МАТЕМАТИКА

УДК 511.33

О СЛОЖНОСТИ ЗАДАЧИ ФАКТОРИЗАЦИИ НАТУРАЛЬНЫХ ЧИСЕЛ

© Ш.Т.Ишмухаметов, Р.Г.Рубцова

В статье рассматривается проблема обоснования сложности алгоритмов факторизации натуральных чисел. Процедура факторизации, т.е. разложения чисел на простые множители, широко используется в современной криптографии, однако, на сегодняшний день нет эффективных высоких нижних оценок сложности этих алгоритмов, что снижает доверие к методам криптографии, основывающимся на этой процедуре (метод RSA и ему подобные).
Мы предлагаем идею практического решения этой проблемы.

В 1978 году трое американских ученых Р.Ривест, А.Шамир и Л.Альдеман [1] предложили новую идею шифрования с использованием двух различных ключей: открытого (общедоступного) и частного (закрытого) для кодирования и декодирования текстовых сообщений. Этот метод получил название метода RSA по первым буквам фамилий авторов этого метода. Для проверки стойкости своего метода авторы опубликовали фразу английского языка, зашифрованную с помощью метода RSA, и предложили широкой общественности попробовать расшифровать эту фразу. Математической основой метода RSA явилась алгоритмическая сложность задачи факторизации заданного натурального числа **N** на два составляющих его простых множителя. Для расшифровки указанной фразы необходимо было разложить 129-значное натурально число **N** на простые множители **p** и **q**, содержащие соответственно 65 и 64 десятичных знака. Лишь в 1994 году четыре автора Д.Аткинс, М.Графф, А.Ленстра и П.Лейланд [2] сообщили о дешифровке этой фразы. Процедура дешифровки была выполнена с помощью специально разработанного метода факторизации, получившего название метода квадратичного решета, и выполнялась в течение 220 дней примерно на 1600 компьютерах, объединенных сетью Интернет.

Идея использования двух различных ключей для шифрования и дешифрования сообщений явилась чрезвычайно революционной и подхлестнула интерес широкой математической общественности к науке криптографии. За короткий срок было предложено большое число новых современных алгоритмов, улучшающих и расширяющих алгоритмы RSA [3, 4, 5].

Метод RSA получил дальнейшее распространение в связи с громадным ростом локальных и глобальных компьютерных сетей. Он встроен в большинство современных Web-браузеров (Internet Explorer, Opera, Mozilla Firefox и др.) и позволяет производить шифрование конфиденциальных данных на основе протокола SSL прозрачно для пользователя. С помощью этого метода пересылаются зашифрованные пароли для доступа к Интернет-ресурсам и базам данных, номера кредитных карт для оплаты Интернет-услуг и многое другое. Также на этом методе основана идея электронно-цифровой подписи, которая законодательно поддерживается соответствующими указами многих стран, в том числе и России. По Закону 2001 года "Об электронно-цифровой подписи", одобренному Российским Парламентом, электронная подпись на документе приравнивается к собственноручной подписи автора, которая подтверждает подлинность и целостность документа.

Тем не менее, для установки полного уровня доверия к методу RSA необходимо его математическое обоснование. В частности, необходимо показать, что проблема факторизации натуральных чисел, лежащая в основе RSA, является алгоритмически сложной проблемой и имеет нижнюю оценку сложности выше полиномиальной.

Данная задача имеет важное практическое приложение и исследовалась многими математиками и специалистами-криптологами в течение уже более 30 лет. Тем не менее, несмотря на большое количество усилий в этом направлении, не было достигнуто никакого существенного прогресса. Лучшие алгоритмы факторизации, известные на сегодняшний день, имеют субэкспоненциальную сложность от длины натурального числа **N**. Например, метод квадратичного решета, разработанный в 1981 году К.Померанцем и улучшенный Девисом-Монтгомери, имеет верхнюю оценку сложности $O(e^{C\sqrt{\ln N \cdot \ln\ln N}})$ для некоторой постоянной **C**. В то же время не удается получить нижних оценок для алгоритма факторизации выше полиномиальной.

Проблема получения высоких нижних оценок для задач криптографии близка к другой известной проблеме дискретной математики **P≠NP**, ко-

торая попала в список семи золотых проблем математики, за решение каждой из которых объявлена премия в 1 млн.долларов. Трудность задачи получения высоких нижних оценок обосновывается в монографии Р.Г.Нигматуллина [6].

Нами предложена идея практического обоснования сложности факторизации натуральных чисел. Рассмотрим эту идею более подробно.

Пусть A и B – натуральные числа заданной длины, $A = a_m \;\; a_{m-1} \;\; ... \;\; a_2 \;\; a_1$, $B = b_k \;\; b_{k-1} \;\; ... \;\; b_2 \;\; b_1$ – их двоичное представление, $C = A \cdot B$, $m \geq k$. Очевидно, C должно содержать m+k двоичных разрядов. Оценим задачу нахождения чисел A и B по заданным значениям C, m, k. Существует $N_A = 2^{m-1}$ вариантов числа A длины m (от набора 100 ...0 длины m до набора 111 ...1 той же длины) и $N_B = 2^{k-1}$ вариантов числа B длины k. Общее число вариантов представления $C = A \cdot B$ обозначим через N_c. Очевидно, $N_c \leq 2^{m+k-2}$. Пусть $I = \{i_1, \;\; i_2 \;\; ... \;\; i_t\}$ – произвольное подмножество множества $\{1, \; 2, \; ... \; m+k\}$, $\overline{\sigma} = (\sigma_1, \;\; \sigma_2 \;\; ... \;\; \sigma_t\}$ – произвольный кортеж длины t, состоящий из 0 и 1. Обозначим через $N_{I,\sigma}$ число вариантов различных значений A и B, при которых произведение $C = A \cdot B$ совпадает на разрядах из множества I с кортежом $\overline{\sigma}$. Число $N_{I,\sigma}$ существенно зависит от выбора $\overline{\sigma}$. Чем меньше $N_{I,\sigma}$, тем меньше вариантов выбора чисел A и B, тем быстрее можно найти числа A и B по заданному C. В этом случае ключи C, соответствующие малым значениям $N_{I,\sigma}$, будут слабыми и поддаваться быстрому взлому.

Рассмотрим пример. Пусть A и B имеют длину m=k=4. Существует $N_c \leq 2^{m+k-2} = 2^6 = 64$ различных вариантов произведения $C = A \cdot B$. Возьмем сначала I={1} (нумерацию разрядов C установим справа налево). Выборка $\overline{\sigma}$ может принять только два возможных значения 0 и 1. Если $\overline{\sigma} = 0$, то нетрудно подсчитать, что $N_{I,\sigma} = 48$ (число вариантов 4-значных чисел A и B, произведение которых $C = A \cdot B$ совпадает в последнем разряде с 0), в то же время как для $\overline{\sigma} = 1$, это число составляет $N_{I,\sigma} = 16$. Если рассмотреть I={1, 2}, то существует 4 варианта выборки $\overline{\sigma}$: (0, 0), (0, 1), (1, 0) и (1, 1). Соответствующие $N_{I,\sigma}$ равны соответственно 32, 16, 8 и 8. Для I = {1, 2, 3} и для восьми кортежей $\overline{\sigma}$ длины 3 соответствующее распределение будет иметь вид: 20, 12, 8, 8 ,4 ,4 , 4, 4. По этим данным можно сделать вывод, что последние четыре значения кортежей $\overline{\sigma}$ дают меньшее число вариантов для A и B. Значит, если C имеет последние четыре цифры (из восьми), совпадающими с кортежами (1, 1, 0, 0), (1, 1, 0, 1), (1, 1, 1, 0) и (1, 1, 1, 1), то число различных вариантов A и B не превысит 4. В действительности, если учесть, что в криптографии используется только разложение C на простые множители A и B, то число вариантов уменьшится еще значительнее.

Такой разбор может быть легко запрограммирован и выполнен на компьютере, который сможет проанализировать, какие значения ключей являются более стойкими к атаке путем перебора. Усилив перебор более быстрыми методами факторизации типа метода квадратичного решета, можно проанализировать ключи, подверженные атакам с помощью этих методов, и построить асимптотические закономерности реального усиления стойкости ключей в зависимости от роста длины. При отсутствии теоретических оценок сложности наша методика позволяет выполнить оценку сложности процедуры факторизации, достаточную для практических целей.

* * * * * * * * * *

1. Rivest R.L., Shamir A., Aldeman L. A method for obtaining digital signatures and public-key cryptosystems // Commun. ACM. 1978. V.21, No.2. P.120-126.
2. Atkins D., Graff M., Lenstra A.K. and Leyland P.C. The magic words are squeamish ossifrage // ASIACRYPT-94, Lect. Notes in Comput. Sci. V. 917. Springer, 1995.
3. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии, М., 2002.
4. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М., 2003.
5. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: постреление и анализ. М., 1999.
6. Нигматуллин Р.Г. Нижние оценки сложности и сложность универсальных схем. Казань, 1990.

ON A COMPLEXITY OF THE PROBLEM OF FACTORIZATION OF NATURAL NUMBERS

S.T.Ishmukhametov, R.G.Rubtsova

The article deals with the problem of factorization of naturals. The procedure of factorization of natural numbers into a product of primes is widely used in modern Cryptography but in the present there are not high effective lower bounds for evaluation of the complexity of this procedure. This decreases the level of confidence into crypto methods based on the procedure (the RSA method and similar).
The idea of practical decision on detaining high lower bounds is suggested.