УДК 511:003.26.09

С.Д. Винничук, Е.В. Максименко

УСКОРЕНИЯ МЕТОДА ФАКТОРИЗАЦИИ ФЕРМА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПРИБЛИЖАЮЩИХ КОЭФФИЦИЕНТОВ

Предложен способ ускорения метода Ферма факторизации чисел за счет использования приближающих коэффициентов, когда вместо решения уравнения $Y^2 = X^2 - N$ в целых числах, где $N = p \cdot q$ при больших значениях отношений q/p $(q > p)$, решается уравнение $Y^2 = X^2 - KN$ для $K > 1$. Поскольку отношение q/p неизвестно, то для поиска коэффициента K предлагается использовать метод покрытия. В случае использования исключительно целых нечетных K предложен упрощенный алгоритм их выбора.

Ключевые слова: факторизация, метод Ферма, прореживание, ускорение.

Вступление. Одним из широко используемых алгоритмов в задачах криптографической защиты информации является RSA алгоритм, с чем связан повышенный интерес к его криптоанализу. Анализ известных примеров компрометации RSA алгоритма, приведенный в работе [1] показал, что все они не являются эффективнее решения задачи факторизации. Основные методы факторизации представлены в работах [2-4]. Ряд таких методов, включая метод квадратичного решета и решета числового поля, используют идеи классического алгоритма Ферма. Поэтому можно предположить, что усовершенствования метода Ферма факторизации чисел может послужить основой для ускорения и других методов факторизации, в связи с чем разработка способов ускорения метода Ферма факторизации чисел вида $N = p \cdot q$ представляется актуальной задачей. В настоящей статье исследуются способы ускорения метода Ферма за счет подбора коэффициентов a и b, приближающих к единице отношение (ap)/(bq).

Постановка задачи. Пусть задано составное нечетное число *N*, которое следует разложить на множители:

$$N = p \cdot q \tag{1}$$

где p и q некоторые нечетные числа, не обязательно являющиеся простыми. В дальнейшем будем полагать, что $p < q$. Если же числа p и q являются простыми, то представление (1) является единственно возможным. В случае составных p и q вариантов представления (1) может быть несколько. Для случая разложения на множители числа N *N* методом Ферма полагаем, что множители числа N распределены в составных p и q так, что отношение q/p является минимальным по величине.

В классическом методе Ферма для определения p и q решают уравнение

$$X^2 = N + Y^2, \tag{2}$$

где x и y – целые положительные числа. Если в уравнении (2) неизвестную *X* представить в виде $X = \left(\left\lfloor\sqrt{N}\right\rfloor + 1\right) + x = x_0 + x$, то решение уравнения (2) получают перебором значений $x = 0$, 1, 2, …, до тех пор, пока в (2) остаток $X^2 - N$ не окажется полным квадратом целого числа. А поскольку число операций в методе Ферма пропорционально числу значений x, то временная сложность алгоритма метода пропорциональна величине

$$x = X - x_0 \approx (p + q)/2 - \sqrt{N}. \tag{3}$$

Если в (3) множитель p малый (например, $p = 3{,}5$), то с ростом N число x будет расти пропорционально N, т.е. временная сложность метода Ферма $T(N) = O(N)$. Но при $Y^2 \le 2X$ решение уравнения (2) получается уже при $x = 0$. Поэтому принято считать, что метод Ферма эффективен при близких значениях p и q. В то же время в литературных источниках нет оценки такой близости. В связи с этим предлагается уточненная оценка временной сложности исходного метода Ферма и обсуждаются вопросы возможных путей ускорения этого метода.

Уточненная оценка сложности метода Ферма.

Пусть

$$q = (1+\alpha)^2 p\,. \tag{4}$$

Тогда соотношение (3) для оценки величины *x* можно представить в виде функции от p и α,

$$x = X - x_0 \approx (p+q)/2 - \sqrt{N} = (p+q)/2 - \sqrt{pq} = 0.5\left(\sqrt{q} - \sqrt{p}\right)^2 = 0.5\left((1+\alpha)\sqrt{p} - \sqrt{p}\right)^2 = \frac{p\alpha^2}{2}$$

функции от q и α,

$$x = X - x_0 \approx 0.5\left(\sqrt{q} - \sqrt{p}\right)^2 = 0.5\left(\sqrt{q} - \sqrt{q}/(1+\alpha)\right)^2 = \frac{q\alpha^2}{2(1+\alpha)^2},$$

а также представить через N и α

$$x = X - x_0 \approx 0.5\left(\sqrt{q} - \sqrt{p}\right)^2 = \sqrt{\frac{p\alpha^2}{2} \cdot \frac{q\alpha^2}{2(1+\alpha)^2}} = \frac{\sqrt{N}\alpha^2}{2(1+\alpha)}\,. \tag{5}$$

Ценность оценки (5) состоит в том, что с ее помощью можно определять число итераций в методе Ферма, а именно значение x по информации относительно α.

Пусть, например, известно, что $p < \sqrt{N} < 1.1p$. Тогда $p^2 < N = pq < 1.21p^2$, т.е. $p < q < 1.21p$ и $\alpha < 0.1$. Следовательно, число *x* оценивается сверху величиной

$$x \approx \frac{\sqrt{N}\alpha^2}{2(1+\alpha)} < \frac{0.01}{2.2}\sqrt{N}\,.$$

На основании оценки (5) при известной оценке для α возможно определить минимальное значение числа $N = N_{min}$, для которого разложение на множители возможно не более чем за x шагов метода Ферма. Действительно, пусть задано значение x и верхняя оценка для α: $0 < \alpha \le \alpha_0$. Тогда из (5) находим:

$$\sqrt{N} \approx x\frac{2(1+\alpha)}{\alpha^2} > x\frac{2(1+\alpha_0)}{\alpha_0^2} \approx \sqrt{N_{min}}$$

или, после возведения в квадрат,

$$N \approx x^2\frac{4(1+\alpha)^2}{\alpha^4} > x^2\frac{2(1+\alpha_0)^2}{\alpha_0^4} \approx N_{min}\,. \tag{6}$$

Возможные подходы к ускорению исходного метода Ферма на основании оценки (5).

Алгоритм метода Ферма можно представить как цикл, в котором перебираются значения x от 0 до $\frac{\sqrt{N}\alpha^2}{2(1+\alpha)}$, где на каждом шаге цикла определяется разность $X^2 - N$ и из нее извлекается корень. Процесс заканчивается тогда, когда корень является целым числом. Ускорение работы такого алгоритма и обеспечение повышения эффективности алгоритма метода Ферма возможно на основании следующих способов:

1. просеивания возможных значений x, т.е. отказ от проверки соотношения (2) (проверка остатка на полный квадрат) для случаев, когда иными, более простыми по вычислительной сложности, способами заранее установлено, что при таком значении *x* остаток $X^2 - N$ не может быть полным квадратом;
2. Выбора или разработки эффективных алгоритмов выполнения операций извлечения корня из $X^2 - N$ и возведения в квадрат больших чисел.
3. уменьшения коэффициента α за счет перехода от соотношения (1) к

$$KN = abN = ap \cdot bq\,, \tag{7}$$

где коэффициент $\alpha_1 = \left|\sqrt{ap/(bq)} - 1\right|$ ближе к нулю чем $\alpha = \left|\sqrt{q/p} - 1\right|$.

Способы ускорения алгоритма метода Ферма за счет просеивания возможных значений X рассматриваются в работах [5, 6]. В работе [7] представлен модифицированный метод вычисления квадратного корня. В настоящей статье обсуждаются вопросы повышения эффективности метода Ферма за счет выбора коэффициента $K = a \cdot b$ в соотношении (7) для уменьшения α.

Идея использования множителей K в соотношении (7) известна давно. Ее использовали для популяризации метода Ферма в работе [8]. Она же была положена в основу модификации метода Ферма, предложенную Шерманом Леманом в работе [9], где показано, что описанный модифицированный метод обладает временной сложностью $O(n^{1/3})$. В [9] отмечено, что уже в работе [10] исследовался вопрос поиска небольших a и b таких, что a/b близко к p/q. Если такие a и b найдены, то для $N' = abpq = ap \cdot bq$ близкими будут $a \cdot p$ и $b \cdot q$, которые уже просто определить с помощью метода Ферма. Тогда $K = a \cdot b$.

В работе [8] показано, что за время порядка $O(N^{1/3})$ можно найти подходящее K для случая $p > N^{1/3}$, хотя сам способ его поиска не описан. Поэтому эффективный поиск подходящего K остается актуальной задачей. Способы определения $K = a \cdot b$ рассматриваются ниже.

Допустимые значения приближающих коэффициентов.

Принимая $K = a \cdot b$ для достижения примерного равенства $ap \approx bq$ легко заметить, что если d наибольший общий делитель чисел a и b, причем $d > 1$, то для коэффициента α, определяемого в соотношении (4) с учетом приближающих множителей получим:

$\alpha = \sqrt{\frac{ap}{bq}} - 1 = \sqrt{\frac{da_1p}{db_1q}} - 1 = \sqrt{\frac{a_1p}{b_1q}} - 1$, где a_1 и b_1 – взаимно простые числа. Определим условия, при которых уравнение

$$X^2 = a_1b_1N + Y^2, \tag{8}$$

будет иметь решение в виде

$$X = \frac{a_1p + b_1q}{2},\ Y = \frac{|a_1p - b_1q|}{2}. \tag{9}$$

Следующее утверждение определяет требования к произведению $a \cdot b$ при взаимно простых a и b.

Утверждение 1. Если числа a и b взаимно простые то уравнение (8) имеет решение только в случаях, когда произведение $a \cdot b$ либо нечетное, либо нацело делится на 8.

Доказательство. Для доказательства утверждения 1 проанализируем три варианта:

1. произведение $a \cdot b$ нечетное, либо $ab(\mathrm{mod}8) = 0$.
2. $ab(\mathrm{mod}4) = 2$,
3. $ab(\mathrm{mod}8) = 4$.

Рассмотрим уравнение

$$\left(X^2(\mathrm{mod}8) - (abN)(\mathrm{mod}8)\right)(\mathrm{mod}8) = Y^2(\mathrm{mod}8). \tag{10}$$

В уравнении (10) $X^2(\mathrm{mod}8)$ и $Y^2(\mathrm{mod}8)$ могут принимать только значения равные 0, 1 или 4. Для первого из вариантов число $ab(\mathrm{mod}8)$ может принимать значения 0, 1, 3, 5 и 7. Для этих значений $ab(\mathrm{mod}8)$ покажем, что уравнение (8) всегда имеет хотя бы одно решение. Для этого проверим выполнение соотношения (10) при всех возможных значениях $X(\mathrm{mod}8)$. Результаты анализа приведены в табл.1, где полужирным отмечены значения $X(\mathrm{mod}8)$, являющиеся решением уравнение (10) при $ab(\mathrm{mod}8)$ равных 0, 1, 3, 5 и 7.

Таблиця 1

Определение решений уравнений (10) для варианта 1.

abN(mod8)	X(mod8)	0	1	2	3	4	5	6	7
	$X^2(\text{mod}8)$	0	1	4	1	0	1	4	1
0	$(X^2(\text{mod}8)-0)(\text{mod}8)$	**0**	**1**	**4**	**1**	**0**	**1**	**4**	**1**
	$(X^2(\text{mod}8)-0)(\text{mod}8)=Y^2(\text{mod}8)$? да – '+', нет – '–'	+	+	+	+	+	+	+	+
1	$(X^2(\text{mod}8)-1)(\text{mod}8)$	7	**0**	3	**0**	7	**0**	3	**0**
	$(X^2(\text{mod}8)-1)(\text{mod}8)=Y^2(\text{mod}8)$? да – '+', нет – '–'	–	+	–	+	–	+	–	+
3	$(X^2(\text{mod}8)-3)(\text{mod}8)$	5	6	**1**	6	5	6	**1**	6
	$(X^2(\text{mod}8)-3)(\text{mod}8)=Y^2(\text{mod}8)$? да – '+', нет – '–'	–	–	+	–	–	–	+	–
5	$(X^2(\text{mod}8)-5)(\text{mod}8)$	3	**4**	7	**4**	3	**4**	7	**4**
	$(X^2(\text{mod}8)-5)(\text{mod}8)=Y^2(\text{mod}8)$? да – '+', нет – '–'	–	+	–	+	–	+	–	+
7	$(X^2(\text{mod}8)-7)(\text{mod}8)$	**1**	2	5	2	**1**	2	5	2
	$(X^2(\text{mod}8)-7)(\text{mod}8)=Y^2(\text{mod}8)$? да – '+', нет – '–'	+	–	–	–	+	–	–	–

В случае $\text{abN}(\text{mod}8)=0$ из условия, что $N(\text{mod}8)>0$ следует, что $\text{ab}(\text{mod}8)=0$. Если же $\text{ab}(\text{mod}8)$ равно 1, 3, 5 или 7, то при нечетных $N(\text{mod}8)$ произведение $\text{abN}(\text{mod}8)=(\text{ab}(\text{mod}8)\cdot N(\text{mod}8))(\text{mod}8)$ может равнять только нечетному числу 1, 3, 5 или 7. Для всех таких значений в табл. 1 показано, что уравнение (10) имеет решение. Поэтому утверждение 1 для варианта 1 доказано.

Рассмотрим теперь случай, когда $\text{ab}(\text{mod}4)=2$, т.е. вариант 2. Если выполнено соотношение (10), то будет выполняться и соотношение

$$(X^2(\text{mod}4)-(\text{abN})(\text{mod}4))(\text{mod}4)=Y^2(\text{mod}4). \qquad (11)$$

При этом для варианта 2 при нечетном N $(\text{abN})(\text{mod}4)=2$. А поскольку в уравнении (11) $X^2(\text{mod}4)$ и $Y^2(\text{mod}4)$ могут принимать только значения равные 0 или 1, то $(X^2(\text{mod}4)-2)(\text{mod}4)$, будет равняться либо 2 (при $X^2(\text{mod}4)=0$), либо 3 (при $X^2(\text{mod}4)=1$). Но $Y^2(\text{mod}4)$ не может быть равным ни 2 ни 3. Поэтому уравнение (11) не имеет решения, т.е. не имеет решения и уравнение (8).

Пусть теперь $\text{ab}(\text{mod}8)=4$. Тогда число $\text{abN}(\text{mod}8)$ может принимать только значение 4. Определим все возможные значения $X(\text{mod}8)$, при которых уравнение (11) всегда имеет решение. Для этого проверим выполнение соотношения (11) при всех возможных значениях $X(\text{mod}8)$. Результаты анализа приведены в табл.2, где полужирным отмечены значения $X(\text{mod}8)$, являющиеся решением уравнение (11).

Таблиця 2

Определение решений уравнений (9) для варианта 3

$X(\text{mod}8)$	0	1	2	3	4	5	6	7
$X^2(\text{mod}8)$	0	1	4	1	0	1	4	1
$(X^2(\text{mod}8)-4)(\text{mod}8)$	**4**	5	**0**	5	**4**	5	**0**	5
$(X^2(\text{mod}8)-4)(\text{mod}8)=Y^2(\text{mod}8)$? да – '+', нет – '–'	+	–	+	–	+	–	+	–

Из данных таблицы 2 следует, что решение уравнения (1) возможно только при четных значениях $X(\mathrm{mod}8)$.

При этом разница $\left(X^2(\mathrm{mod}8)-(abN)(\mathrm{mod}8)\right)(\mathrm{mod}8)=\left(X^2(\mathrm{mod}8)-4\right)(\mathrm{mod}8)$, равная $Y^2(\mathrm{mod}8)$, принимает значения либо 0, либо 4. Следовательно, как $X(\mathrm{mod}8)$, так и $Y(\mathrm{mod}8)$ являются четными числами, т.е. не удовлетворяют условиям утверждения 1, поскольку имеют общий множитель 2, т.е. не являются взаимно простыми.

Утверждение 1 доказано.

В ряде случаев важным может быть случай, когда a и b одновременно являются четными.

Утверждение 2. Если одно из взаимно простых чисел a_1 и b_1 является четным, то целочисленное решение имеет уравнение

$$X^2=4a_1b_1N+Y^2, \tag{12}$$

где X и Y нечетные числа.

Доказательство утверждения 2 следует из того, что при умножении чисел a_1 и b_1 на 2 не меняется значение отношения $\frac{a_1p}{b_1q}=\frac{2a_1p}{2b_1q}$, а уравнение (12) имеет решение:

$X=\frac{2a_1p+2b_1q}{2}=a_1p+b_1q$, $Y=\frac{|2a_1p-2b_1q|}{2}=|a_1p-b_1q|$, где числа X и Y являются целыми и нечетными.

Из утверждений 1 и 2 следует, что в случае, когда $k\,\mathrm{mod}4=(ab)\,\mathrm{mod}4=2$, уравнение (8) не может иметь решения и если есть необходимость в использовании приближающих коэффициентов, пропорциональных a и b, то каждое из взаимно простых a и b достаточно умножить на 2.

Интервальный поиск приближающих коэффициентов или метод покрытия

Пусть $p<q$ и $a<p$. Если b^* такое, что $a/b^*=p/q$, то $b^*=aq/p$, то произведение $ab^*N=a\cdot\frac{aq}{p}\cdot p\cdot q=a^2q^2$, т.е. является полным квадратом и число шагов по поиску пробного значения X равно 1. Но при $НОД(p,q)=1$ число b^* не может быть целым. Поэтому b выбирается как близкое целое к aq/p. Но поскольку p и q неизвестны, то необходимо осуществлять поиск a и b в широком диапазоне их значений. При этом существенным является вопрос: а сколько вариантов a и b следует найти, чтобы гарантированно разложить на множители число N? Для ответа на этот вопрос введем понятие интервал действия коэффициента K в соотношении (7).

а. Интервал действия действительного коэффициента K.

Пусть задано некоторое ограничение на предельное значение x в соотношении (5) равное xx. Например, в случае, когда за 1 сек. машинного времени анализируется $5*10^9$ значений X, то в качестве xx можем выбрать число $5*10^9$. Определим область значений коэффициента K, при произвольном из значений которого в соответствии с формулой (5) выполнены ограничения:

$$\begin{cases} xx>\sqrt{NK}\cdot\alpha^2/2/(1+\alpha)=0.5\cdot\sqrt{pqK}\cdot\left(\sqrt{\frac{q}{pK}}-1\right)^2/\sqrt{\frac{q}{pK}}, & q>pK \\ xx>\sqrt{Nk}\cdot\alpha^2/2/(1+\alpha)=0.5\cdot\sqrt{pqK}\cdot\left(\sqrt{\frac{pK}{q}}-1\right)^2/\sqrt{\frac{pK}{q}}, & q<pK \end{cases},$$

которые преобразуются к виду:

$$\begin{cases} 2xx > pK\left(\sqrt{\frac{q}{pK}}-1\right)^2 = p\left(\sqrt{\frac{q}{p}}-\sqrt{K}\right)^2 = p\left(\alpha+1-\sqrt{K}\right)^2, & q > pK \\ 2xx > q\left(\sqrt{\frac{pK}{q}}-1\right)^2 = \left(\sqrt{pK}-\sqrt{q}\right)^2 = p\left(\sqrt{\frac{q}{p}}-\sqrt{K}\right)^2 = 0.5\cdot p\left(\alpha+1-\sqrt{K}\right)^2, & q < pK \end{cases}. \quad (13)$$

Первое из уравнений (13) определяет значения K, при которых $q > pK$, т.е. при $K < q/p$ или $\alpha > \sqrt{K}-1$. А второе – при $K > q/p = (1+\alpha)^2$ или $\alpha < \sqrt{K}-1$. Следовательно, $\frac{2xx}{p} > \left(\alpha+1-\sqrt{K}\right)^2$, $\sqrt{\frac{2xx}{p}} > \left|\alpha+1-\sqrt{K}\right| = \left|\sqrt{K}-\alpha-1\right|$ или $-\sqrt{\frac{2xx}{p}} < \sqrt{K}-\alpha-1 < \sqrt{\frac{2xx}{p}}$, т.е. K принадлежит множеству

$$K \in \left(\max\left[1, \left(\alpha+1-\sqrt{\frac{2xx}{p}}\right)^2\right]^2, \left(\alpha+1+\sqrt{\frac{2xx}{p}}\right)^2\right) = (K_{min}, K_{max}), \quad (14)$$

которое, в дальнейшем, будем называть интервалом действия коэффициента K.

Учитывая то, что величина p неизвестна, заменим ее на $\sqrt{N}$ в предположении, что отношение q/p близкое к единице. Тогда условие (14) превратится в более жесткое ограничение для k вида

$$K \in \left(\max\left[1, \left(\sqrt{\frac{q}{p}}-\sqrt{\frac{2xx}{\sqrt{N}}}\right)^2\right]^2, \left(\sqrt{\frac{q}{p}}+\sqrt{\frac{2xx}{\sqrt{N}}}\right)^2\right) = (K_{min}, K_{max}) \quad (15)$$

или

$$\sqrt{K} \in \left(\max\left(1, \sqrt{\frac{q}{p}}-\sqrt{\frac{2xx}{\sqrt{N}}}\right), \sqrt{\frac{q}{p}}+\sqrt{\frac{2xx}{\sqrt{N}}}\right) = \left(\sqrt{K_{min}}, \sqrt{K_{max}}\right), \quad (16)$$

в которых из предположения о значении отношения q/p уже можно определять K_{min} и K_{max}. Покажем это на конкретном примере.

Пусть задано число N и мы ищем его делители q и p при условии, что $q/p < K$. Тогда на полуинтервале $[1, K)$ будем выбрать последовательность коэффициентов K, интервалы действия которых покрывают полуинтервал $[1, K)$, где в пределах каждого интервала действия число пробных x не будет превышать xx. Рассмотрим пример выбора коэффициентов K в случае $N = 999247$ при ограничении $xx < 50$, $q/p < 7$.

Первоначально исходим из того, что значение $K_1 = 1$ при $(q/p)_1 = 1$, $a = b = 1$. Проверяем соотношение (8) для первых $xx = 50$ значений X, начиная с x_0. Если решение не получено, то отношение q/p превышает $K_{max,1}$, которое определяем из соотношения (16)

$$K_{max,1} < \left(\sqrt{\frac{q}{p}}+\sqrt{\frac{2xx}{\sqrt{N}}}\right)^2 < \left(1+\sqrt{\frac{2\cdot 50}{1000}}\right)^2 = \left(\sqrt{0.1}+1\right)^2 = 1.732. \quad (17)$$

Следовательно, в результате первых 50 пробных значений *x* проверены все варианты p, для которых $q/p \le 1.732$. Поэтому на следующем шаге умножим p на 1.732 одновременно умножив и N на 1.732, и определим аналогично (17) величину k_2

$$K_2 < \left(\sqrt{\frac{q}{p\cdot K_{max,1}}}+\sqrt{\frac{2xx}{\sqrt{N\cdot K_{max,1}}}}\right)^2 \approx \left(1+\sqrt{\frac{2\cdot 50}{1000\cdot 1.316}}\right)^2 = (0.276+1)^2 \approx 1.627,$$

а по нему $K_{max,2} = 1.732\cdot 1.627 \approx 2.818$. При дальнейших вычислениях получим:

$$K_3 \approx \left(1+\sqrt{\frac{2\cdot 50}{1000\cdot 1.679}}\right)^2 = (1+0{,}244)^2 = 1.548,$$

$$K_{max,3} = 2.818\cdot 1.548 = 4.361$$

$$K_4 \approx \left(1+\sqrt{\frac{2\cdot 50}{1000\cdot 2.088}}\right)^2 = (1+0.219)^2 = 1.489,$$

$$K_{max,4} = 4.361\cdot 1.489 = 6.478$$

а в общем виде

$$K_{i+1} \approx \left(1+\sqrt{\frac{2\cdot xx}{\sqrt{N\cdot K_{max,i}}}}\right)^2. \qquad (18)$$

$$K_{max,i+1} = K_{max,i}\cdot K'_{i+i}$$

Таким образом потребовалось четыре операции умножения числа N на корректирующие множители для покрытия отношения $q/p < 7$ и числа пробных значений $x \le xx \le 50$ для разложения на множители числа 999247. Без учета процедуры прореживания это потребовало менее 200 проверок выполнения равенства в уравнении (2), хотя 999247 = 383·2609, отношение $q/p \approx 6.812$ и для метода Ферма требуется анализировать 498 пробных значений X.

б. Оценка временной сложности метода покрытия

В заглавии подраздела 5.1 специально отмечалось, что корректирующий множитель является действительным, хотя решение задачи необходимо получать в целых числах. Поэтому каждый раз после определения значения K_{max} его необходимо представлять в виде $K_i N$ и вместо K_{max} рассматривать число abN. Но такой упрощенный подход дает возможность оценить минимальное время, необходимое для разложение чисел на множители модифицированным методом Ферма.

Теоретическая оценка (18) является приближенной и сложной для определения числа

$$M(\log_2 N, xx, \log_2 K) = M(n, xx, k) \qquad (19)$$

элементов последовательности значений $K_i N$ при определении решения уравнения (8), где предельное значение отношения q/p меньше некоторого значения K. Максимальная величина K может равняться $N/9$ при $p = 3$. Поэтому для определения числа элементов в последовательности значений $K_i N$ (а на его основе оценки вычислительной сложности модифицированного метода Ферма) использовались численные эксперименты. В численных экспериментах в качестве исследуемых параметров использовались:

- число n двоичных разрядов $N (n = \log_2 N)$;
- значение xx;
- отношение $K = q/p$.

При расчетах с фиксированными N и xx определялись $M(n, xx, k)$ для разных значений K, не превышающих некоторое K_{max}. Для удобства представления результатов, а также их сравнений, числа K принимались равными степени двойки. При исследованиях влияния xx на $M(n, xx, k)$ значения xx также принимались равными степени двойки. При фиксированных значениях N, xx и K числа $M(n, xx, k)$ определялись по количеству последовательных вычислений.

$$
\begin{aligned}
x_i^0 &= \sqrt{N_i} \\
y_i &= \sqrt{\left(x_i^0 + xx\right)^2 - N_i} \\
q_i &= x_i^0 + y_i \\
p_i &= x_i^0 - y_i \\
K'_{i+1} &= q_i / p_i \\
K_{i+1} &= K_i \cdot K'_{i+1} \\
N_{i+1} &= N \cdot K_{i+1}
\end{aligned}
\quad . \qquad (20)
$$

В ходе вычислений при достижении величиной K_i текущего значения K в файл выводились значения $M(n, xx, k)$ а по ним строились ряд Excel - диаграмм.

Результаты исследований влияния числа xx на $M(n, xx, k)$ при $K_{max} = N/1024$ представлены диаграммами рис.1-2 с использованием логарифмической шкалы значений по всем переменным.

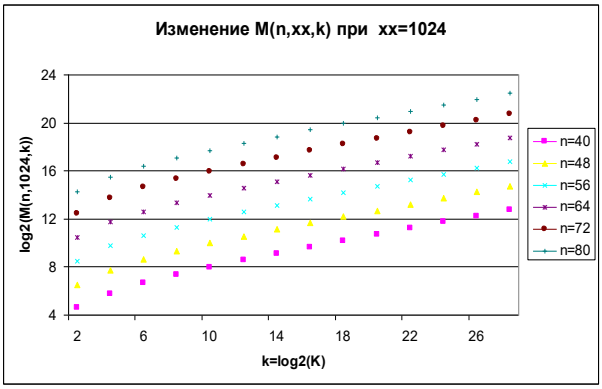

Рис.1

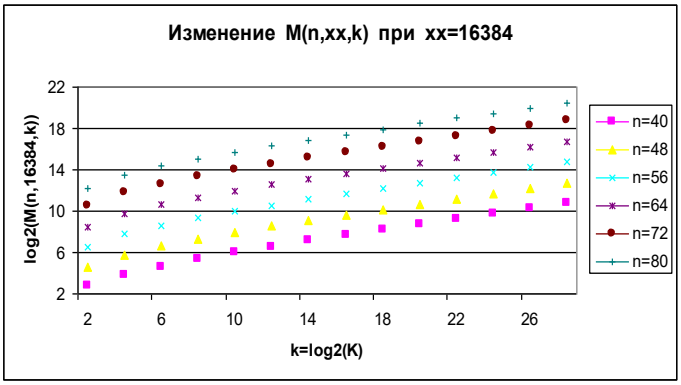

Рис.2

Анализ данных, иллюстрируемых на рис. 1-2, показывает, что при увеличении числа разрядов N растут и значения $M(n, xx, k)$, но за счет увеличения xx в 4 раза число $M(n, xx, k)$ в два раза уменьшается.

Если для факторизации произвольных чисел N при значениях $p < N^{1/4}$ использовать деление N/p до $p < N^{1/4}$, а при $p > N^{1/4}$ искать p модифицированным методом Ферма, то временная сложность такого комплексного метода будет определяться соотношением между N и xx. По данням численных экспериментов, представленных на диаграмме рис.2, при $xx = 2^{12}$ и $q/p < N^{1/2}$ величина $\log_2(M(n, xx, k = n/2))$ равняется: 24.75 при $n = 80$, 21.75 при $n = 72$, 18.75 при $n = 64$. При этом отношение 80/24.75>72/21.75> 64/18.75. Это отношение уменьшается при меньших N.

При $xx = 2^{14}$ и $q/p < N^{1/2}$ величина $\log_2(M(n, xx, k = n/2))$ равняется: 24.75 при $n = 80$, 20.75 при $n = 72$,, 17.75 при $n = 64$, (данные представлены на диаграмме рис.2). При этом отношение 80/23.75>72/20.75>64/17.75 и оно уменьшается при меньших N .Очевидно, что путем подбора xx для фиксированного N при $\log_2(N^{1/2})$ можно достичь числа $M(n, xx, k)$, не превышающего $N^{1/4}$. Данные о влиянии xx на $M(n, xx, k)$ в случае фиксированного N представлены на диаграмме рис.3, где значения $\log_2(M(n, xx, k))$ определялись по заданным значениям xx и $\log_2 K$.

На рис. 3 заметен более медленный рост $\log_2(M(n,xx,k))$ по сравнению с $\log_2 K$ при больших значениях соотношений q/p: при увеличении $\log_2 K$ на единицу величина $\log_2(M(n,xx,k))$ увеличивается на 1/4. Но при этом для максимального $\log_2 K = 47$ значения $\log_2(M(n,xx,k))$ примерно всего в два раза меньше $\log_2 K$, где при $xx = 1024$ $\log_2(M(n,xx,k)) = 0.5 \cdot \log_2 K$. Если предположить, что $q/p < N^{1/2}$, Экспериментально определено, что при $q/p < N^{1/2}$ для числа $N \le 2^{72}$ число шагов $M(n,xx,k)$ не превысит $N^{1/4}$ при $xx = 2^{16}$. При $N \le 2^{80}$ $M(n,xx,k)$ не превысит $N^{1/4}$ при $xx = 2^{22}$.

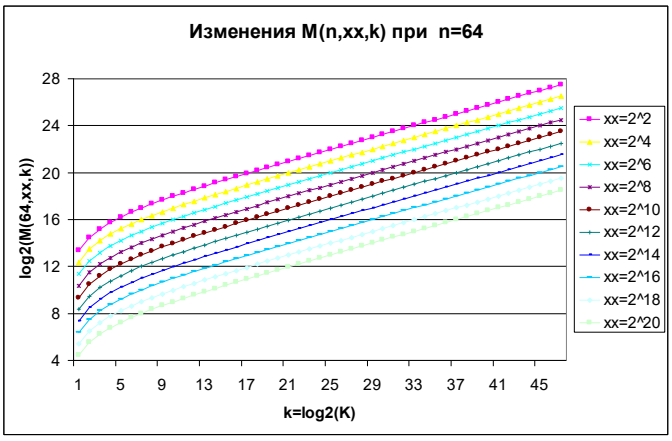

Рис.3.

Уменьшить влияние xx на $M(n,xx,k)$ при росте N можно за счет увеличения отношений q/p, полагая $p > N^{1/3}$. Тогда $q/p > N^{1/3}$ и для разложения чисел на множители можно воспользоваться модифицированным методом Ферма для $q/p > N^{1/3}$ и ρ-методом Полларда для отношений $q/p < N^{1/3}$.

Известно, что временная сложность ρ-метода Полларда оценивается величиной $O(p^{1/2})$ [11]. Поэтому временная сложность ρ-метода Полларда для этого случая $q/p < N^{1/3}$ будет величиной порядка $O(N^{1/6})$. В таком случае можно утверждать, что при $q/p < N^{1/3}$ с помощью ρ-метода Полларда можно факторизовать числа порядка 2^{120} и больше. Оценим теперь предельное значение числа N, которое можно факторизовать в случае $q/p > N^{1/3}$ модифицированным методом Ферма.

Расчетным путем была проведена оценка возможности разложения на множители чисел порядка 2^{100} при xx=21.7e+09. Число xx определено как количество значений X, обрабатываемых при определенных в [6] с учетом прореживания за 1 сек [6].

Согласно полученным данным произвольное $N \le 2^{100}$ с учетом использования действительных значений приближающих коэффициентов K_i можно разложить за время, не превышающее 58125 сек (примерно 16 часов) на ПК с следующими характеристиками: тактовая частота 2.4 GHz, ОЗУ 6 ГБ, 32-разрядная операционная система. Но при решения уравнения (8) все коэффициенты K_i представляются рациональным числом a/b. Тогда вместо числа $K_i N$ рассматривается число abN, для которого диапазон покрытия существенно меньше, а число шагов $M(n,xx,k)$ соответственно больше. Следовательно, приведенная оценка времени расчета является заниженной. Для получения верхней оценки воспользуемся следующим алгоритмом.

На первом этапе используем $K_1 = 1$ и $K'_{i+1} = 1$ до тех пор, пока отношение q/p не превзойдет 3. Далее принимаем $K_2 = 3$ и при $K'_{i+1} = 1$ используем его до тех пор, пока отношение q/p не станет больше 5. И так далее до тех пор, пока при некотором K_{i0} за один шаг вычислений (20) число K не увеличится больше чем на единицу. Тогда на всех шагах разложения числа N будет использовано целое нечетное K, но увеличится число шагов вычислений $M'(n,xx,k)$ для соотношений (20). Для определения их числа были проведены численные эксперименты.

Отметим, что число пробных значений X, обрабатываемых с учетом прореживания за 1 секунду $xx = 21.7e+09$, получено при использовании базового основания модуля $bb = 61261200$, характеризующееся минимальным значением коэффициента ускорения $z \approx 337$. С увеличением bb и ростом z вычислительные затраты будут убывать, т.е. за 1 секунду будет обрабатываться с учетом прореживания большее число пробных X. Следовательно, можно утверждать, что модифицированный метод Ферма позволяет разложить на множители числа порядка 2^{100} за приемлемое время при отношениях $q/p < 2^{34}$.

Для чисел порядка 2^{110} при $xx = 21.7e+09$ и отношениях $q/p < 2^{37}$ аналогичное время разложения оценивается сверху 1767787 секундами, что соответствует 491 часу машинного времени.

Выводы

Модификация метода Ферма, включающая алгоритмы просеивания пробных значений X и использование корректирующих множителей, позволила за приемлимое время разлагать на множители числа порядка 2^{100} при $q/p > N^{1/3}$. Если в случае $q/p < N^{1/3}$ воспользоваться ρ-методом Полларда, то с помощью такого комплексного метода возможна факторизация чисел порядка 2^{100} при произвольном соотношении q/p, что превышает предел факторизации чисел методами Ферма не менее чем на 10 двоичных разрядов [13].

Предложенный модифицированный метод Ферма существенно проигрывает по характеристикам временной сложности методам квадратичного решета и решета числового поля. Но эти методы основаны на идее метода Ферма. Поэтому предложенные новые идеи ускорения метода Ферма могут быть использованы и для их ускорения.

Литература

1. Daniel R. L. Brown. Breaking RSA May Be As Difficult As Factoring. – [Электронный ресурс]. Режим доступа: http://www.pgpru.com/novosti /2005/1026vzlomrsabezfaktorizaciirealennoneeffektiven – Название с экрана.

2. Василенко О.Н. Теоретико – числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328с.

3. Song Y. Yan Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) / Y. Yan Song. – Springer, 2009. – 372 pp.

4. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел: учебное пособие. – Казань: Казан. ун., 2011. – 190 с

5. Винничук С. Д. Многократное прореживание для ускорения метода факторизации Ферма при неравномерных шагах для неизвестной / С.Д. Винничук, Е.В. Максименко // Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка: Зб. наук. пр. – К.: Век+. – 2016. – № 64. – С. 13-24.

6. Максименко Е.В. Выбор эффективного базового основания модуля при многократном прореживании пробных значений в методе факторизации Ферма с неравномерным шагом / Е.В. Максименко // Інформатика та математичні методи в моделюванні. – 2016. – Том 6. – №3. – С. 270-279.

7. Винничук С. Д. Методы извлечения корня с остатком из многорозрядных чисел для решения задач ассиметричной криптографии / С. Д. Винничук, О.В. Корнейко, Е.В. Максименко // Захист інформації. – 2016. Том 18. – №4. – С. 336-345.

8. Кордемский Б.А. Так или не так действовал Ферма? (О факторизации чисел). // Научно-популярный физико-математический журнал "Квант". –1972. – №7. – С. 11-13.

9. Lehman R. S. Factoring Large Integers // Math. Comp., 1974. V. 28, pp. 637–646.

10. Lawrence F. W. Factorisation of numbers. Messenger of Math, 1895. V. 24, pp. 100-109.10. 11.McKee J. Speeding Fermat's factoring method // Math. Comp. 1999. V. 68 (228). P. 1729—1737.

11. Кормен Т. Алгоритмы: построение и анализ / Ч. Лейзерсон, Р. Ривест, К. Штайн. 2-е изд. – М.: Вильямс, 2011. – 1296 с.

12. Кнут Д. Искусство программирования. Т. 2. Получисленные методы. 3-е изд. - М.: Вильямс, 2001. – 788 с.

Надійшла 01.03.2017 р. Рецензент: д.т.н., доцент Казакова Н.Ф.