УДК 621.391(075.8)

Трещев Иван Андреевич
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Заведующий кафедрой «Информационная безопасность автоматизированных систем»
Кандидат технических наук
E-Mail: kalkt@yandex.ru

Воробьев Антон Александрович
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Аспирант
E-Mail: zeromem@mail.ru

Худякова Валентина Игоревна
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Студент 3-го курса обучения
E-Mail: valya_787@mail.ru

Об оценке количества малых дешифрующих экспонент криптосистемы RSA, подверженных атаке Винера

Аннотация. В данной работе рассмотрен криптографический алгоритм RSA в разрезе угроз реализаций атак Винера непрерывными дробями. Произведен вывод точной оценки количества шифрующих экспонент, подверженных атаке Винера для заданного $N = pq$, для чего доказана лемма о количестве взаимно-простых с z чисел в отрезке $[1;n]$ при $n < z$, а также рассчитана вероятность выбора подобной слабой экспоненты. Показана возможность введения криптосистемы RSA двумя равносильными способами, и даны рекомендации по реализации с учетом указанной ранее атаки.

Ключевые слова: экспонента; RSA; атака Винера.

Криптографический алгоритм RSA, названный в честь авторов Ривеста, Шамира и Эдлемана, является первым криптографическим алгоритмом с открытым ключом, который достойно выдержал испытание временем. Он основывается на удивительно простой теоретико–числовой идее, – легко перемножить два больших простых числа, но крайне сложно разложить на множители их произведение[1].

Введем криптосистему RSA[2]. Пусть p,q – два различных больших случайно выбранных простых числа. Обозначим

$$N = pq \text{ и } \varphi(N) = (p-1)(q-1),$$

где $\varphi(N)$ – функция Эйлера. Кроме того, выберем шифрующую экспоненту E, удовлетворяющую условию

$$НОД(E, \varphi(N)) = 1.$$

Дешифрующую экспоненту d находят расширенным алгоритмом Евклида[3] по паре значений $[E, \varphi(N)]$. Найденная экспонента удовлетворяет условию

$$Ed = 1 (\mathrm{mod}\, \varphi(N)) \text{ - (1)}$$

Тогда для открытого текста m и его закрытого текста C верны следующие соотношения:

$$C = m^E (\mathrm{mod}\, N),$$
$$m = C^d (\mathrm{mod}\, N).$$

Но, исходя из условия (1) имеем:

$$d = E^{-1} \mathrm{mod}(\phi(N)),$$

$$\forall k \in Z \Rightarrow E \cdot \left| d = E^{-1} + k\phi(N) \right. \Rightarrow$$

$$Ed = 1 + Ek\phi(N) \left| \cdot d^{-1} \right. \Rightarrow$$

$$E = d^{-1} + Ed^{-1}k\phi(N) \Rightarrow$$

$$E = d^{-1} \mathrm{mod}(\phi(N)).$$

Исходя из малой теоремы Ферма[4] имеем, что дешифрующая экспонента d должна удовлетворять условию

$$НОД(d, \varphi(N)) = 1.$$

Таким образом, второй способ определения криптосистемы RSA можно ввести в следующем виде.

Пусть p,q – два различных больших случайно выбранных простых числа. Обозначим

$$N = pq \text{ и } \varphi(N) = (p-1)(q-1),$$

где $\varphi(N)$ – функция Эйлера. Кроме того, выберем дешифрующую экспоненту d, удовлетворяющую условию

$$НОД(d, \varphi(N)) = 1.$$

Шифрующую экспоненту E находят расширенным алгоритмом Евклида[3] по паре значений $[d, \varphi(N)]$.

Криптографический алгоритм RSA достойно выдержал испытание временем, но при реализации криптосистемы на основе криптоалгоритма RSA имеется ряд исключительных ситуаций[2,4,5,6], подвергающих криптосистему различного рода атакам. Одной из таких атак, является атака Винера, основанная на непрерывных дробях[2].

Одним из важнейших результатов в теории непрерывных дробей является то, что $\forall a \in R$, если $\frac{p}{q}$ – несократимая дробь и удовлетворяет неравенству

$$\left| a - \frac{p}{q} \right| \le \frac{1}{2q^2},$$

то $\frac{p}{q}$ – одна из подходящих дробей[7] в разложении a в непрерывную дробь.

Исходя из (1), существует такое целое k, что

$$Ed - k\varphi = 1.$$

Атака Винера непрерывными дробями для криптографического алгоритма RSA[2] заключается в том, что если дешифрующая экспонента $d < \sqrt[4]{\frac{N}{3}}$, то

$$\left| \frac{E}{N} - \frac{k}{d} \right| < \frac{1}{2d^2}.$$

Так как $НОД(k,d) = 1$, то $\frac{k}{d}$ – подходящая дробь при разложении дроби $\frac{E}{N}$ в непрерывную. Следовательно, раскладывая вещественное значение $\frac{E}{N}$ в непрерывную дробь, дешифрующая экспонента подвергается компрометации при последовательной подстановке знаменателей подходящих дробей в выражение

$$\left(M^E\right)^d = M \left(\mathrm{mod}\, N\right),$$

где M – некоторое натуральное случайное число. Общее число проверяемых подходящих дробей оценивается как $O(\ln N)$.

Вычислим количество шифрующих экспонент, подверженных атаки Винера. Для этого рассмотрим множество

$$d = \left[2; \left\lfloor \frac{\sqrt[4]{N}}{3} \right\rfloor \right] \subset N.$$

Так как $(Z/nZ)*$ размерностью

$$\varphi(N) = (p-1)(q-1)$$

является мультипликативной группой[8], то исходя из свойства единственности обратного элемента имеем, что количество шифрующих экспонент E, подверженных атаки Винера на основе непрерывных дробей определяется мощностью множества $\#H(N)$, где

$$H(N) = \{ d_i \mid НОД(d_i, \varphi(N)) = 1, d_i \in d \}.$$

Таким образом, задачу вычисления количества шифрующих экспонент, подверженных атаки Винера можно сформулировать следующим образом: вычислите количеству взаимно–простых чисел в отрезке $X:[2;b]$ с наперед заданным q, при условии, что $b < q$, где

$$b = \left\lfloor \frac{\sqrt[4]{N}}{3} \right\rfloor, q = \varphi(N)$$

Для решения задачи докажем лемму.

Лемма 1. Для заданных $q \in N, n \in N, q > n$ количество взаимно–простых чисел $\varphi^*(q,n)$ из отрезка $[1;n]$ и q выражается соотношением

$$\varphi^*(q,n) = \sum_{d|q} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor,$$

где $\mu(d)$ – функция Мёбиуса.

Доказательство. Для $\forall d \,|\, q$ рассмотрим $\left\lfloor \frac{n}{d} \right\rfloor$, где d является простым делителем q. Очевидно, что данная дробь выражает количество элементов отрезка $[1;n]$, делящихся на d. Используя основную теорему арифметики, произведем разложение q в виде

$$q = p_1^{k_1} p_2^{k_2} \dots p_i^{k_i} \dots p_m^{k_m},$$

где p_i – простые числа, k_i – некоторые натуральные числа.

Далее, рассмотрим для $\forall d \,|\, q$, рассмотрим произведения $\mu(d) \left\lfloor \frac{n}{d} \right\rfloor$. Заметим, что $\mu(d) \neq 0$ тогда и только тогда, когда делитель d может быть представлен в виде $d = \prod_{r_i \in 2^{[1;m]}} p_{r_i}$,

$$i \in [1;2^m], \text{ т.е.}$$

$$\forall d \,|\, q, d = \prod_{r_i \in 2^{[1;m]}} p_{r_i}^{k_w}, w \in [1;\#r_i]$$

выполнимо

$$\mu(d) \left\lfloor \frac{n}{d} \right\rfloor \neq 0 | k_w \in [0;1],$$

где

$$\mu(d) = \begin{cases} 1, & \text{если } \#r_i \pmod 2 = 0, \\ -1, & \text{если } \#r_i \pmod 2 \neq 0. \end{cases}$$

Просуммируем полученный ряд. Имеем:

$$\varphi^*(q,n) = n - \sum_{d \in \{p_i\}} \left\lfloor \frac{n}{d} \right\rfloor + \sum_{d \in \{p_i p_j\}, i > j} \left\lfloor \frac{n}{d} \right\rfloor +$$

$$+ \dots + (-1)^m \left\lfloor \frac{n}{\prod_i p_i} \right\rfloor$$

по теореме о включениях–исключениях, ч.т.д.

Сформулируем следствие леммы 1.

Следствие. Для заданных $q \in N, n \in N, m \in N$, $q > n > m$ количество взаимно–простых чисел $\xi(q,n,m)$ из отрезка $[m;n]$ и q выражается соотношением

$$\xi(q,n,m) = \varphi^*(q,n) - \varphi^*(q,m).$$

Данное следствие является очевидным и не требует доказательства.

Отсюда количество шифрующих экспонент, подверженных атаки Винера может быть найдено как

$$\#H(N) = \xi\left(\varphi(N), \left\lfloor \frac{\sqrt[4]{N}}{3} \right\rfloor, 2\right).$$

Аналогично, для проблемы атак на криптографическую систему RSA в случае $d < N^{0.292}$ [5], оценка количества шифрующих экспонент вычисляется как

$$\#H(N) = \xi\left(\varphi(N), N^{0.292}, 2\right).$$

Таким образом, можно сделать следующие выводы:

1. Криптографическую систему RSA возможно вводить двумя способами, – относительно первоначального выбора шифрующей экспоненты E , так и относительно первоначального выбора дешифрующей экспоненты d .

2. При заданном $N = pq$, количество шифрующих экспонент, подверженных атаке Винера непрерывными дробями, и при значениях $d < N^{0.292}$ выражается значением функции $\#H(N)$, а вероятность выбора подобной шифрующей экспоненты равна

$$\frac{\#H(N)}{N}.$$

3. При реализации криптосистемы RSA, удобнее в использовании второй способ определения, так как позволяет заведомо выбрать значение d так, чтобы противостоять атакам с малой дешифрующей экспонентой.

ЛИТЕРАТУРА

1. Салома, А. Криптография с открытым ключом / А. Салома: Пер. с англ. – М. : Мир, 1995. – 318 с., ил.
2. Смарт, Н. Криптография / Н. Смарт. – М. : Техносфера, 2005. – 528 с.
3. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – 6–е изд., испр. – М. : Государственное издательство технико–теоретической литературы, 1952. – 180 с.
4. Воронков, Б.Н. Элементы теории чисел и криптозащита: Учебное пособие / Б.Н. Воронков, А.С. Щеголеватых. – Воронеж: ГОУВПО «ВГУ», 2008. – 88 с.
5. Boneh, D. Cryptanalysis of RSA with private key d less than $N^{0.292}$ / D. Boneh, G. Durfee // EUROCRYPT 1999. Heidelberg: Springer. – 1999. – LNCS Vol. 1592. – P. 1 – 11.
6. Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities: Revised version of two articles from EUROCRYPT 1996 / D. Coppersmith // Journal of Cryptology. Heidelberg: Springer. – 1997. – Vol. 10(4). – P. 233 – 260.
7. Джоунс, У. Непрерывные дроби. Аналитическая теория и приложения. Пер. с англ. / У. Джоунс, В. Трон – М. : Мир, 1985. – 414 с., ил.
8. Курош, А.Г. Лекции по общей алгебре / А.Г. Курош. – М. : Наука, 1973. – 399 с.

Ivan Treschev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

Anton Vorobyev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: zeromem@mail.ru

Valentine Khudyakov
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: valya_787@mail.ru

On an estimate of the number of small ADK exponential cryptosystem RSA, subject to Wieners attack

Abstract. In this paper we consider the RSA cryptographic algorithm implementations in the context of threats of attacks Wiener continued fractions. Output produced accurate estimates of the number of ciphering exponential prone to attack Wiener given, which prove a lemma about the number of mutually prime to the numbers in the interval when, and calculated the probability of choosing such a weak exponent. The possibility of the introduction of RSA cryptosystem two equipotent methods, and recommendations for implementation, taking into account the previously mentioned attacks.

Keywords: exhibitor; RSA; Wiener attack.

REFERENCES

1. Saloma, A. Kriptografija s otkrytym kljuchom / A. Saloma: Per. s angl. – M. : Mir, 1995. – 318 s., il.
2. Smart, N. Kriptografija / N. Smart. – M. : Tehnosfera, 2005. – 528 s.
3. Vinogradov, I.M. Osnovy teorii chisel / I.M. Vinogradov. – 6–e izd., ispr. – M. : Gosudarstvennoe izdatel'stvo tehniko–teoreticheskoj literatury, 1952. – 180 s.
4. Voronkov, B.N. Jelementy teorii chisel i kriptozashhita: Uchebnoe posobie / B.N. Voronkov, A.S. Shhegolevatyh. – Voronezh: GOUVPO «VGU», 2008. – 88 s.
5. Boneh, D. Cryptanalysis of RSA with private key d less than / D. Boneh, G. Durfee // EUROCRYPT 1999. Heidelberg: Springer. – 1999. – LNCS Vol. 1592. – P. 1 – 11.
6. Coppersmith, D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities: Revised version of two articles from EUROCRYPT 1996 / D. Coppersmith // Journal of Cryptology. Heidelberg: Springer. – 1997. – Vol. 10(4). – P. 233 – 260.
7. Dzhouns, U. Nepreryvnye drobi. Analiticheskaja teorija i prilozhenija. Per. s angl. / U. Dzhouns, V. Tron – M. : Mir, 1985. – 414 s., il.
8. Kurosh, A.G. Lekcii po obshhej algebre / A.G. Kurosh. – M. : Nauka, 1973. – 399 s.