Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 8, Пенза-2012, с. 10-13 (http://пниэи.рф/activity/science/BIT/T8-p10.pdf)

СОПОСТАВИТЕЛЬНЫЙ АНАЛИЗ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ СУЩЕСТВУЮЩИХ МЕТОДОВ ФАКТОРИЗАЦИИ ДЛИННЫХ ЧИСЕЛ

Мацкевич А.Г., Егоров Н.С. (г. Орел)

В современных условиях глобальной информатизации компьютерные технологии получили широкое распространение практически во всех сферах деятельности человека. При этом одной из опасных угроз является угроза несанкционированного доступа к защищаемой информации со стороны внешнего и внутреннего нарушителя. Для противодействия данной угрозе применяются различные методы и средства, наиболее эффективным при этом является криптографическая защита данных.

Существует два класса криптографических алгоритмов: симметричные (один ключевой элемент легко вычисляется при наличии второго; высокая скорость преобразования данных) и несимметричные. Их особенностью является наличие двух ключевых элементов, при этом вычисление одного из них при наличии второго является вычислительно сложной задачей.

Этими задачами являются:

1) дискретного логарифмирования в конечной группе (алгоритм распределения ключей Диффи-Хеллмана);
2) дискретного логарифмирования в группе точек эллиптической кривой (ГОСТ Р 34.10-2001);
3) факторизации длинных чисел(алгоритм RSA).

Рассмотрим подробнее существующие методы факторизации длинных чисел. Существующие методы факторизации можно разделить на две группы:

1) методы, сложность которых экспоненциально зависит от длины числа:
– метод Ферма;
– ρ-алгоритм Полларда;
– (p-1) алгоритм Полларда;
2) алгоритмы, сложность которых – субэкспоненциальная.
– алгоритм Диксона;
– метод квадратичного решета;
– метод Ленстры;
– метод решета числового поля.

Метод факторизации Ферма натурального нечетного числа n состоит в поиске таких целых чисел x и y, что $x^2 - y^2 = n$, что ведет к разложению $n = (x - y) \cdot (x + y)$. Метод быстро работает, если n является произведением двух близких к друг другу сомножителей. В частности, именно поэтому в RSA требуют, чтобы разность между секретными простыми сомножителями модуля была велика. Для разложения на множители нечетного числа n ищутся два числа x и y такие, что $x^2 - y^2 = n$, или $n = (x - y) \cdot (x + y)$. При этом числа $(x + y)$ и $(x - y)$ являются множителями n, возможно, тривиальными (т.е. одно из них равно 1, а другое — n.) Равенство $x^2 - y^2 = n$ равносильно $x^2 - n = y^2$, т. е. тому, что $x^2 - n$ является квадратом. Поиск квадрата такого вида начинается с наименьшего числа, при котором разность $x^2 - n$ неотрицательна. Для каждого

значения x вычисляют $x^2 - n$ и проверяют, не является ли это число точным квадратом. Если нет, x увеличивают на единицу, иначе получено разложение.

Алгоритм Диксона – алгоритм факторизации, использующий в своей основе идею Лежандра, заключающуюся в поиске пары целых чисел x и y таких, что $x^2 \equiv y^2 (\mathrm{mod}\, n)$ и $x \neq \pm y (\mathrm{mod}\, n)$. Метод Диксона является обобщением метода Ферма.

ρ-алгоритм Джона Полларда, предложенный им в 1975 году, служит для факторизации целых чисел. Он основан на том, что вычисляется некий многочлен степени не выше второй от начального числа X – f(X). Алгоритм имеет в названии ρ потому, что эскиз итераций похож на круг с хвостом. Пусть n — составное число. Тогда существует такая константа C, что для любого положительного числа λ вероятность события, состоящего в том, что ρ-метод Полларда не найдет нетривиального делителя n за время $S_t = O(C\sqrt{\lambda\sqrt{n}}(\log n)^3)$, не превосходит величины $e^{-\lambda}$, где λ – параметр алгоритма.

P-1 метод Полларда — алгоритм разложения натурального числа N на простые множители. Алгоритм предназначен для нахождения простых делителей p, у которых p-1 хорошо раскладывается на множители, то есть имеет небольшой максимальный простой делитель. Если обозначить этот максимальный простой делитель B, то алгоритм требует $S_t = O(B \log B \log^2 N)$ действий. Метод очень быстро находит простые факторы малой и средней величины. Актуальным рекордом для P-1 метода является простой делитель числа $960^{119} - 1$, состоящий из 66 десятичных цифр.

Метод квадратичного решета (*Quadratic sieve algorithm*, *сокр.* QS) — представляет собой разновидность метода факторных баз (обобщение метода факторизации Ферма). В качестве факторной базы B берется множество простых чисел, состоящее из $p = 2$ и всех таких нечетных простых чисел p, не превосходящих заданной границы P (которая выбирается из соображений оптимальности), что n — квадратичный вычет по модулю p. Множество S целых чисел, в котором ищутся B-числа (B-число — целое число, делящееся только на простые числа из B) выглядит следующим образом:

$$S = \{t^2 - n \mid [\sqrt{n}] + 1 \le t \le [\sqrt{n}] + A\}$$

Далее, вместо того, чтобы брать одно за другим $s \in S$, и делить его на простые числа из B, берутся одно за другим каждое $p \in B$ и проверяется делимость на p (и его степени) одновременно для всех $s \in S$ -. Для построения списка всех простых p, не превосходящих A, можно использовать решето Эратосфена.

Факторизация с помощью эллиптических кривых (англ. *elliptic curve method*, сокр. *ECM*) является третьим по скорости работы после общего метода решета числового поля и метода квадратичного решета. На практике часто используется для выявления (отбрасывания) небольших простых делителей числа. Если полученное после работы алгоритма число все еще является составным, то остальные сомножители — большие числа. При увеличении количества кривых шансы найти простой сомножитель возрастают. Дано составное целое нечетное число n. Нужно найти его нетривиальный делитель d, $1 < d < n$. Идею данного подхода можно описать следующим образом:

1) случайно выбирается эллиптическая кривая

$$E : y^2 = x^3 + ax + b\,,$$

где $a, b \in Z_n$ -, и некоторая точка P=(x,y) на ней. Если попытка разложения окажется неудачной, следует взять другие *E* и *P* и повторить алгоритм сначала.

2) . Выбирается целое число *k*, делящееся на степени малых простых чисел (не больших некоторого *B*), не превосходящих *C*, то есть

$$k = \prod_{\ell \le B} \ell^{\alpha_i},$$

где $\alpha_i = \lfloor \log_l C \rfloor$ — наибольший из возможных показателей, при котором $\ell^{\alpha_i} \le C$.

3) Вычисление *kP* (все действия производятся по модулю *n*).

При применении алгоритма Евклида вместо обращения знаменателя по модулю *n*, получаем нетривиальный наибольший общий делитель этого знаменателя и *n*, то есть, собственный делитель числа *n*.

Основная идея метода решета числового поля принадлежит Джону Полларду, который предложил выполнять просеивание не в кольце целых чисел *Z*, как в методе квадратичного решета, а в алгебраическом числовом поле.

Теоретический график зависимости представлен на рисунке 1.

Несмотря на большое количество существующих методов, при определенной длине ключа данная криптосистема имеет высокую стойкость к факторизации. Поэтому задача модификации существующих методов факторизации очень актуальна. Наряду с модификацией уже существующих методов, очень важна разработка принципиально новых алгоритмов. Но тем не менее при модификации существующих методов можно добиться хороших результатов.

Основными направлениями модификации являются распараллеливание вычислительных задач (применительно к факторизации на эллиптических кривых), использование быстрых вычислений, применение новых алгоритмов, оптимизация процесса вычислений и другие. Из графика зависимости видно, что наиболее перспективными для модификации являются метод Ленстры и метод решета числового поля.

Можно выделить следующие направления модификации данных методов факторизации:

1) распараллеливание вычислений на различных эллиптических кривых в методе Ленстры.

2) применение быстрых алгоритмов манипуляции полиномами.

Обоснование и реализация модифицированных алгоритмов факторизации длинных чисел является направлением дальнейших исследований.

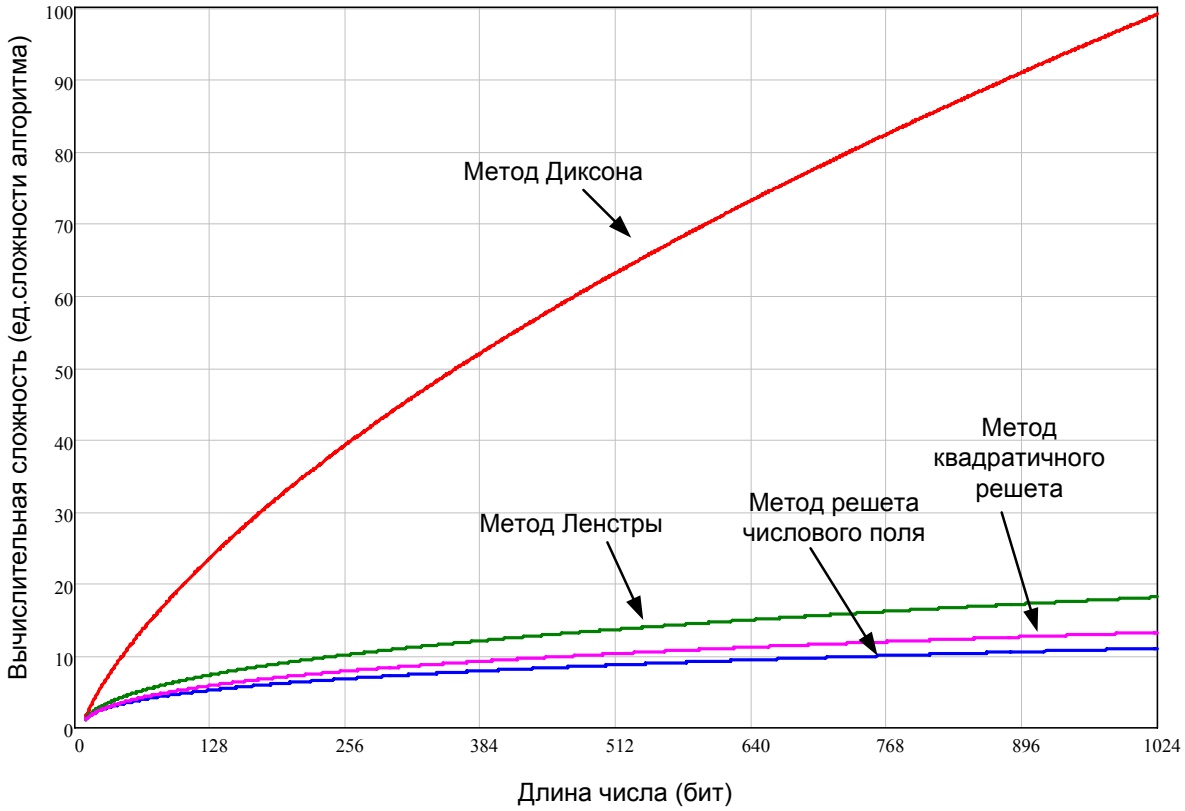

Рисунок 1. График зависимости вычислительной сложности от длины числа

Исследование существующих методов факторизации позволит изучить, проанализировать и выявить недостатки и возможные пути усовершенствования существующих алгоритмов факторизации. При исследовании алгоритмов важно выделять функциональные блоки алгоритма и их модифицировать. В методе решета числового поля очень важно быстро вычислить полином просеивания, а также построить факторные базы, методом распараллеливания.

Литература:

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, МЦНМО 2003.

2. Briggs M. E. An Introduction to the General Number Field Sieve, Blacksburg, Virginia, 1998.

Материалы поступили 09.04.2012, опубликовано в Интернет 20.04.2012 по положительной рецензии д.т.н., доц. Иванова А.И. (Пенза).