  - $C_i = 2^7 (mod\ 33) = 128\ (mod\ 33) = 29$
- Передает объекту B криптограмму: $C_1, C_2, C_3 = 9, 1, 29$.

Действия объекта B:

- Расшифровывает принятую криптограмму C_1, C_2, C_3 используя секретный ключ ≡ = 3 по формуле:$\boldsymbol{M_i = C_i^{K_{\text{в}}}\ (mod\ N)} = C_i^3\ (mod\ 3)$
  - $M_1 = 9^3\ (mod\ 33) = 729\ (mod\ 33) = 3$.
  - $M_2 = 1^3\ (mod\ 33) = 1\ (mod\ 33) = 1$.
  - $M_2 = 29^3\ (mod\ 33) = 24389\ (mod\ 33) = 2$.

Объект получил исходное сообщение, которое послал объект A.

Список литературы / References

1. *Кнут Д.* Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. М.: Мир, 1977.
2. *Schneier B.* «Applied Cryptography: Protocols, Algorithms, and Source Code in C». John Wiley & Sons, New York, 2nd edition, 1996.