Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

# Взлом системы RSA

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 421 Группы

направления 02.03.01 математика и компьютерные науки

механико-математический факультет

Ретюнской Анастасии Владимировны

Научный руководитель
доцент, к.ф-м.н., доцент Е. В. Сецинская

Зав. кафедрой
зав.каф., к.ф-м.н. А. М. Водолазов

Саратов 2017

**Введение.** Информация — это одна из самых ценных вещей в современной жизни. На протяжении всей своей истории человек испытывал потребность в шифровке той или иной информации. Неудивительно, что из этой потребности выросла целая наука — криптография. Криптография — это наука об обеспечении безопасности данных. Она занимается поисками решений четырех важных проблем безопасности: конфиденциальности, аутентификации, целостности и контроля участников взаимодействия. Эффективными системами криптографической защиты являются криптосистемы с открытым ключом, называемые также асимметричными криптосистемами. В таких системах для зашифрования данных используется один ключ, а для расшифрования — другой.

В настоящее время наиболее развитым методом криптографической защиты информации с известным ключом является RSA. Данный алгоритм был предложен одним из первых в конце 70-х годов XX века. Его название составлено из первых букв фамилий авторов: Р. Райвеста (R. Rivest), А. Шамира (A. Shamir) и Л. Адлемана (L. Adleman). Алгоритм RSA является, наверно, наиболее популярным и широко применяемым асимметричным алгоритмом в криптографических системах. Его криптостойкость основывается на сложности разложения на множители больших чисел, а именно — на исключительной трудности задачи определить секретный ключ на основании открытого, так как для этого потребуется решить задачу о существовании делителей целого числа.

Данная работа содержит три раздела. В первом разделе приведены основные сведения из теории чисел. Во втором разделе рассматриваются различные методы разложения целых чисел на множители, а именно: метод пробных делений, метод Ферма, (P-1)-метод Полларда, а также метод Шермана-Лемана и алгоритм Ленстры. В третьем разделе подробно разбирается алгоритм RSA и его уязвимость.

Вопрос стойкости алгоритма RSA является актуальным, так как с раз-

витием телекоммуникационных технологий возникла потребность в быстром и безопасном обмене данными. В настоящее время данный алгоритм применяется практически во всех программных продуктах, использующих передачу данных по незащищенным каналам связи. RSA является стандартом, принятым практически во всем мире.

**Основное содержание работы.**

**Определение 1.5.** *Функция Эйлера $\varphi(n)$ — это мультипликативная арифметическая функция, равная количеству натуральных чисел, меньших $n$ и взаимно простых с ним.*

**Свойства функции Эйлера**

1. $\varphi(mn) = \varphi(m)\varphi(n)$ — мультипликативность;
2. $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \dfrac{d}{\varphi(d)}$ — обобщенная мультипликативность;
3. $\varphi(p) = p - 1$ — функция Эйлера от простого числа;
4. $\varphi(p^n) = p^n - p^{n-1}$ — функция Эйлера от степени простого числа;
5. $\varphi(n) = n\prod\limits_{p|n}\left(1 - \dfrac{1}{p}\right),\ n > 1$ — функция Эйлера от натурального числа.

**Теорема 1.2** (Малая теорема Ферма)**.** *Если $p$ — простое число, $a$ — целое число, не делящееся на $p$, то $a^{p-1} - 1$ делится на $p$.*

Данная теорема стала одной из главных теорем для исследований не только в теории целых чисел, но и в более широких областях.

Рассмотрим различные методы разложения целых чисел на множители.

С помощью метода пробных делений число $n$ проверяется на простоту. Если $n$ — составное, то $n = ab$, где $1 < a \leqslant b$, причем $a \leqslant \sqrt{n}$. Поэтому для $d = 2, 3, \ldots, [\sqrt{n}]$ мы проверяем, делится ли $n$ на $d$? Если делитель числа $n$ не будет найден, то $n$ — простое. В противном случае будет найден минимальный простой делитель числа $n$, т.е. мы разложим $n$ на два множителя [1, 9].

Алгоритм Ферма, рассматривая различные случаи, ищет представление $n$ в виде $n = u^2 - v^2$, откуда получается разложение $n = (u - v)(u + v) = ab$. Работаем с величинами

$$r_k = x_k^2 - y_k^2 - n, \quad k = 0, 1, 2, \ldots$$

Начальное значение $(x_0, y_0) = ([\sqrt{n}], 0)$. Увеличение номера $k$ происходит по следующим правилам. Если $r_k = 0$, то цель достигнута,

$$n = x_k^2 - y_k^2 \ = (x_k - y_k)(x_k + y_k),$$

и алгоритм останавливается. Если $r_k > 0$, то

$$(x_{k+1}, y_{k+1}) := (x_k, y_k + 1),$$

если же $r_k < 0$, то

$$(x_{k+1}, y_{k+1}) := (x_k + 1, y_k);$$

затем

$$r_{k+1} := x_{k+1}^2 - y_{k+1}^2 - n.$$

(P-1)-метод Полларда основан на следующей идее. Предположим, что у числа $n$, которое мы хотим разложить на множители, есть простой делитель $p$, такой что число $p - 1$ является $B$-степенно-гладким для некоторой границы гладкости $B > 0$. Значит, для любого простого числа $q, q \mid p - 1$, выполнено неравенство

$$q^{\nu_q(p-1)} \leqslant B.$$

Следовательно, $p - 1 \mid \text{НОК}(1, 2, \ldots, B)$. Если мы выберем $a \in N$ такое, что $(a, n) = 1$, то по малой теореме Ферма

$$a^{\text{НОК}(1,2,\ldots,B)} \equiv 1 \pmod{n}.$$

Отсюда следует, что НОД$(a^{\text{НОК}(1,2,\ldots,B)}-1,n)$ делится на $p$ и поэтому содержит нетривиальный делитель $n$ (НОД может быть и равен $n$).

Алгоритм Шермана-Лемана детерминированно раскладывает $n$ на множители за $O(n^{1/3})$ арифметических операций.

**Алгоритм.**

Пусть $n$ нечетно, $n>8$.

**1 шаг.** Для $a=2,3,\ldots,[n^{1/3}]$ проверить условие $a|n$. Если на этом шаге мы не разложили $n$ на множители, то переходим к шагу 2.

**2 шаг.** Если на 1 шаге делитель не найден и $n$ — составное, то $n=pq$, где $p,q$ — простые числа, и

$$n^{1/3}<p\leqslant q<n^{2/3}.$$

Тогда для всех $k=1,2,\ldots,[n^{1/3}]$ и всех $d=0,1,\ldots,[n^{1/6}/(4\sqrt{k})]+1$ проверить, является ли число

$$([\sqrt{4kn}]+d)^2-4kn$$

квадратом натурального числа. Если является, то для

$$A=[\sqrt{4kn}]+d \text{ и } B=\sqrt{A^2-4kn}$$

выполнено сравнение

$$A^2\equiv B^2 \pmod{n}.$$

В этом случае проверить условие

$$A<(A\pm B,n)<n.$$

Если это условие выполнено, то мы разложили $n$ на два множителя и алгоритм останавливается.

Если алгоритм не нашел разложение $n$ на два множителя, то $n$ — простое число.

Алгоритм Ленстры основывается на следующей теореме.

**Теорема 2.1.** *Пусть $r, s, n$ — натуральные числа, удовлетворяющие условиям*

$$1 \leqslant r < s < n, \quad n^{1/3} < s, \quad (r, s) = 1.$$

*Тогда существует не более 11 делителей $r_i$, числа $n$ таких, что*

$$r_i \equiv r \pmod{s}.$$

*Имеется алгоритм, который находит все эти $r_i$ за $O(\log n)$ арифметических операций.*

**Алгоритм.**

На входе заданы числа $r, s, n \in \mathbb{N}$, удовлетворяющие условиям теоремы.

**1 шаг.** С помощью обобщенного алгоритма Евклида найти

$$r^* \in \mathbb{N}, \ r^* r \equiv 1 \pmod{s}.$$

Найти $r'$ такое, что $r' \equiv r^* n \pmod{s}$, $0 \leqslant r' < s$.

**2 шаг.** Для очередного значения $= 0, 1, 2, \ldots$ найти числа $a_i, b_i, c_i$ по следующим правилам:

$$a_0 = s, \quad b_0 = 0, \quad c_0 = 0,$$

$$a_1 \equiv r' r^* \pmod{s}, \quad 0 < a_1 \leqslant s, \quad b_1 = 1, \quad c_1 \equiv \frac{n - rr'}{s} \cdot r^* \pmod{s},$$

и при $i \geqslant 2$

$$a_i = a_{i-2} - q_i a_{i-1}, \quad b_i = b_{i-2} - q_i b_{i-1}, \quad c_i = c_{i-2} - q_i c_{i-1} \pmod{s}.$$

Здесь целые числа $q_i$ однозначно определяются условиями

$$0 \leqslant a_i < a_{i-1} \ \text{ при } i \text{ четном},$$

$$0 < a_i \leqslant a_{i-1} \ \text{ при } i \text{ нечетном}.$$

Фактически, $q_i$ — частное от деления $a_{i-2}$ на $a_{i-1}$ за исключением случая, когда $i$ нечетно и остаток от деления равен нулю. Отметим, что $a_i$ монотонно не возрастают и на четных номерах — убывают.

**3 шаг.** Для очередного набора $a_i, b_i, c_i$ найти все целые числа $c$, удовлетворяющие условиям

$$\begin{aligned} & c = c_i \pmod{s} \\ & |c| < s, && \text{если } i \text{ четное} \\ & 2a_ib_i \leqslant c \leqslant \frac{n}{s^2} + a_ib_i, && \text{если } i \text{ нечетное} \end{aligned}$$

Таких $c$ будет не более двух; для четного $i$ это очевидно, а для нечетных $i$ докажем это ниже.

**4 шаг.** Для каждого $c$ из шага 3 решить в целых числах систему уравнений

$$\begin{cases} xa_i + yb_i = c, \\ (xs + r)(ys + r') = n. \end{cases}$$

Если $x$ и $y$ окажутся неотрицательными целыми числами, то добавить $xs + r$ к списку искомых делителей.

**5 шаг.** Если $a_i = 0$, то алгоритм заканчивает работу. Иначе возвращаемся на шаг 2 к следующему значению $i$.

Далее приводится алгоритм RSA и рассматривается его уязвимость.

Алгоритм RSA использует тот факт, что пока не существует достаточно быстрых алгоритмов разложения целых чисел на множители. Процедура построения абонентом секретного и открытого ключей состоит в следующем. Абонент выбирает два простых числа $a, b$ и вычисляет их произведение $n = ab$. Далее абонент случайным образом выбирает два натуральных числа $e, d$, меньших $\varphi(n) = (a-1)(b-1)$, удовлетворяющих сравнению

$$ed \equiv 1 \pmod{\varphi(n)}$$

Открытым ключом данного абонента будет пара $(n, e)$. Секретным ключом —

число $d$. Числа $a$ и $b$ также должны держать в секрете, но рассматривать тройку $(a, b, d)$ в качестве секретного ключа необязательно, т.к. числа $a, b$ используются только на стадии генерации чисел $n, e, d$. Поэтому числа $a, b$ можно уничтожить.

**Описание алгоритма**

*Данные: Открытый ключ* $(n, e)$ *и секретный ключ* $d$ *абонента* $A$.

*Требуется: Передать абоненту* $A$ *сообщение* $x \in \mathbb{Z}/n\mathbb{Z}$ *абонента* $B$.

*1. Абоненту* $B$ *вычислить* $y = x^e$ *и передать результат абоненту* $A$.

*2. Абоненту* $A$ *положить* $x = y^d$.

В кольце $\mathbb{Z}/n\mathbb{Z}$ выполняется тождество $x^{\varphi(n)} = 1$. Поэтому $y^d = x^{ed} = x$. Следовательно, алгоритм корректен.

Данный алгоритм предлагает простой способ большому числу абонентов обмениваться друг с другом конфиденциальной информацией по незащищенным каналам связи. Для этого каждому абоненту нужно завести два ключа: секретный и открытый, выложив последний в открытый доступ. Тогда любой другой абонент сможет послать ему сообщение, зашифрованное с помощью открытого ключа, расшифровать которое за разумное время сможет только адресат.

Отметим, что не все наборы $(a, b, d)$ надежны. Например, если число $n + 1$ или $n - 1$ легко раскладывается на множители, то для числа $n$ можно успешно применить $(N \pm 1)$-методы факторизации, то есть секретный ключ в этом случае найдется довольно быстро. Кроме того, числа $a$ и $b$ не должны быть слишком близкими, т.к. тогда они будут близки к $\sqrt{n}$ и число $n$ можно будет быстро разложить на множители при помощи метода Ферма. Необходимо также, чтобы ни $a - 1$, ни $b - 1$ не являлось произведением маленьких простых чисел, т.к. в этом случае число $n$ можно будет быстро факторизовать при помощи (P-1)-метода Полларда [4, 6, 15].

**Общий модуль.** Если пары ключей выдаются пользователям одним центральным распределяющим органом, то можно зафиксировать единый для

всех модуль $n = ab$ и генерировать только пары чисел $e$ и $d$. Из следующей теоремы будет видно, что любой пользователь за короткое время способен быстро восстанавливать секретный ключ по любому открытому.

**Теорема 3.1.** *Пусть натуральные числа $n, e, d$ удовлетворяют условиям*

$$ed \equiv 1 \pmod{\varphi(n)},\ e < \varphi(n),\ d < \varphi(n)$$

*и пусть $n = ab$, где $a$ и $b$ — нечетные простые числа. Тогда существует полиномиальный вероятностный алгоритм, при помощи которого, зная числа $n, e, d$ можно найти разложение числа $n$. Обратно, зная разложение числа $n$ и число $e$, можно за полиномиальное время найти $d$.*

**Малый секретный ключ.** Поскольку при применении алгоритма RSA требуется возводить в степень $d$, может возникнуть желание взять в качестве $d$ не очень большое число. Однако, как видно из следующей теоремы, при малом $d$ систему можно взломать за весьма короткое время.

**Теорема 3.2.** *Пусть $n, e, d$ — натуральные числа,*

$$ed \equiv 1 \pmod{\varphi(n)}, e < \varphi(n), d < n^{1/4}/3 \text{ и пусть } n = pq,$$

*где $p$ и $q$ — нечетные простые числа, такие что $q < p < 2q$. Тогда существует полиномиальный алгоритм, при помощи которого, зная числа $n$ и $e$, можно найти число $d$.*

**Малый открытый ключ.** Для того, чтобы число $d$ не было слишком маленьким, часто в качестве $e$ берут какое-нибудь небольшое число, тогда $d$ будет гарантированно большим. Однако, при слишком маленьком $e$ может появиться множество других проблем. При использовании различных приемов, устраняющих данные проблемы, возникает вопрос небезопасности и злоумышленник может воспользоваться возможностями,которые дает следующая теорема, принадлежащая Копперсмиту.

**Теорема 3.3.** *Пусть* $n$ *— натуральное число и* $f(t) \in \mathbb{Z}[t]$ *многочлен степени* $s$ *со старшим коэффициентом* $1$. *Пусть также фиксировано некоторое число* $\varepsilon > 0$. *Тогда существует алгоритм,сложность которого полиномиально зависит от величины* $\ln n$, *при помощи которого можно найти все такие целые числа* $t_0$, *что* $|t_0| < n^{1/s-\varepsilon}$ *и* $f(t_0) \equiv 0 \pmod{n}$.

**Заключение.** В ходе работы были приведены основные определения, сформулированы и доказаны необходимые теоремы. Подробно рассмотрен алгоритм RSA и его уязвимость.

В процессе реализации метода пробных делений и метода Ферма получены следующие данные. При проверке числа 363 время выполнения метода пробных делений составило 3.203 секунды, а время выполнения алгоритма Ферма 3.745 секунды. Затем проверялось число 655359999, при этом время выполнения метода пробных делений — 6.737 секунды, метода Ферма — 4.052 секунды. В результате сравнения времени выполнения вышеперечисленных методов для разных чисел, можно сделать вывод о том, что метод Ферма работает быстрее с большими числами.

Таким образом, был вскрыт ряд проблем, имеющих отношение к рассматриваемой теме, и сделаны выводы о необходимости дальнейшего изучения и улучшения данного вопроса.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1 Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии. — М. МЦНМО, 2003. — С. 328.

2 Виноградов, И. В. Основы теории чисел. — 6-е издание переработанное и дополненное. — М.-Л. Гостехиздат, 1952 — С. 180.

3 Герман, О. Н., Нестеренко, Ю. В. Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. образования. — М. Академия, 2012. — С. 272. — (Сер. Бакалавриат)

4 Алферов, А. П., Зубов, А. Ю., Кузьмин, А. С., Черёмушкин, А. В. Основы криптографии. — М. Гелиос АРВ, 2-е издание. 2002. — С. 480.

5 Боревич, З. И., Шафаревич, И. Р. Теория чисел. М. Наука, 1985. — С. 500.

6 Ахо, А., Хопкрофт, Дж., Ульман, Дж. Построение и анализ вывычислительных алгоритмов. М. Мир, 1979. — С. 536.

7 Нечаев, В. И. Элементы криптографии. — М. Высшая школа, 1999. — С. 109.

8 Ноден, П., Китте, К. Алгебраическая алгоритмика. М. Мир, 1999. — С. 720.

9 Кнут, Д. Искусство программирования. Т.2. Получисленные алгоритмы. Вильяме: М.— СПб.— Киев, 3-е издание. 2000. — С. 832.

10 Чебышев, П. Л. Полное собрание сочинений. Т.1. Теория чисел. АН СССР, 1946. — С. 346.

11 Bach, E., Shallit, J. Algorithmic number theory. V.1. MIT Press, 1996. — P. 346.

12 Bosnia, W., van der Hulst, M.P. Faster primality testing (extended abstract) // Advances in Cryptology — EuroCrypt’89 / Jean-Jacques Quisquater and Joos Vandewalle, editors. Berlin: Springer-Verlag, 1989. (Lect. Notes in Comput. Sci.; V. 434). P. 652–656.

13 McKee, J. Speeding Fermat's factoring method // Math. Сотр. 1999. V. 68 (228). P. 1729 — 1737.

14 Pohst, M. A modification of the LLL-reduction algorithm //J. Symb. Сотр. 1987. V. 4. P. 123—128.

15 Pohst, M., Zassenhaus, H. Algorithmic algebraic number theory. Cambridge University Press, 1989. — P. 465.

16 Bressoud, D.M. Factorization and primality testing. Springer-Verlag, 1989. — P. 237.

17 Brillhart, J., Tonascia, J., Weinberger, P. On the Fermat quotient //Computers in number theory. London, N.Y. Acad. Press, 1971. P. 213—222.

18 Cohen, H. A course in computational algebraic number theory. Springer-Verlag, 1993. — P. 563.

19 Cox, D., Little, J., O'Shea, D. Ideals, verietes and algorithms. N.Y. Springer-Verlag, 1992. — P. 553. (Undergraduate Texts in Mathematics).

20 Ernuall, R., Metsankyla, T. On the p-divisibility of Fermat quotients // Math. Comp. 1997. V. 66 (219). P. 1353—1365.