COMPUTATIONAL METHODS

УДК 004.056.55::519.6

ЕВГЕНИЙ МАКСИМЕНКО

СПОСОБ ЭФФЕКТИВНОГО ИСПОЛЬЗОВАНИЯ ПРИРАЩЕНИЙ ПРИ МНОГОКРАТНОМ ПРОРЕЖИВАНИИ ПРОБНЫХ ЗНАЧЕНИЙ ДЛЯ МЕТОДА ФАКТОРИЗАЦИИ ФЕРМА

Среди современных методов криптографической защиты информации наибольшее применение получили так называемые асимметричные алгоритмы, к числу которых относится алгоритм RSA (Rivest-Shamir-Adleman). Его криптографическая стойкость основана на трудности выполнения задачи факторизации многоразрядных чисел. В основе большинства методов факторизации лежит ряд фундаментальных соотношений классического алгоритма Ферма. Одним из направлений повышения его эффективности является модифицирование существующих или разработка новых алгоритмов выполнения алгебраических операций с большими числами. К числу таких можно отнести операцию модульного деления в процедурах предварительного просеивания пробных значений X. Предлагается модифицированный метод прореживания пробных значений в алгоритме факторизации Ферма, основным преимуществом которого является отказ от выполнения арифметически сложных операций модульного деления больших последовательностей и замена их на процедуру модульного деления малых чисел.

Ключевые слова: алгоритм RSA, факторизация, алгоритм Ферма, метод решета, прореживание пробных значений.

Постановка проблемы в общем виде. Среди разнообразия современных методов защиты информации алгоритм асимметричного шифрования RSA (Rivest-Shamir-Adleman) де-факто является стандартом для многих криптографических систем и приложений. Известно, что криптографическая стойкость данного алгоритма основана на трудности выполнения задачи факторизации многоразрядных чисел и не является эффективней задачи компрометации его программно-аппаратных реализаций [1]. На данный момент асимптотически самыми быстрыми методами факторизации многоразрядных чисел являются метод квадратичного решета и решета числового поля, построенные на фундаментальных соотношениях алгоритма Ферма и просеивания в факторных базах [2, 3, 4]. Исходя из сказанного можно утверждать, что усовершенствование существующих методов ускорения разложения чисел вида $N = p \cdot q$ представляется актуальной задачей.

Одним из направлений снижения вычислительной сложности метода Ферма является уменьшения количества операций извлечения квадратного корня за счет реализации процедуры просеивания значений X [5]. Суть метода заключается в следующем.

Пусть задано составное нечетное число $\mathrm{N} = p \cdot q$, которое следует разложить на множители, где p и q некоторые нечетные числа, не обязательно являющиеся простыми. Согласно исходному варианту метода Ферма для определения p и q решают уравнение

$$X^2 = N + Y^2, \tag{1}$$

где X и Y – целые положительные числа.

В уравнении (1) неизвестную X представим в виде

$$X = \left(\left\lfloor \sqrt{N} \right\rfloor + 1\right) + x = x_0 + x. \tag{2}$$

Тогда решение уравнения (1) получают перебором значений x = 0, 1, 2, …, до тех пор, пока остаток $X^2 - N$ не окажется полным квадратом целого числа, т.е.

$$Y^2 = X^2 - N, \tag{3}$$

где $N = X^2 - Y^2 = (X - Y)\cdot(X + Y) = p \cdot q$, а переменные X и Y определяются через p и q согласно соотношений

$$\begin{cases} X = (p + q)/2; \\ Y = (q - p)/2. \end{cases} \quad (4)$$

При этом нет необходимости проверять все варианты значений $X^2 - N$, а достаточно рассмотреть только те значения X, при которых разность $X^2 - N$ будет полным квадратом. Такой результат легко получить, если от равенства (3) перейти к равенству

$$Y^2 \bmod b = (X^2 - N) \bmod b, \quad (5)$$

что эквивалентно выполнению соотношения

$$(Y \bmod b)^2 \bmod b = ((X \bmod b)^2 \bmod b - N \bmod b) \bmod b. \quad (6)$$

Следует отметить, что если выполняется соотношение (3), то для произвольного b имеет место равенство (5), причем обратное неверно, т.е. из выполнения (5) не следует выполнение (3). Однако если не выполняется соотношение (5), то не будет выполняться и соотношение (3). Поэтому те X, при которых не выполняется (5), исключаются из рассмотрения.

Таким образом, при переходе от соотношения Ферма (1) к его аналогу (5) для остатков от деления X^2, Y^2 и N на основание модуля b возможно исключение из рассмотрения части значений $X^2 - N$, тем самым исключается необходимость выполнения достаточно трудоемкой операции извлечения квадратного корня для недопустимых значений X.

Идея использования при прореживании только тех X, для которых остаток от деления на некоторое основание модуля разности $X^2 - N$ также будет квадратичным остатком, впервые была предложена самим Пьером Ферма. Математик рассматривал величину $X^2 - N$ и, исходя из значений двух младших разрядов, делал вывод о том, является ли эта величина полным квадратом (последние 2 разряда полного квадрата должны быть 00, e1, e4, 25, o6 или e9, где e – четная, а o – нечетная цифры) [5]. Сравнение младших разрядов с возможными значениями есть не что иное, как рассмотрение остатков от деления числа по модулю, в случае П.Ферма – по модулю 100.

Данный подход к усовершенствованию метода факторизации чисел принято называть прореживанием возможных значений [5].

Прореживание возможных *X* в методе Ферма при одном основании модуля *b*. Назовем допустимыми те значения X по модулю некоторого основания b, при которых разность $(X^2 - N) \bmod b$ является квадратичным остатком по модулю b, и недопустимыми остальные. Исключение из дальнейшего анализа недопустимых пробных значений X будем называть их прореживанием.

Обозначим через $M(b)$ – множество квадратичных остатков по модулю b. Тогда выполнение условия (6) означает, что существует квадратичный остаток $w \in M(b)$, такой что

$$(w - N \bmod b) \bmod b \in M(b). \quad (7)$$

Следовательно, X допустимо, если для $(X \bmod b)^2 \bmod b = w$ выполняется условие (7).

Приведем пример использования такой процедуры прореживания.

Пример 1. Пусть N=383443. В качестве основания модуля будем использовать b=60.

1. Определение возможных квадратичных остатков по модулю b. Для случая b=60 квадратичные остатки приведены в табл.1.

Таблица 1 – Квадратичные остатки по модулю b=60

X mod b	0	1	**2**	3	4	5	6	7	**8**	9	10	11
X^2 mod b	**0**	**1**	**4**	**9**	**16**	**25**	**36**	**49**	4	**21**	**40**	1
X mod b	12	13	14	15	16	17	18	19	20	21	**22**	23
X^2 mod b	**24**	49	16	**45**	16	49	24	1	40	21	4	49
X mod b	24	25	26	27	**28**	29	30	31	**32**	33	34	35

Продолжение таблицы 1

$X^2 \bmod b$	36	25	16	9	4	1	0	1	4	9	16	25
$X \bmod b$	36	37	**38**	39	40	41	42	43	44	45	46	47
$X^2 \bmod b$	36	49	4	21	40	1	24	49	16	45	16	49
$X \bmod b$	48	49	50	51	**52**	53	54	55	56	57	**58**	59
$X^2 \bmod b$	24	1	40	21	4	49	36	25	16	9	4	1

Анализ представленных в таблице значений позволяет утверждать, что возможные квадратичные остатки по модулю b=60 могут принимать лишь следующие значения: 0, 1, 4, 9, 16, 21, 24, 25, 36, 40, 45, 49.

2. Определение квадратичных остатков по модулю 60, для которых выполняется соотношение (7).

Пусть, например, N=383443. Тогда $N \bmod b = 43$. Для всех вариантов квадратичных остатков определим разности $\left((X \bmod 60)^2 \bmod 60 - 43\right) \bmod 60$ и выясним, являются ли они квадратичными остатками по модулю b. Результаты вычислений приведены в табл. 2.

Таблица 2 – Результаты определения остатков $\left(X^2 \bmod b - 43\right) \bmod 60$ для всех вариантов квадратичных остатков по модулю b=60

$X^2 \bmod 60$	0	1	**4**	9	16		21	25	36	40	45	49
$\left(X^2 \bmod 60 - 43\right) \bmod 60$	17	18	**21**	26	33		38	42	53	57	2	6

Согласно данных табл. 2 единственным возможным квадратичным остатком, для которого выполняется соотношение (7), является $X^2 \bmod b = 4$.

3. Определение допустимых значений $X \bmod b$, для которых $X^2 \bmod b = 4$.

Согласно табл. 1, допустимыми значениями $X \bmod b$ для b=60 могут быть только значения 2, 8, 22, 28, 32, 38, 52 и 58. Для значений $X \bmod b = 0$, 1, 3, 4, 5, 6, 7, 9, 10, 11, 12 и т.д. разница $X^2 - N$ не может быть полным квадратом, а значит, их можно исключить из процедуры проверки.

4. Поиск неизвестных X и Y.

В общем виде допустимые значения X можно представить в виде

$$X_i = \left[x_0 / b\right] \cdot b + X_i \bmod b, \qquad (8)$$

где i=1, 2, 3, … n, а n – количество допустимых значений X. Поскольку все пробные значения X должны быть большими чем $\sqrt{N}$, то необходимо определять начальное допустимое значение X, которое при выполнении условия $X > \sqrt{N}$ для N=383443 будет равно 622.

а) определение начального значения $X_{нач}$ для реализации процедуры просеивания.

С учетом того, что согласно (2) $x_0 = \left[\sqrt{N}\right] + 1 = \left[\sqrt{2329}\right] + 1 = 620$, где 620 = 60·10+20, допустимыми могли бы быть значения X: $X_{нач}$=600+22=622>$\sqrt{N}$, X_1=600+28=628, X_2=600+32=632, X_3=600+38=638, X_4=600+52=652, X_5=600+58=658. Все дальнейшие допустимые значения X получаются из приведенных последовательным добавлением ”внешнего” шага приращения b=60 т.е. X_6=600+60+2=662, X_7=600+60+8=668, X_8=600+60+22=682 и далее 688, 692, 698, 712, 718, 722, ….

б) Проверка допустимых X на полный квадрат.

В табл. 3 приведены результаты проверок будет ли разница $X^2 - N$ полным квадратом для допустимых X.

Таблица 3 – Результаты проверок на полный квадрат разностей $X^2 - 383443$ для допустимых значений X.

X			622	628	632	638	652	658
$X^2 - 383443$			3441	10941	15981	23601	41661	49521

Продолжение таблицы 3

$\sqrt{X^2-383443}$			58,66	104,59	126,41	153,63	204,11	222,53
X	662	668	682	688	692	698	712	718
$X^2-383443$	54801	62781	81681	89901	95421	106761	123501	132081
$\sqrt{X^2-383443}$	234,09	250,56	285,80	299,83	308,90	322,12	351,43	363,43
X	722	728	742	748	752	758	772	778
$X^2-383443$	137841	146541	167121	176061	182061	191121	212541	221841
$\sqrt{X^2-383443}$	371,26	382,81	408,80	419,60	426,68	437,17	461,02	**471**

Таким образом, согласно табл. 3 полный квадрат разности получен для X=778. С учетом (3) определяем значения p и q:

$$p = 778 + 471 = 1249,$$
$$q = 778 - 471 = 307.$$
$$N = 1249 \cdot 307 = 383443.$$

Как видно из табл. 3 полный квадрат разности $X^2-383443$ получен для X =778 за 22 проверки разностей вместо 158 аналогичных проверок без использования предварительного прореживания.

Прореживание возможных *X* в методе Ферма при нескольких основаниях модуля *b*. Дальнейшее ускорение метода факторизации Ферма возможно путем использования процедуры многократного прореживания, когда оценка допустимости X проверяется не только для одного основания модуля, а для некоторого их числа. При таком подходе на каждом последующем этапе просеивания ”проверку” на принадлежность к числу возможных значений “проходят” только значения, просеянные на предыдущем – метод решета (алгоритм D согласно [5]).

Продемонстрируем эффект использования нескольких оснований модуля при решении уравнения (6) на следующем примере.

Пример 2. Пусть N=383443, b=60 – основное, а b_1=11 – дополнительное основание модуля.

а) Определение допустимых значений X для b_1=11.

Для дополнительного основания b_1=11 определим возможные квадратичные остатки.

Таблица 4 – Квадратичные остатки по модулю b_1=11

$X \bmod 11$	0	1	2	**3**	**4**	**5**	**6**	**7**	**8**	9	10
$X^2 \bmod 11$	**0**	**1**	**4**	**9**	**5**	**3**	3	5	9	4	1

Возможные квадратичные вычеты $(X^2 \bmod b_1 - N \bmod b_1) \bmod b_1$ представлены в табл. 5.

Таблица 5 – Результаты определения остатков $(X^2 \bmod 11 - 5) \bmod 11$ для всех вариантов квадратичных остатков по модулю b_1=11

$X^2 \bmod 11$	0	1	**3**	4	**5**	**9**
$(X^2 \bmod 11 - 5) \bmod 11$	6	7	**9**	10	**0**	**4**

С учетом того, что допустимыми квадратичными остатками, для которых выполняется соотношение (7), являются $X^2 \bmod 11 = 3$, $X^2 \bmod 11 = 5$ и $X^2 \bmod 11 = 9$ по табл. 4 определяем значения допустимых $X \bmod b$:

$$X \bmod b_1 = 3, 4, 5, 6, 7 \text{ и } 8.$$

б) Поиск неизвестных X и Y.

Результаты проверок на полный квадрат разностей $X^2 - 383443$ для допустимых значений X представлены в табл. 6. Воспользуемся результатами просеивания, полученными в предыдущем примере.

Таблица 6 – Результаты проверок на полный квадрат разностей $X^2 - 383443$ для допустимых значений X с учетом использования дополнительного основания модуля b_1=11.

X_i			622	628	632	638	652	658
$X_i \bmod 11$			6	1	5	0	3	9
$X_i \bmod 11 \in X \bmod b_1$? *			+	-	+	-	+	-
$\sqrt{X_i^2 - 383443}$			234,09		126,41		204,11	
X_i	662	668	682	688	692	698	712	718
$X_i \bmod 11$	2	8	0	6	10	5	8	3
$X_i \bmod 11 \in X \bmod b_1$? *	-	+	-	+	-	+	+	+
$\sqrt{X_i^2 - 383443}$		250,56		299,83		322,12	351,43	363,43
X_i	722	728	742	748	752	758	772	778
$X_i \bmod 11$	7	2	5	0	4	10	2	8
$X_i \bmod 11 \in X \bmod b_1$? *	+	-	+	-	+	-	-	+
$\sqrt{X_i^2 - 383443}$	371,26		408,80		426,68			**471**

Примечание. * (‘+’ – да, ‘-‘ – нет).

Как видно из табл. 6 полный квадрат разности $X^2 - 383443$ получен для X=778 за 12 проверок разностей вместо 22 аналогичных проверок при одном основании модуля т.е. при использовании дополнительного основания модуля приблизительно для половины значений допустимых X (46%) не выполнялась процедура вычисления квадратного корня.

Рассмотренный модулярный метод называется методом решета (сита), так как можно представить, что все целые числа проходят через решето, пропускающее только те значения, которые ”попадают” в диапазон допустимых значений *Xmodb*. Каждое сито в отдельности отсеивает примерно половину оставшихся значений. Когда же просеивание ведется при помощи попарно взаимно простых модулей, то на основании китайской теоремы об остатках каждое сито работает независимо от остальных. Поэтому, если выполнять просеивание относительно, скажем, 30 различных простых чисел, то для того, чтобы определить, будет ли величина $X^2 - N$ полным квадратом для Y^2, достаточно из каждых 2^{30} величин проверить только одну [5].

Однако следует отметить, что в случае реализации процедуры предварительного просеивания, позволяющей не выполнять проверочное извлечение корня для части возможных значений, на каждом этапе возникает необходимость осуществления модульного деления на определенное значение модуля. С учетом того, что в современной асимметричной криптографии в качестве ключа используются последовательности не менее 2^{2048} [6], это достаточно сложная процедура, требующая больших вычислительных и временных затрат.

Усовершенствованный метод прореживания возможных *X* в методе Ферма. В процессе работы с алгоритмом предварительного просеивания было замечено, что при проверке на принадлежность допустимым возможных значений X те же результаты можно получить если проверять не с сами значения X, а величину их приращений.

Суть предлагаемого метода просеивания заключается в том, что в отличие от классического деления проверочного значения X на некоторое основание модуля, реализуется модульное деление величины приращения существенно меньшего за само значение X, что исключает процедуру определения $Xmodb_i$ для больших чисел X.

Проиллюстрируем выигрыш от применения усовершенствованного метода прореживания на следующем примере.

Пример 3. Пусть N=383443, b=60 – основное, а b_1=11 – дополнительное основание модуля.

Согласно расчетов, полученных в примере 1 (п.3), $X_i \bmod 60 = 2, 8, 22, 28, 32, 38, 52$ и 58. Обозначим через $\Delta X_j = \left(X_{j+1} \bmod 60 - X_j \bmod 60\right) \bmod 60$. Получим следующие их значения:

ΔX_1=8-2=6;
ΔX_2=22-8=14;
ΔX_3=28-22=6;
ΔX_4=32-28=4;
ΔX_5=38-32=6;
ΔX_6=52-38=14;
ΔX_7=58-52=6;
ΔX_8=(60+2-58)=4.

Ранее было определено стартовое значение $X_{нач}$ = 622. Ему соответствует некоторое стартовое ΔX_j. Поскольку *622mod60* = 22, а приращение 22 использовано при вычитании в ΔX_3, то стартовое j равно 3.

Обозначим $\Delta\lambda_i$ – шаг приращений возможных X относительно начального значения $X_{нач}$=622. При $X=X_{нач}$ $\Delta\lambda_0$=0, при $X_1=X_{нач}+\Delta X_3$=628 и $\Delta\lambda_1=\Delta\lambda_0+\Delta X_3$=0+6=6, при $X_2=X_1+\Delta X_4$=628+4=632 и $\Delta\lambda_2=\Delta\lambda_1+\Delta X_4$=6+4=10, при $X_3=X_2+\Delta X_5$=632+6=638 и $\Delta\lambda_3=\Delta\lambda_2+$ $+\Delta X_5$=10+6=16, при $X_4=X_3+\Delta X_6$=638+14=652 и $\Delta\lambda_4=\Delta\lambda_3+\Delta X_6$=16+14=30, при $X_5=X_4+\Delta X_7$=652+6=658 и $\Delta\lambda_5=\Delta\lambda_4+\Delta X_7$=30+6=36, при $X_6=X_5+\Delta X_8$=658+4=662 и $\Delta\lambda_6=\Delta\lambda_5+$ $+\Delta X_8$=36+4=40, при $X_7=X_6+\Delta X_1$=662+6=668 и $\Delta\lambda_7=\Delta\lambda_6+\Delta X_1$=40+6=46, при $X_8=X_7+\Delta X_2$=668+14=682 и $\Delta\lambda_8=\Delta\lambda_7+\Delta X_2$=46+14=60= b, при $X_9=X_8+\Delta X_3$=682+6=688 и $\Delta\lambda_9=$ $\Delta\lambda_8+\Delta X_3$=60+6=66 и т.д.

В результате получили следующую последовательность $\Delta\lambda_i$= 6, 10, 16, 30, 36, 40, 46, 60, 66 …. Ее можно продолжать до получения решения уравнения (1), что реализовано в табл. 7.

Таблица 7 – Результаты проверок на полный квадрат разностей $X^2 - 383443$ для допустимых значений X с учетом использования дополнительного основания модуля b_1=11 при $X_{нач} \bmod 11 = 6$ усовершенствованным методом

X	622	628	632	638	652	658	662	668
$\Delta\lambda$	0	6	10	16	30	36	40	46
$6+\Delta\lambda$	6	12	16	22	36	42	46	52
$(6+\Delta\lambda) \bmod 11$	6	1	5	0	3	9	2	8
Допустимые Xmod11 *	+	-	+	-	+	-	-	+
$\sqrt{X^2-383443}$	234,09		126,41		204,11			250,56
X	682	688	692	698	712	718	722	728
$\Delta\lambda$	60	66	70	76	90	96	100	106
$6+\Delta\lambda$	66	72	76	82	96	102	106	112
$(6+\Delta\lambda) \bmod 11$	0	6	10	5	8	3	7	1
Допустимые Xmod11 *	-	+	-	+	+	+	+	-
$\sqrt{X^2-383443}$		299,83		322,12	351,43	363,43	371,26	
X	742	748	752	758	772	778		
$\Delta\lambda$	120	126	130	136	150	156		
$6+\Delta\lambda$	126	132	136	142	156	162		
$(6+\Delta\lambda) \bmod 11$	5	0	4	10	2	8		

Продолжение таблицы 7

Допустимые Xmod11 *	+	-	+	-	-	+		
$\sqrt{X^2-383443}$	408,80		426,68			**471**		

Примечание. * (‘+’ – да, ‘-‘ – нет).

Данные табл. 7 подтверждают, что при переходе к приращениям получаются те же результаты, что и в табл. 6. Но в случае больших чисел N не только X, но и $\Delta\lambda$ могут оказаться большими и будет намного сложнее определять остатки от деления на b_1 числа ($\Delta\lambda_i$+ $X_{нач}modb_1$), где $X_{нач}modb_1$ определено ранее и является относительно малым числом. В таком случае предлагается использовать приращения до некоторого числа $\Delta\lambda_{max}$, являющегося малым, например, меньшим за 2^{31} (предельное положительное при описаниях типа long) и кратным b. При $X = X_{нач}$ и каждый раз при достижении приращения $\Delta\lambda_{max}$ (т.е. для $X_{нач}+\Delta\lambda_{max}$, $X_{нач}+ 2\Delta\lambda_{max}$ и т.д.) будем обозначать X как $X_{фикс}$ и находить $X_{фикс}modb_i$. Для иллюстрации такого подхода принимаем $\Delta\lambda_{max}$=60 (число, кратное 60). Результаты вычислений представлены в табл. 8.

Таблица 8 – Результаты проверок на полный квадрат разностей $X^2-383443$ для допустимых значений X с учетом использования дополнительного основания модуля b_1=11 при ограничениях для $\Delta\lambda$.

X	622	628	632	638	652	658	662	668	682
$\Delta\lambda$	0	6	10	16	30	36	40	46	60
$\Delta\lambda$ =?= $\Delta\lambda_{max}$ *	-	-	-	-	-	-	-	-	+
$X_{фикс}$mod11+$\Delta\lambda$= 622mod11+$\Delta\lambda$= 6+$\Delta\lambda$	6	12	16	22	36	42	46	52	
$(6+\Delta\lambda)\bmod 11$	6	1	5	0	3	9	2	8	
Допустимые Xmod11 *	+	-	+	-	+	-	-	+	
$\sqrt{X^2-383443}$	234,1		126,4		204,1			250,6	
$\Delta\lambda = \Delta\lambda_{max}$, $X_{фикс} = X = 682$, $\Delta\lambda$=0									
X	682	688	692	698	712	718	722	728	742
$\Delta\lambda$	0	6	10	16	30	36	40	46	60
$\Delta\lambda$ =?= $\Delta\lambda_{max}$ *	-	-	-	-	-	-	-	-	+
$X_{фикс}$mod11+$\Delta\lambda$= 682mod11+$\Delta\lambda$= 0+$\Delta\lambda$	0	6	10	16	30	36	40	46	
$(0+\Delta\lambda)\bmod 11$	0	6	10	5	8	3	7	2	
Допустимые Xmod11 *	-	+	-	+	+	+	+	-	
$\sqrt{X^2-383443}$		299,8		322,1	351,4	363,4	371,3		
$\Delta\lambda = \Delta\lambda_{max}$, $X_{фикс} = X = 742$, $\Delta\lambda$=0									
X	742	748	752	758	772	778			
$\Delta\lambda$	0	6	10	16	30	36			
$\Delta\lambda$ =?= $\Delta\lambda_{max}$ *	-	-	-	-	-	-			
$X_{фикс}$mod11+$\Delta\lambda$= 742mod11+$\Delta\lambda$= 5+$\Delta\lambda$	5	11	15	21	35	41			
$(5+\Delta\lambda)\bmod 11$	5	0	4	10	2	8			
Допустимые Xmod11 *	+	-	+	-	-	+			
$\sqrt{X^2-383443}$	408,8		426,7			471			

Примечание. * (‘+’ – да, ‘-‘ – нет).

В последнем варианте использования приращений с ограничениями все операции по определению $Xmodb_i$ выполняются уже только для малых чисел вне зависимости от величины чисел N и X.

Вывод. Усовершенствованный метод прореживания пробных значений X позволяет отказаться от выполнения арифметически сложных операций модульного деления больших значений X на малое число, заменив их процедурой модульного деления малых чисел, что обеспечивает меньшую вычислительную сложность.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

[1] D. Brown, “Breaking RSA May Be As Difficult As Factoring”, *Journal of Cryptology*, vol. 29, iss. 1, pp. 220-241, January 2016. doi: 10.1007/s00145-014-9192-y.

[2] О.Н. Василенко. *Теоретико–числовые алгоритмы в криптографии*. Москва, Россия: МЦНМО, 2003.

[3] Ш.Т. Ишмухаметов. *Методы факторизации натуральных чисел.* Казань, Республика Татарстан: Казанский федеральный университет, 2011.

[4] А.В. Корнейко, и А.В. Жилин, “Анализ известных вычислительных методов факторизации многоразрядных чисел”, *Моделювання та інформаційні технології*, вип. 61, с. 3-13, 2011.

[5] Д. Кнут. *Искусство программирования. Том 2.* Москва, Россия: Мир, 1979.

[6] “RSA. Security Solutions to Address Cyber Threats”. [Online]. Available: https://www.rsa.com. Accessed on: Jan. 19, 2016.

Статья поступила в редакцию 23.02.2016.

REFERENCES

[1] D. Brown, “Breaking RSA May Be As Difficult As Factoring”, *Journal of Cryptology*, vol. 29, iss. 1, pp. 220-241, January 2016. doi: 10.1007/s00145-014-9192-y.

[2] O.N. Vasilenko. *Number-theoretic algorithms in cryptography*. Moskow, Russia: MTsNMO, 2003.

[3] Sh.T. Ishmukhametov. *Factoring methods of integers.* Kazan, Republic of Tatarstan: Kazan Federal University, 2011.

[4] A.V. Korneiko, and A.V. ZHilin, “Analysis of the known methods for computing the factorization of large numbers”, *Modelling Problems in Power Engineering*, iss. 61, pp. 3-13, 2011.

[5] D. Knut. *Art of Computer Programming. Vol. 2.* Москва, Moskow, Russia: Mir, 1979.

[6] “RSA. Security Solutions to Address Cyber Threats”. [Online]. Available: https://www.rsa.com. Accessed on: Jan. 19, 2016.

ЄВГЕН МАКСИМЕНКО

СПОСІБ ЕФЕКТИВНОГО ВИКОРИСТАННЯ ПРИРОСТУ ПРИ БАГАТОРАЗОВОМУ ПРОРІДЖУВАННЯ ПРОБНИХ ЗНАЧЕНЬ ДЛЯ МЕТОДУ ФАКТОРИЗАЦІЇ ФЕРМА

Серед сучасних методів криптографічного захисту інформації найбільше застосування отримали так звані асиметричні алгоритми, до числа яких належить алгоритм RSA (Rivest-Shamir-Adleman). Його криптографічна стійкість визначається складнощами виконання завдання факторизації багаторозрядних чисел. В основі більшості методів факторизації лежить ряд фундаментальних співвідношень класичного алгоритму Ферма. Одним з напрямків підвищення його ефективності є модифікування існуючих або розроблення нових алгоритмів

виконання алгебраїчних операцій з великими числами. До числа таких можна віднести операцію модульного ділення в процедурах попереднього проріджування пробних значень *X*. Пропонується модифікований метод проріджування пробних значень в алгоритмі факторизації Ферма, основною перевагою якого є відмова від виконання арифметично складних операцій модульного поділу великих послідовностей і заміна їх на процедуру модульного розподілу малих чисел.

Ключові слова: алгоритм RSA, факторизація, алгоритм Ферма, метод решета, проріджування пробних значень.

YEVHEN MAKSYMENKO

THE WAY OF EFFECTIVE USE OF INCREMENTAL WITH MULTIPLE THINNING OF TEST VALUES FOR FERMAT'S FACTORING METHOD

Among the modern methods of cryptographic information protection asymmetric algorithms is most widely used. A special place among them is occupied by RSA (Rivest-Shamir-Adleman) encryption algorithm, which recommended the use a number of international standards and recommendations. RSA cryptographic resistance is based on the difficulty of the task execution of multi-digit numbers factorization and is not an effective problem of compromising its software and hardware implementations. Currently the “fastest” ways of decomposition the big numbers into factors are methods of the general number field sieve (GNFS), the quadratic sieve (QS) algorithm and the elliptic curve factorization method (ECM). It is known that the basis of these methods are based on a number of fundamental relations of Fermat’s classical algorithm, proceeding from which it can be argued that the improvement of Fermat’s method can have an impact on reducing the computational complexity of modern factorization methods listed above. One of the ways to increase the efficiency of the improved Fermat's factoring method is a modification of existing or developing new algorithms of execution the algebraic operations with large numbers. Among these can be the operation of the modular division in procedures for advance sieving of test values *X*. A modified method of thinning test values in Fermat’s factoring algorithm is proposed, the main advantage of which is the refusal to perform complex arithmetic operations of modular division of large sequences and replacing them with the procedure of the modular division of small numbers.

Keywords: RSA algorithm, factorization, Fermat's algorithm, the sieve method, thinning of test values.

Евгений Васильевич Максименко, заместитель заведующего кафедрой кибербезопасности и применения автоматизированых информационных систем и технологий, Государственное учреждение “Институт специальной связи и защиты информации Национального технического университета Украины ”Киевский политехнический институт”, Киев, Украина.

E-mail: iszzi@i.ua.

Євген Васильович Максименко, заступник завідувача кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Державний заклад ”Інститут спеціального зв’язку та захисту інформації Національного технічного університету України ”Київський політехнічний інститут”, Київ, Україна.

Yevhen Maksymenko, deputy head of academic department cybersecurity and application of information systems and technologies, State institution “Institute of special communications and information protection National technical university of Ukraine “Kyiv polytechnic institute”, Kyiv, Ukraine.