УДК 004.056.55

Ю. Ф. Болтнев, М. В. Алешникова, Е. В. Козьминых

ИССЛЕДОВАНИЕ УСЛОВИЙ ПРИМЕНИМОСТИ АТАКИ ВИНЕРА НА КРИПТОСИСТЕМУ RSA

Рассматривается атака Винера на малый секретный ключ в криптосистеме RSA. Представлена новая граница на секретный ключ, выведенная при более общих предположениях. Показано, что новая граница точнее границы Винера при выполнении классических условий. Получены условия применимости атаки Винера при превышении границы на секретный ключ. Даны рекомендации по выбору параметров разработчику криптосистемы.

The paper considers the Wiener's attack for a small secret key in the RSA cryptosystem. Presented a new bound on the secret key, derived under more general assumptions. It is shown that the obtained bound is more accurate than the Wiener's bound under the classical conditions. The conditions of applicability of Wiener's attack when the bound on the secret key is exceeded. Recommendations on the choice of parameters for the cryptosystem developer are given.

Ключевые слова: криптосистема RSA, атака Винера, граница Винера, цепная дробь, подходящие дроби.

Keywords: RSA cryptosystem, Wiener's attack, Wiener's bound, continued fraction, convergents.

Введение

Для криптосистемы RSA с открытым ключом (e, N) и секретным ключом (d, p, q) хорошо известна атака на малый секретный ключ d, носящая название атаки Винера [1; 3; 4]. Эта атака основана на следующей теореме [4].

Теорема 1 (Винер). *Пусть задана криптосистема RSA с параметрами* $N = pq$, $ed \equiv 1 (mod \phi(N))$, $q<p<2q$, $d < \frac{1}{3} N^{\frac{1}{4}}$. *Тогда ключ d эффективно вычислим.*

Поскольку $ed \equiv 1 \left(mod\ \varphi(N)\right)$, то существует некоторое целое число k, такое, что выполняется равенство

$$ed - 1 = k\varphi(N), \tag{1}$$

где k — некоторый коэффициент кратности.

Утверждение теоремы означает, что при $d < \frac{1}{3} N^{\frac{1}{4}}$ выполняется неравенство

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}, \tag{2}$$

из которого следует, что дробь $\frac{k}{d}$ является одной из подходящих дробей для числа $\frac{e}{N}$, количество которых не превышает $2\log_2 N$.

© Болтнев Ю. Ф., Алешникова М. В., Козьминых Е. В., 2019
Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2019. № 1. С. 42 – 48.

Последний факт опирается на следующую теорему из теории цепных дробей [1; 2].

Теорема 2 (достаточный признак подходящей дроби). *Если* α *– некоторое действительное число, причем* $\frac{a}{b}$ *– несократимая рациональная дробь, такая, что* $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$, *то* $\frac{a}{b}$ *– одна из подходящих дробей к числу* α.

Поскольку количество подходящих дробей не более $2\log_2 N$, то можно последовательным их перебором найти искомый секретный ключ. В этом случае атака производится по известному [1; 3] алгоритму.

Алгоритм атаки Винера

ВВОД: $N, e, M, C = M^e \pmod N$
ВЫВОД: $d : ed \equiv 1 \pmod{(\varphi(N))}$

1. Положить $\alpha = \frac{E}{N}$.
2. Разложить α в цепную дробь: $\alpha = [q_0, q_1, \ldots, q_i, \ldots, q_s]$, $s < 2\log_2 N$.
3. *Для* $i = 1, 2, \ldots$ вычислить:

   3.1. P_i, Q_i: $\delta_i = \frac{P_i}{Q_i}$ – i-я подходящая дробь к α.

   3.2. Если $C^{Q_i} \equiv M \pmod N$, то вернуть $d = Q_i$.

Уточнение границы Винера

В условиях теоремы Винера должно выполняться неравенство $q < p < 2q$. В следующей теореме мы получим границу на секретный ключ d при более общих условиях. В предыдущих обозначениях докажем следующую теорему.

Теорема 3. *Секретный ключ* d *в криптосистеме RSA является эффективно вычислимым, то есть величина* $\frac{k}{d}$ *является подходящей дробью для дроби* $\frac{e}{N}$, *если* $d < \frac{1}{\sqrt{2\alpha}} N^{\frac{1}{4}}$, *где* $\alpha = \frac{h+1}{\sqrt{h}}, p = hq$.

Доказательство. Нашей целью является получение границы на секретный ключ d, из которой будет следовать неравенство (2).

Для функции Эйлера имеем

$$\varphi(N) = (p-1)(q-1) = pq - p - q + 1 = N - p - q + 1.$$

Отсюда $N - \varphi(N) = p + q - 1$. Оценим разность $N - \varphi(N)$.

Введем обозначение $h = \frac{p}{q}$. Тогда $p = hq$ и для величины $N = pq$ можно записать $N = q^2 h$. Выразим отсюда переменную q:

$$q = \sqrt{\frac{N}{h}}.$$

Тогда

$$p + q = hq + q = (h + 1)q = \frac{h+1}{\sqrt{h}}\sqrt{N}.$$

Обозначим $\alpha = \frac{h+1}{\sqrt{h}}$, получим соотношение

$$N - \varphi(N) = p + q - 1 = \alpha\sqrt{N} - 1. \quad (3)$$

Учитывая (3), имеем следующую оценку:

$$\Delta = \left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed - Nk}{Nd}\right| = \left|\frac{1 + k\varphi(N) - Nk}{Nd}\right| = \left|\frac{k\big(N - \varphi(N)\big) - 1}{Nd}\right| <$$

$$< \frac{k|N-\varphi(N)|}{Nd} = \frac{k(p+q-1)}{Nd} < \frac{k(p+q)}{Nd} = \frac{k\alpha\sqrt{N}}{Nd} = \frac{k\alpha}{d\sqrt{N}}.$$

Таким образом, получили оценку

$$\Delta = \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{k\alpha}{d\sqrt{N}}. \quad (4)$$

Из равенства (1) следует, что $ed > k\varphi(N)$. Поскольку обычно полагают, что $e < \varphi(N)$, то получим неравенство $\frac{k}{d} < 1$.

Из него и неравенства (4) следует, что

$$\Delta < \frac{\alpha}{\sqrt{N}}.$$

Выясним, при каких условиях имеет место равносильное (2) неравенство

$$\frac{\alpha}{\sqrt{N}} < \frac{1}{2d^2}. \quad (5)$$

Неравенство (5) равносильно неравенствам

$$d^2 < \frac{\sqrt{N}}{2\alpha} \text{ и } d < \frac{N^{\frac{1}{4}}}{\sqrt{2\alpha}}.$$

Последнее неравенство и выражает искомую новую границу Винера.

Таким образом, нами было произведено обобщение теоремы Винера при более общих условиях и получена новая граница для секретного ключа.

Заметим, что полученная граница лучше классической границы Винера. Так, при $h \approx 2$, $\alpha = \frac{h+1}{\sqrt{h}} = \frac{3}{\sqrt{2}}$. В этом случае получим границу $d < \frac{N^{\frac{1}{4}}}{\sqrt{2\alpha}} = 0{,}4855N^{\frac{1}{4}}$, что лучше границы $d < \frac{1}{3}N^{\frac{1}{4}}$, предложенной в теореме Винера, примерно на 46 %.

Также при росте h увеличивается α, а коэффициент $c = \frac{1}{\sqrt{2\alpha}}$ понижается. При большом h он станет меньше $\frac{1}{3}$ и классической границей Винера пользоваться будет нельзя. Разрешая относительно h уравнение $\frac{1}{\sqrt{2\alpha}} = \frac{1}{3}$, получим $h \approx 18{,}2$. То есть пока выполняется соотношение $\frac{p}{q} < 18{,}2$, можно пользоваться прежней, классической границей Винера (несколько заниженной). В ином случае следует использовать нашу границу.

Условия применимости атаки Винера

Введем обозначение $d_{\text{кр}} = \frac{1}{\sqrt{2\alpha}} N^{\frac{1}{4}}$. Тогда новая граница Винера принимает вид

$$d < d_{\text{кр}}. \tag{6}$$

Проведенные нами численные эксперименты показали, что атака Винера зачастую приводит к успеху, если даже секретный ключ превышает границу Винера (6). Причины этого явления раскрываются в следующей теореме.

Теорема 4. *Пусть $r = \frac{d}{d_{\text{кр}}}$ – коэффициент кратности превышения границы Винера (6). Тогда атака гарантированно приведет к успеху, если выполнится условие $k < \frac{1}{r} d_{\text{кр}}$. Если же случайно выполнится условие $\frac{d_{\text{кр}}}{r} \le k < \frac{2d_{\text{кр}}}{r}$, то атака может привести к успеху с некоторой вероятностью.*

Доказательство.

1. Ранее уже отмечалось, что неравенство (2)

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

является достаточным условием того, что $\frac{k}{d}$ – подходящая дробь для дроби $\frac{e}{N}$. При доказательстве теоремы 3 была получена оценка (4):

$$\Delta = \left| \frac{e}{N} - \frac{k}{d} \right| < \frac{k\alpha}{d\sqrt{N}}.$$

Отсюда получим, что достаточное условие для подходящей дроби будет выполнено, если выполняется условие $k < \frac{\sqrt{N}}{2\alpha d} = \frac{d_{\text{кр}}^2}{d}$, которое проще переписать в виде $k < \frac{d_{\text{кр}}}{r}$.

2. Известно [2], что необходимым условием того чтобы $\frac{k}{d}$ была подходящей дробью для дроби $\frac{e}{N}$, является выполнение неравенства

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{1}{d^2}. \tag{7}$$

Рассуждая аналогично пункту 1, получим, что неравенство (7) будет выполнено, если случайно выполнится условие $k < \frac{2d_{\text{кр}}}{r}$.

Оценим вероятность выполнения неравенств в условиях теоремы 4. Выше уже отмечалось, что параметр k принимает свои значения в интервале $0 < k < d$. На основании численных экспериментов можно предположить, что значения величины $\frac{k}{d}$ распределены равномерно на интервале [0, 1]. Данная нулевая гипотеза была проверена по статистическому критерию согласия Пирсона на выборке объема 10^6 при числе степеней свободы $r = 9$ и уровне значимости $\alpha = 0{,}05$. По результатам теста можно считать эту нулевую гипотезу не противоречащей опытным данным.

Тогда для вероятности выполнения неравенства $1 \le k < \frac{d_{кр}}{r}$ имеем

$$P\left(1 \le k < \frac{d_{кр}}{r}\right) = \frac{\frac{d_{кр}}{r}}{d} = \frac{1}{r^2}.$$

Аналогично и для вероятности выполнения неравенства $\frac{d_{кр}}{r} < k < \frac{2d_{кр}}{r}$ имеем

$$P\left(\frac{d_{кр}}{r} \le k < \frac{2d_{кр}}{r}\right) = \frac{1}{r^2}.$$

Рекомендации разработчику

Для того чтобы убедиться в безопасности выбранных параметров криптосистемы RSA, разработчику необходимо провести вычисления и проверки согласно следующему алгоритму.

Алгоритм проверки параметров RSA

1. Вычислить $\varphi(N) = (p-1)(q-1)$.
2. Вычислить $k = \frac{ed-1}{\varphi(N)}$.
3. Вычислить $h = \frac{p}{q}, \alpha = \frac{h+1}{\sqrt{h}}$.
4. Вычислить $d_{кр} = \frac{N^{\frac{1}{4}}}{\sqrt{2\alpha}},\ r = \frac{d}{d_{кр}}$.
5. В том случае, если d не превышает границу Винера, ($d < d_{кр}$), то криптосистема будет легко взломана описанным методом.
6. Если ключ оказался в промежутке $d_{кр} < d < {d_{кр}}^2$ и случайно (с вероятностью $\frac{1}{r^2}$) выполняется условие $1 \le k < \frac{d_{кр}}{r}$, то атака гарантированно будет успешной.
7. Если случайно (с вероятностью $\frac{1}{r^2}$) выполняется двойное неравенство $\frac{d_{кр}}{r} \le k < \frac{2d_{кр}}{r}$, то вероятность взлома по статистике составляет до 50 %.

Пример 1. Исходные данные:

N = 303098468963 = 778579 · 389297; e = 2421079; d = 125191.

Обозначим $k_{кр} = \frac{d_{кр}}{r}$.

Согласно алгоритму, имеем

$$d_{кр} = 360{,}22;\ r = 347{,}53;\ k_{кр} \approx 1{,}037;\ \ k = 1.$$

Видим, что выполнено условие $k < k_{кр}$.

Последовательность подходящих дробей к $\frac{e}{N}$: $\left[0, \frac{1}{125191}, \frac{2}{250383} \ldots\right]$.

Атака будет успешна, поскольку $\frac{k}{d} = \frac{1}{125191}$ — подходящая дробь для дроби $\frac{e}{N}$.

Этот пример демонстрирует успешность атаки даже при превышении границы Винера почти в 350 раз.

Пример 2. Исходные данные:

$$N = 200250077 = 10007 \cdot 20011;\ e = 65492543;\ d = 107.$$

Имеем

$$d_{\text{кр}} = 57{,}75;\ r = 1{,}85;\ k_{\text{кр}} \approx 31{,}17;\ k = 35.$$

Видим, что выполнено условие $k_{\text{кр}} < k < 2k_{\text{кр}}$.

Последовательность подходящих дробей к $\frac{e}{N}$: $\left[0, \frac{1}{3}, \frac{17}{52}, \frac{35}{107} \ldots\right]$.

Атака будет успешна, поскольку $\frac{k}{d} = \frac{35}{107}$ — подходящая дробь для дроби $\frac{e}{N}$.

Пример 3. Исходные данные:

$$N = 200250077 = 10007 \cdot 20011;\ e = 65618339;\ d = 119.$$

Имеем

$$d_{\text{кр}} = 57{,}75;\ r = 2{,}06;\ k_{\text{кр}} \approx 28{,}03,\ k = 39.$$

Видим, что выполнено условие $k_{\text{кр}} < k < 2k_{\text{кр}}$.

Последовательность подходящих дробей к $\frac{e}{N}$: $\left[0, \frac{1}{3}, \frac{19}{58}, \frac{58}{177}, \frac{1121}{3421} \ldots\right]$.

Атака не будет иметь успеха, поскольку $\frac{k}{d} = \frac{39}{119}$ не является подходящей дробью для дроби $\frac{e}{N}$.

Список литературы

1. *Глухов М.М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В.* Введение в теоретико-числовые методы криптографии : учеб. пособие. СПб. ; М., 2011.

2. *Нестеренко Ю.В.* Теория чисел. М., 2008.

3. *Смарт Н.* Криптография. М., 2005.

4. *Wiener M.* Cryptanalysis of Short RSA Secret Exponents // IEEE Trans. Inform. Theory. 1990. Vol. 36, iss. 3. P. 553—558.

Об авторах

Юрий Федорович Болтнев — доц., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: IBoltnev@kantiana.ru

Марина Валерьевна Алешникова — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: aleshnikova_m_v@mail.ru

Елена Викторовна Козьминых — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: lena_kozm@mail.ru

The authors

Yury F. Boltnev, Associate Professor, I. Kant Baltic Federal University, Russia.
E-mail: IBoltnev@kantiana.ru

Marina V. Aleshnikova, Assistant Professor, I. Kant Baltic Federal University, Russia.
E-mail: aleshnikova_m_v@mail.ru

Elena V. Kozminykh, Assistant Professor, I. Kant Baltic Federal University, Russia.
E-mail: lena_kozm@mail.ru