Дальневосточный математический журнал. 2018. Т. 18. № 2. С. 189–194

УДК 519.719.2
MSC2010 94A60

© А. А. Илларионов[1,2], С. А. Чепурко[2]

Об атаке Винера на шифр RSA

Предлагается элементарная модификация атаки Винера на шифр RSA. Алгоритм использует только аппарат непрерывных дробей. Его сложность равна $O(d^2 m^{-1/2} \ln m)$ (при условии $m^{1/4} \ll d \ll m^{1/2}$, $e \leqslant m$), где m, d и e — модуль, секретная и открытая экспоненты криптосистемы RSA. Требуемое количество памяти — $O(\ln m)$.

Ключевые слова: *RSA, атака Винера, криптоанализ RSA.*

1. Введение

Наиболее распространенной на сегодняшний день криптосистемой с открытым ключом является шифр RSA [1]. Напомним определения. Модуль m шифра RSA есть произведение $m = pq$ двух (больших) простых чисел p и q. Секретная экспонента d и открытая экспонента e — это натуральные числа, связанные сравнением

$$ed \equiv 1 \pmod{\varphi}, \tag{1}$$

где $\varphi = \varphi(m) = (p-1)(q-1)$ (функция Эйлера). Пара (e,m) является открытым ключом, а натуральное d — секретным. Шифрование открытого текста $x \in \mathbb{Z}_m = \{0, \ldots, m-1\}$ и расшифрование шифртекста $y \in \mathbb{Z}_m$ производится по формулам

$$y = x^e \pmod{m}, \quad x = y^d \pmod{m}.$$

Далее всюду считаем, что

$$q < p < 2q. \tag{2}$$

Эти ограничения естественны с точки зрения криптостойкости шифра.

В общем случае криптостойкость шифра RSA определяется сложностью решения задачи факторизации. Отметим, что для взлома шифра достаточно найти хотя бы один из четырех секретных параметров p, q, φ, d.

[1] Хабаровское отделение Института прикладной математики ДВО РАН, 680000, г. Хабаровск, ул. Дзержинского, 54.
[2] Тихоокеанский государственный университет, 680035, г. Хабаровск, ул. Тихоокеанская, 136.
Электронная почта: illar_a@list.ru (А. А. Илларионов), chepurkojm@gmail.com (С. А. Чепурко).

Для увеличения скорости расшифрования можно использовать небольшую секретную экспоненту d. Такой выбор оправдан, если есть большая разница в мощности коммутирующих устройств. Например, в случае использования цифровой подписи RSA при взаимодействии «большой компьютер — смарт-карта». Однако в 1990 г. Винер [2] описал полиномиальный алгоритм взлома шифра RSA, работающий, если $d = O(m^{1/4})$. Атака Винера основана на теории непрерывных дробей.

Любое рациональное α единственным образом раскладывается в конечную непрерывную (цепную) дробь:

$$\alpha = [q_0; q_1, q_2, \ldots, q_s] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_s}}},$$

где $q_0 = [\alpha]$ (целая часть) и $q_j = q_j(\alpha) \in \mathbb{N}$ (неполные частные), причем $q_s \geqslant 2$. Несократимая дробь $P_n/Q_n = [q_0; q_1, \ldots, q_n]$ называется n-й подходящей для α.

Согласно (1) существует такое натуральное k, что

$$ed = 1 + k\varphi. \tag{3}$$

Теорема (см. [2]). *Пусть $e \leqslant m$ и $d < m^{1/4}/3$. Тогда k/d — подходящая дробь для e/m.*

Таким образом, если $d < m^{1/4}/3$, то для взлома шифра RSA достаточно разложить e/m в непрерывную дробь, найти все подходящие дроби и проверить их «на роль» k/d. Количество подходящих дробей для e/m не превосходит $O(\ln m)$. Количество элементарных арифметических операций, требуемых для нахождения всех подходящих дробей, также есть величина $O(\ln m)$. Поэтому алгоритм является полиномиальным.

В [3–5] были предложены модификации алгоритма Винера, которые являются полиномиальными при условии, что $d = O(m^{1/4} \ln^t m)$, $t \in (0, +\infty)$. Они основаны на рассмотрении диофантовых приближений к дроби e/m. Бонех и Дерфи [6], а также Бломер и Мэй [7] предложили атаки на шифр RSA в случае, когда $d = O(m^{0{,}292})$. Алгоритмы из [6, 7] используют методы геометрии чисел, LLL-алгоритм и метод Копперсмита нахождения небольших целочисленных корней многочленов с целочисленными коэффициентами. Они являются полиномиальными при условии, что справедлив двумерный аналог теоремы Копперсмита. В настоящей заметке предлагается еще одна модификация атаки Винера, использующая только непрерывные дроби. Она более простая для реализации и, возможно, более эффективная, чем алгоритмы из [3–5].

2. Модификация атаки Винера

Определим

$$\alpha = m - \frac{3}{\sqrt{2}}\sqrt{m} + 1, \quad \beta = m - 2\sqrt{m} + 1.$$

Из (2) вытекает, что

$$\alpha \leqslant \varphi \leqslant \beta.$$

Лемма. *Пусть* $Q \in \mathbb{Z} \cap [\alpha, \beta]$, *причем*

$$|\varphi - Q| < \frac{\alpha^2}{e}\left(\frac{1}{2d^2} - \frac{1}{d\alpha}\right).$$

Тогда k/d *— подходящая дробь для* e/Q.

Доказательство. Сразу отметим, что НОД $(k, d) = 1$. Так как

$$\left|\frac{k}{d} - \frac{e}{Q}\right| = \left|\frac{k}{d} - \frac{e}{\varphi} + \frac{e}{\varphi} + \frac{e}{Q}\right| = \left|\frac{1}{d\varphi} + \frac{e(Q-\varphi)}{\varphi Q}\right| \leqslant \frac{1}{d\alpha} + e\frac{|Q-\varphi|}{\alpha^2} < \frac{1}{2d^2},$$

то требуемое утверждение вытекает из свойств подходящих дробей. □

Возьмем любое натуральное N и определим

$$h = \frac{\beta - \alpha}{N}, \quad b_j = \left[\alpha + \frac{h}{2} + jh + \frac{1}{2}\right], \quad j = \overline{0, N-1}.$$

Теорема 1. *Пусть* $\theta = \sqrt{1 + e^{-1}} - e^{-1/2}$, *причем*

$$ed^2 < \theta\alpha^2. \tag{4}$$

Если

$$N \geqslant \frac{m^{1/2}ed^2}{c\alpha^2} \cdot \frac{1}{\theta - ed^2\alpha^{-2}}, \qquad c = 3\sqrt{2} + 4, \tag{5}$$

то найдется такой номер $j \in \{0, \ldots, N-1\}$, *что* k/d *— подходящая дробь для* e/b_j.

Доказательство. Пусть b_j — ближайшее к φ число из $\{b_0, \ldots, b_{N-1}\}$. Так как $\alpha \leqslant \varphi \leqslant \beta$, то, используя (5), находим

$$|b_j - \varphi| \leqslant \frac{h}{2} + \frac{1}{2} = \frac{\beta - \alpha}{2N} + \frac{1}{2} = \frac{m^{1/2}}{2cN} + \frac{1}{2} \leqslant \frac{\alpha^2\theta - ed^2}{2ed^2} + \frac{1}{2} = \frac{\alpha^2\theta}{2ed^2}. \tag{6}$$

Согласно выбору θ

$$e^{1/2}\theta + 2\theta^{1/2} - e^{1/2} = 0 \quad \Longrightarrow \quad \sqrt{\frac{e}{\theta}} = \frac{2}{1-\theta}.$$

Поэтому, используя условие (4), получаем

$$\frac{1}{\alpha} < \frac{1}{d}\sqrt{\frac{\theta}{e}} = \frac{1-\theta}{2d}.$$

Поэтому

$$\frac{\alpha^2}{e}\left(\frac{1}{2d^2} - \frac{1}{d\alpha}\right) > \frac{\alpha^2\theta}{2ed^2}.$$

Используя (6), заключаем

$$|b_j - \varphi| < \frac{\alpha^2}{e}\left(\frac{1}{2d^2} - \frac{1}{d\alpha}\right).$$

Значит, k/d — подходящая дробь для e/b_j согласно лемме. □

Замечание 1. Пусть $e < m$ и $d = O(m^{1/2})$. Тогда $e \gg m^{1/2}$ согласно соотношению (3). Поэтому $\theta = 1 + O(m^{-1/4})$. Кроме того, $\alpha = m + O(m^{1/2})$. В современных приложениях модуль шифра RSA является очень большим числом ($m \gtrsim 2^{2048}$). В этом случае условия (4), (5) выполняются при

$$d < (1 - \varepsilon_1)\, m^{1/2}, \qquad N \geqslant \frac{1}{c(1-\varepsilon_2)} \cdot \frac{d^2}{m^{1/2}} \cdot \frac{e}{m},$$

где $\varepsilon_1, \varepsilon_2$ — некоторые малые числа. Поэтому алгоритм нахождения секретного ключа d, вытекающий из теоремы, является полиномиальным, если

$$d = O(e^{-1/2} m^{3/4} \ln^t m) = O(m^{1/4} \ln^t m), \qquad t \in (0, +\infty).$$

Замечание 2. Можно предложить два способа проверки равенства $P/Q = k/d$.
1-й способ. Если $P/Q = k/d$, то согласно (3) p, q можно найти из соотношений

$$eQ = 1 + P(p-1)(q-1), \quad m = pq.$$

2-й способ. Выбираем натуральное $\mathrm{g} \geqslant 2$, например, $\mathrm{g} = 2$. Если $Q = d$, то

$$\mathrm{g}^{eQ} \equiv \mathrm{g} \pmod{m}. \tag{7}$$

Второй способ эффективнее с точки зрения быстродействия. Пусть P_i/Q_i, $i = \overline{0,s}$ — подходящие дроби для $e/b_j = [q_0; q_1, \ldots, q_s]$. Для вычисления чисел $y_i = \mathrm{g}^{eQ_i} \pmod{m}$ удобно применить рекуррентные соотношения

$$Q_{i+1} = q_{i+1} Q_i + Q_{i-1} \quad \Longrightarrow \quad y_{i+1} = y^{q_{i+1}} y_{i-1}.$$

Используя алгоритм быстрого возведения вычетов в степень, получаем, что количество умножений в кольце вычетов $\mathbb{Z}_m$, требуемых для нахождения всех $y_i = \mathrm{g}^{eQ_i} \pmod{m}$, не больше, чем

$$O\left(\ln m + \sum_{i=1}^{s} (\ln q_i + 1)\right) = O(\ln m).$$

Отметим, что выполнение условия (7) не гарантирует равенства $Q = d$. Для дробей, удовлетворяющих (7), следует проверить выполнение равенства (7) с другим g. Если результат положительный, то окончательная проверка может быть проведена, например, с помощью 1-го способа. Конец замечания.

Алгоритмы из [3–5] требуют знания величины R, ограничивающей сверху число $d^2 m^{-1/2}$, причем их сложность зависит от R (а не от $d^2 m^{-1/2}$). Можно предложить следующую модификацию атаки Винера, не требующую предварительной оценки значения $d^2 m^{-1/2}$.

Схема алгоритма.

1. Полагаем $h = \beta - \alpha$.
2. Полагаем $b = [\alpha + h/2 + 1/2]$.

2.1. Ищем k/d среди подходящих дробей для e/b. Если таковое обнаружено, то конец алгоритма.

2.2. Если $[b+h+1/2] < \beta$, то заменяем b на $[b+h+1/2]$ и переходим к шагу 2.1.

3. Заменяем h на $h/2$ и переходим к шагу 2.

Пусть $e \leqslant m$, $d \leqslant (1-\varepsilon_1)m^{1/2}$ и m — большое. Согласно теореме 1 и замечаниям 1, 2 сложность (количество элементарных арифметических операций) предложенного алгоритма равна

$$O\left(\frac{d^2}{m^{1/2}} \cdot \frac{e}{m} \ln m\right) = O(d^2 m^{-1/2} \ln m),$$

Она (асимптотически при $m \to +\infty$) меньше, чем сложность алгоритма из [3], примерно равна сложности алгоритма из [4] и больше, чем сложность алгоритма из [5]. Сложность последнего равна $O(dm^{-1/4}\ln m)$. Отметим, что алгоритм из [5] использует вариант атаки «встреча посередине» и требует порядка $O(dm^{-1/4}\ln m)$ битов памяти. Предложенный в настоящей работе алгоритм требует порядка $O(\ln m)$ битов памяти.

Список литературы

[1] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, **21**, (1978), 120–126.

[2] M.,J. Wiener, "Cryptanalysis of short RSA secret exponents", *IEEE Trans. Inform. Theory*, **36**, (1990), 553–558.

[3] E. R. Verheul, H. C. A. van Tilborg, "Cryptanalysis of "less short" RSA secret exponents", *Appl. Algebra Engrg. Comm. Computing*, **8**, (1997), 425–435.

[4] A. Dujella, "Continued fractions and RSA with small secret exponent", *Tatra Mt. Math. Publ.*, **29**, (2004), 101–112.

[5] A. Dujella, "A variant of Wiener's attack on RSA", *Computing*, **85**, (2009), 77–83.

[6] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than 0.292", *in Advances in Cryptology-EUROCRYPT '99*, Lecture Notes in Computer Science, v. 1592, Springer, Berlin, Germany, 1999, 1–11.

[7] J. Blomer, A. May, "Low secret exponent RSA revisited", *Cryptography and Lattice - Proceedings of CaLC 2001*, Lecture Notes in Comput. Sci., v. 2146, 2001, 4–19.

Работа первого автора выполнена при финансовой поддержке гранта Министерства образования и науки Хабаровского края (договор 129/2018Д от 06.08.2018).

Illarionov A. A., Chepurko S. A. On Wiener's attack on RSA cryptosystem. *Far Eastern Mathematical Journal.* 2018. V. 18. No 2. P. 189–194.

ABSTRACT

We propose a modification of Wiener's attack on the RSA cryptosystem. The algorithm uses only continuous fractions. It's complexity is not greater than $O(d^2 m^{-1/2} \ln m)$, where m is the modulus, d is the secret exponent of RSA.

Key words: *RSA, Wiener's attack, cryptanalysis of RSA.*