

Исследование условий применимости атаки Винера на криптосистему RSA

Болтнев Ю.ф.
БФУ им.И.Канта
Калининград

Калининград, 2019

Описание криптосистемы RSA

p, q – простые

$N = pq$ – модуль RSA

e – шифрующая экспонента

d – расшифровывающая экспонента

$ed \equiv 1 \bmod \varphi(N)$, где $\varphi(N) = (p - 1)(q - 1)$

(N, e) – открытый ключ

(N, d) – секретный ключ

Алгоритм RSA

$m: 0 \leq m < N$ – очередной блок

Боб

есть открытый ключ Алисы

Алиса

владеет своим закрытым ключом



Теорема Винера

Если $q < p < 2q$ и $d < \frac{1}{3} N^{\frac{1}{4}}$

то d – эффективно вычислима

Идея:

$$\Delta = \left| \frac{e}{N} - \frac{k}{d} \right| < \frac{1}{2d^2} \Rightarrow \frac{k}{d} - \text{подходящая дробь для } \frac{e}{N}$$

$$k : ed = 1 + k\varphi(N)$$

Алгоритм атаки Винера

Ввод: N, e, t, c

Вывод: d

1. $\alpha = \frac{e}{N}$

2. $\alpha \rightarrow [q_0, q_1, \dots, q_i, \dots, q_s], s < 2 \log_2 N$

3. Для $i = 1, 2, \dots$ вычислить:

3.1 $\delta_i = \frac{P_i}{Q_i}$ – подходящая дробь к α

3.2 . Если $c^{Q_i} = t$, то вернуть $d = Q_i$

Сложность: $O(\log_2 N)$

Пример атаки

Ввод: $N = 200250077$, $e = 83963251$,

$m = 8624851$, $c = 67153474$

Вывод: $d = 31$

$$1. \alpha = \frac{e}{N} = \frac{83963251}{200250077}$$

$$2. \alpha \rightarrow \left[0, \frac{1}{2}, \frac{2}{5}, \frac{3}{7}, \frac{5}{12}, \frac{13}{31}, \dots, \frac{83963251}{200250077} \right]$$

$$3.1 \delta_6 = \frac{13}{31} - \text{подходящая дробь к } \alpha$$

$$3.2. 67153474^{31} = 8624851 \bmod 200250077$$

Теорема Винера

Если $q < p < 2q$ и $d < \frac{1}{3} N^{\frac{1}{4}}$

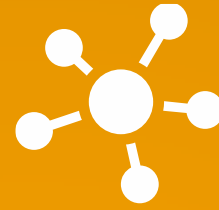
то d – эффективно вычислима



d – эффективно вычислима
то есть величина $\frac{k}{d}$ является подходящей
дробью для несекретной дроби $\frac{e}{N}$

если $d < \frac{N^{\frac{1}{4}}}{\sqrt{2\alpha}}$, где $\alpha = \frac{h+1}{\sqrt{h}}$; $p = hq$.

Пример



$$d < \frac{1}{3} N^{\frac{1}{4}};$$

$$h = 2; \alpha = \frac{3}{\sqrt{2}}. \quad d < \frac{N^{\frac{1}{4}}}{\sqrt{2\alpha}} = 0.4855 N^{\frac{1}{4}}.$$

Следствие

$$\Delta = \left| \frac{e}{N} - \frac{k}{d} \right| < \frac{k\alpha}{d\sqrt{N}} \quad (1)$$

$$k < \frac{d_{\text{кр}}}{r}, \text{ где } r = \frac{d}{d_{\text{кр}}} \quad (2)$$

$$\Delta < \frac{1}{2d^2} \quad (3)$$

$$d_{\text{кр}} = \frac{N^{\frac{1}{4}}}{\sqrt{2\alpha}}$$

Обзор результатов

$d < d_{\text{кр}}$	$d_{\text{кр}} < d < d_{\text{кр}}^2$	
Успех с вероятностью 100%	$1 \leq k < \frac{d_{\text{кр}}}{r}$	$\frac{d_{\text{кр}}}{r} \leq k < \frac{2d_{\text{кр}}}{r}$
	Успех с вероятностью 100%	Успех с вероятностью 20–30%.

Пример

$N = 200250077; d_{кр} = 57$

$d < d_{кр}$	$d_{кр} < d < d_{кр}^2$	
$d = 49; k = 46$ $\frac{d_{кр}}{r} \approx 66.3; r = 0.85$ $[0, 1, \frac{15}{16}, \frac{46}{49},$ $\frac{107}{114}, \frac{153}{163}, \dots]$	$1 \leq k < \frac{d_{кр}}{r}$	$\frac{d_{кр}}{r} \leq k < \frac{2d_{кр}}{r}$
	$d = 97; k = 3$ $\frac{d_{кр}}{r} \approx 33.5; r = 1.71$ $[0, \frac{1}{32}, \frac{2}{65}, \frac{3}{97},$ $\frac{68}{2199}, \frac{153}{163}, \dots]$	$d = 79; k = 43$ $\frac{d_{кр}}{r} \approx 41.1; r = 1.4$ $[0, 1, \frac{1}{2}, \frac{6}{11},$ $\frac{37}{38}, \frac{43}{79}, \frac{80}{147}, \dots]$

Пример

$N = 64634012142622 \dots$ (617 знаков, 1024 бита)

$e = 63219248034527 \dots$ (611 знаков)

$d = 77410015190 \dots$ (157 знаков)

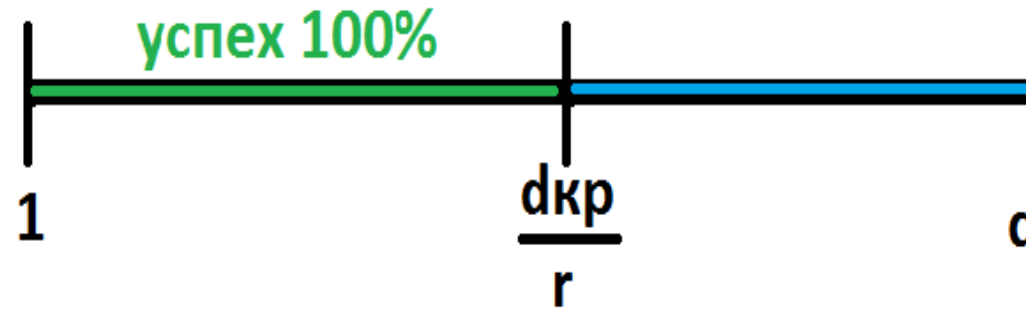
d – знаменатель 279 подходящей дроби

$$r = \frac{d}{d_{\text{кр}}} = 1000$$

Проблема: какова вероятность успешности атаки?

$d < d_{\text{кр}}$	$d_{\text{кр}} < d < d_{\text{кр}}^2$	
Успех с вероятностью 100%	$1 \leq k < \frac{d_{\text{кр}}}{r}$	$\frac{d_{\text{кр}}}{r} \leq k < \frac{2d_{\text{кр}}}{r}$
	Успех с вероятностью 100%	Успех с вероятностью 20–30%.

Вероятность успешной атаки



$$d = r d_{кр}$$

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

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

Рекомендации разработчику

$$1 < d < d_{\text{кр}} - 100\%$$

$$d_{\text{кр}} < d < d_{\text{кр}}^2 \text{ и } 1 \leq k < \frac{d_{\text{кр}}}{r} - 100\%$$

$$d_{\text{кр}} < d < d_{\text{кр}}^2 \text{ и } \frac{d_{\text{кр}}}{r} \leq k < \frac{2d_{\text{кр}}}{r} - 20-30\%$$

Единая редакция
НАУЧНЫХ ЖУРНАЛОВ
БФУ им. И. Канта

[Вход](#) | [Регистрация](#)

Наука одна: двух наук нет, как нет двух вселенных...
Александр Герцен

[поиск](#) >>>[DOI-генератор](#) [Поиск по DOI на Crossref.org](#)[Главная](#)[Журналы](#)[Выпуски](#)[Политика журнала](#)[Реквизиты](#)[Редакционная коллегия](#)[Редакционная этика](#)[Контакты Редакции](#)[Правила оформления и
предоставления статей](#)[Подать статью online](#)

Главная | Вестник Балтийского федерального университета им. И. Канта. Серия: ФИЗИКО-МАТЕМАТИЧЕСКИЕ И ТЕХНИЧЕСКИЕ НАУКИ
№1 | Математика и информатика

ИССЛЕДОВАНИЕ УСЛОВИЙ ПРИМЕНИМОСТИ АТАКИ ВИНЕРА КРИПТОСИСТЕМУ RSA

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

Страницы 42-48

Статья [Загрузить](#)

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

Ключевые слова (англ.) RSA cryptosystem, Wiener's attack, Wiener's bound, continued fraction, convergents

Аннотация Рассматривается атака Винера на малый секретный ключ в криптосистеме RSA. Показано, что граница Винера при выполнении классических условий. Получены условия применимости при превышении границы на секретный ключ. Даны рекомендации по выбору параметров криптосистемы.

Аннотация The paper considers the Wiener's attack for a small secret key in the RSA cryptosystem

Вестник БФУ им И.Канта

[https://journals.kantiana.ru/vestnik/
4225/12566/](https://journals.kantiana.ru/vestnik/4225/12566/)