Математическая логика, алгебра и теория чисел

Mathematical logic, algebra and number theory

УДК 511.235+519.719.2

АНАЛИЗ RSA-КРИПТОСИСТЕМЫ В АБСТРАКТНЫХ ЧИСЛОВЫХ КОЛЬЦАХ

Н. В. КОНДРАТЁНОК[1)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Квантовые компьютеры могут представлять реальную угрозу для некоторых современных криптосистем, например таких, как RSA-криптосистема. Аналог последней в абстрактных числовых кольцах не подвержен этой угрозе, так как в настоящий момент нет алгоритмов факторизации идеалов, использующих квантовые вычисления. В настоящей работе исследована RSA-криптосистема в абстрактных числовых кольцах, доказаны аналоги теорем, связанных с ее криптостойкостью. В частности, доказан аналог теоремы Винера о малой секретной экспоненте. Изучен метод, аналогичный методу повторного шифрования, и на его основе получены необходимые ограничения на параметры криптосистемы. Также показано, что в числовых дедекиндовых кольцах задача факторизации полиномиально эквивалентна факторизации в целых числах.

Ключевые слова: RSA-криптосистема; абстрактное числовое кольцо; дедекиндово кольцо; факторизация; идеал.

Благодарность. Автор признателен за полезные замечания по данной статье своему научному руководителю – кандидату физико-математических наук М. М. Васьковскому.

Образец цитирования:
Кондратёнок НВ. Анализ RSA-криптосистемы в абстрактных числовых кольцах. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020;1:13–21.
https://doi.org/10.33581/2520-6508-2020-1-13-21

For citation:
Kondratyonok NV. Analysis of the RSA-cryptosystem in abstract number rings. *Journal of the Belarusian State University. Mathematics and Informatics.* 2020;1:13–21. Russian.
https://doi.org/10.33581/2520-6508-2020-1-13-21

Автор:
Никита Васильевич Кондратёнок – магистрант факультета прикладной математики и информатики. Научный руководитель – кандидат физико-математических наук М. М. Васьковский.

Author:
Nikita V. Kondratyonok, master's degree student at the faculty of applied mathematics and computer science.
nkondr2006@rambler.ru
https://orcid.org/0000-0002-6109-5635

Журнал Белорусского государственного университета. Математика. Информатика. 2020;1:13–21
Journal of the Belarusian State University. Mathematics and Informatics. 2020;1:13–21

ANALYSIS OF THE RSA-CRYPTOSYSTEM IN ABSTRACT NUMBER RINGS

N. V. KONDRATYONOK[a]

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*

Quantum computers can be a real threat to some modern cryptosystems (such as the RSA-cryptosystem). The analogue of the RSA-cryptosystem in abstract number rings is not affected by this threat, as there are currently no factorization algorithms using quantum computing for ideals. In this paper considered an analogue of RSA-cryptosystem in abstract number rings. Proved the analogues of theorems related to its cryptographic strength. In particular, an analogue of Wiener's theorem on the small secret exponent is proved. The analogue of the re-encryption method is studied. On its basis the necessary restrictions on the parameters of the cryptosystem are obtained. It is also shown that in numerical Dedekind rings the factorization problem is polynomial equivalent to factorization in integers.

Keywords: RSA-cryptosystem; abstract number ring; Dedekind ring; factorization; ideal.

Acknowledgements. I thank my supervisor PhD (physics and mathematics) M. M. Vas'kovskii for reading the work and comments.

Введение

Впервые криптосистема RSA была предложена Р. Ривестом, А. Шамиром и Л. Адлеманом в августе 1977 г. Полное ее описание опубликовано в журнале «Communications of the ACM» в феврале 1978 г. [1]. Алгоритм был основан на вычислительной сложности задачи факторизации натуральных чисел. Впоследствии сделано много обобщений этой криптосистемы. Известны ее модификации для многочленов и гауссовых чисел [2–5]. В работе [6] представлен аналог RSA-криптосистемы в квадратичных кольцах, а также доказан ряд теорем, связанных с ее безопасностью, в том числе описан способ защиты от атаки методом повторного шифрования и доказан аналог теоремы Винера о малой секретной экспоненте. В [7] RSA-криптосистема обобщена на случай произвольных абстрактных числовых колец, в качестве элементов криптосистемы предлагается брать не элементы кольца, а его идеалы. В отличие от классической RSA-криптосистемы такое обобщение неуязвимо от взлома с помощью квантовых алгоритмов факторизации, так как аналогичный алгоритм для абстрактных числовых колец пока не разработан.

Цель работы – изучение аналога RSA-криптосистемы в абстрактных числовых кольцах, а также доказательство аналогичных теорем, связанных с ее безопасностью.

Рассмотрим произвольное кольцо R. *Идеалом* кольца R называется подкольцо, замкнутое относительно умножения на элементы из R. Коммутативное кольцо с единицей и без делителей нуля называется *дедекиндовым*, если любой собственный идеал в нем раскладывается в конечное произведение простых идеалов. Более того, можно показать, что это разложение единственно с точностью до перестановки множителей.

Определение [8]. Абстрактное числовое кольцо – это такое дедекиндово кольцо R, что $\left|R/\mathfrak{m}\right| < \infty$ для любого ненулевого идеала $\mathfrak{m}$.

Примеры абстрактных числовых колец [8]:

• кольцо целых алгебраических чисел числового поля K;

• кольцо координат $\mathbb{F}_q\left[C^\circ\right]$ неособой интегральной аффинной кривой $C^\circ/\mathbb{F}_q$.

Мощность множества $R/\mathfrak{m}$ называется нормой $\mathfrak{m}$ и обозначается $\mathcal{N}(\mathfrak{m})$.

Далее будем рассматривать только абстрактные числовые кольца.

В кольце R можно ввести аналог функции Эйлера $\varphi(\mathfrak{m}) = \left|\left(R/\mathfrak{m}\right)^\times\right|$, где $\left(R/\mathfrak{m}\right)^\times$ – группа единиц. Имеет место свойство мультипликативности:

$$\varphi\left(\prod_{i=1}^{k}\mathfrak{m}_i^{\alpha_i}\right) = \prod_{i=1}^{k}\varphi\left(\mathfrak{m}_i^{\alpha_i}\right).$$

В случае максимального идеала $\mathfrak{m}$ также выполнено следующее свойство:

$$\varphi\left(\mathfrak{m}^\alpha\right) = \left(\mathcal{N}(\mathfrak{m})\right)^\alpha - \left(\mathcal{N}(\mathfrak{m})\right)^{\alpha-1}.$$

Для введенного аналога функции Эйлера справедлива теорема Эйлера.

Утверждение 1 [7]. Пусть R – абстрактное числовое кольцо, $m \in \mathbb{R}$, $\mathfrak{U} \subset R$ – идеал. Если $Rm + \mathfrak{U} = R$, то $m^{\varphi(\mathfrak{U})} \equiv 1 (\mathrm{mod}\, \mathfrak{U})$.

Обозначим через $\mathcal{O}_K$ кольцо целых алгебраических чисел произвольного числового поля K. Кольцо $\mathcal{O}_K$ является абстрактным числовым кольцом. Также пусть $\mathcal{O}_K^{\times}$ – группа единиц кольца $\mathcal{O}_K$, $\mathrm{Nm}(m)$ – норма элемента $m \in \mathcal{O}_K$, $\mathcal{O}_{K,\mathfrak{m}} = \mathcal{O}_K / \mathfrak{m}$ и $\mathcal{O}_{K,\mathfrak{m}}^{\times}$ – аддитивная и мультипликативная группа вычетов по модулю $\mathfrak{m}$ соответственно.

Существует два способа представления идеалов [9; 10]:

• $\mathbb{Z}$-представление: $\mathfrak{p} = \oplus_{i=\overline{1,n}} \mathbb{Z}\alpha_i$, где $\alpha_i \in \mathcal{O}_K$;

• 2-представление: для любого $\alpha \in \mathfrak{p}$ существует $\beta \in \mathfrak{p}$ такое, что $\mathfrak{p} = \alpha\mathcal{O}_K + \beta\mathcal{O}_K$.

Будем обозначать идеалы в 2-представлении через (α, β), порожденный элементом $\alpha \in \mathcal{O}_K$ главный идеал – через $(\alpha) = \alpha\mathcal{O}_K$.

Утверждение 2. Пусть $\mathfrak{m} \in \mathcal{O}_K$. Тогда $\mathcal{N}((m)) = |\mathrm{Nm}(m)|$, также $(m) | (\mathrm{Nm}(m))$.

Напомним теорему Копперсмита, которая используется ниже при доказательстве одной из теорем о безопасности криптосистемы.

Теорема Копперсмита [11]. *Пусть $f(x, y)$ – неприводимый многочлен от двух переменных над $\mathbb{Z}$ со степенью δ по каждой переменной отдельно. Пусть X, Y – границы предполагаемого решения (x_0, y_0) и W – модуль максимального коэффициента $f(xX, yY)$. Если $XY \le W^{2/(3\delta)}$, то существует полиномиальный относительно* $\log W$ *и* 2^{δ} *алгоритм, который позволяет найти все (x_0, y_0) такие, что $f(x_0, y_0) = 0$, $|x_0| \le X$ и $|y_0| \le Y$.*

Теорема Дедекинда [12]. *Пусть $K = \mathbb{Q}(\theta)$ – числовое поле, $f(T)$ – минимальный многочлен алгебраического числа θ в $\mathbb{Z}[T]$. Для простого рационального числа p, не делящего индекс $[\mathcal{O} : \mathbb{Z}[\theta]]$, запишем: $f(T) \equiv \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} (\mathrm{mod}\, p)$, где $\pi_i(T)$ – различные монические неприводимые многочлены в $\mathbb{F}_p[T]$, $i = \overline{1, p}$. Тогда $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, где $\mathfrak{p}_i = (p_i, T_i(\theta))$, $T_i(T) \equiv \pi_i(T) (\mathrm{mod}\, p)$.*

Аналог RSA-криптосистемы в дедекиндовых кольцах

В работе [7] был предложен аналог RSA-криптосистемы в R и доказана его корректность. Генерация ключей этой системы происходит следующим образом:

• выбираются максимальные идеалы $\mathfrak{p}$, $\mathfrak{q} \subset R$;

• вычисляется значение функции Эйлера $\varphi(\mathfrak{N})$, где $\mathfrak{N} = \mathfrak{p}\mathfrak{q}$;

• выбирается целое число $e \in [1, \varphi(\mathfrak{N})]$ такое, что $(e, \varphi(\mathfrak{N})) = 1$;

• по расширенному алгоритму Евклида вычисляется число d такое, что $ed \equiv 1 (\mathrm{mod}\, \varphi(\mathfrak{N}))$.

Пара $(\mathfrak{N}, e)$ публикуется в качестве открытого ключа RSA, а пара $(\mathfrak{N}, d)$ играет роль закрытого ключа RSA. Отображение $f : R/\mathfrak{N} \to R/\mathfrak{N}$, $f(x) \equiv x^e (\mathrm{mod}\, \mathfrak{N})$, называется функцией шифрования, отображение $f^{-1} : R/\mathfrak{N} \to R/\mathfrak{N}$, $f^{-1}(x) \equiv x^d (\mathrm{mod}\, \mathfrak{N})$, – функцией расшифрования.

Нетрудно заметить, что, зная разложение на множители $\mathfrak{N} = \mathfrak{p}\mathfrak{q}$ для RSA-модуля, можно эффективно найти секретный ключ. В [6] получено обратное утверждение для норменно-евклидовых колец. Докажем аналогичную теорему для произвольного кольца с единственной факторизацией. Далее в теоремах будем рассматривать кольцо R определенного вида, а именно кольцо $\mathcal{O}_K$ целых алгебраических чисел числового поля K. Известно, что оно дедекиндово и удовлетворяет условиям выше.

Теорема 1. *Пусть $\mathcal{O}_K$ – кольцо с единственной факторизацией. В этом случае каждому идеалу соответствует некоторый элемент кольца. Пусть (N, e, d) – параметры RSA-криптосистемы в $\mathcal{O}_K$. Если d известно, то N можно эффективно разложить на множители с вероятностью не менее $\frac{1}{2}$ за полиномиальное относительно длины N количество арифметических операций в $\mathcal{O}_K$.*

Доказательство. Пусть $s = ed - 1 = 2^t u$, где $t, u \in \mathbb{Z}$ и u нечетное. Так как $\varphi(N) | s$, то $x^s \equiv 1 (\mathrm{mod}\, N)$ для всех $x \in \mathcal{O}_{K,N}^{\times}$. Обозначим $\mathcal{S}_N$ множество таких элементов $a \in \mathcal{O}_{K,N}^{\times}$, что $a^u \equiv 1 (\mathrm{mod}\, N)$ или существует $k \in \{0, \ldots, t-1\}$, при котором $a^{2^k u} \equiv -1 (\mathrm{mod}\, N)$. Пусть $A = \mathcal{O}_{K,N}^{\times} \setminus \mathcal{S}_N$. Рассмотрим произвольный элемент $a \in A$ и выберем наименьшее положительное число k такое, что $a^{2^k u} \equiv 1 (\mathrm{mod}\, N)$. Пусть

$b \equiv a^{2^{k-1}u} (\mathrm{mod}\, N)$. Легко заметить, что $b^2 \equiv 1 (\mathrm{mod}\, N)$ и $b \not\equiv \pm 1 (\mathrm{mod}\, N)$. Следовательно, $(b-1,\ N)$ – собственный делитель N. В [13] показано, что наибольший общий делитель $(b-1,\ N)$ можно вычислить за полиномиальное относительно $\log \mathrm{Nm}(N)$ число арифметических операций в $\mathcal{O}_K$. Аналогично случаю норменно-евклидовых колец можно показать, что $|\mathcal{S}_N| \le \frac{\varphi(N)}{2}$. Доказательство завершено.

Следующая теорема является аналогом теоремы Винера о малой секретной экспоненте [14]. Таковой для квадратичного кольца с единственной факторизацией был доказан в [6].

Теорема 2. *Пусть* $(\mathfrak{N},\ e,\ d)$, $\mathfrak{N} = \mathfrak{pq}$, *– параметры RSA-криптосистемы в абстрактном числовом кольце R, причем выполнено соотношение* $\mathcal{N}(\mathfrak{q}) < \mathcal{N}(\mathfrak{p}) < \alpha^2 \mathcal{N}(\mathfrak{q})$, *где* $\alpha > 1$. *Если* $d < \frac{\left(\mathcal{N}(\mathfrak{N})\right)^{1/4}}{\sqrt{2\alpha+2}}$, *то d можно эффективно вычислить за полиномиальное относительно* $\log \mathcal{N}(\mathfrak{N})$ *число бинарных операций.*

Доказательство. Пусть $ed - 1 = k\varphi(\mathfrak{N})$, $k \in \mathbb{Z}$. Так как $\mathcal{N}(\mathfrak{q}) + \mathcal{N}(\mathfrak{p}) < (\alpha+1)\sqrt{\mathcal{N}(\mathfrak{N})}$, то $\mathcal{N}(\mathfrak{N}) - \varphi(\mathfrak{N}) = \mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) - 1 < (\alpha+1)\sqrt{\mathcal{N}(\mathfrak{N})}$. Поскольку $k\varphi(\mathfrak{N}) < ed$, $e < \varphi(\mathfrak{N})$, то $k < d$. Из последнего следует неравенство

$$\frac{(\alpha+1)k}{d\sqrt{\mathcal{N}(\mathfrak{N})}} < \frac{1}{2d^2}.$$

Принимая в расчет соотношения выше, получим

$$\left| \frac{e}{\mathcal{N}(\mathfrak{N})} - \frac{k}{d} \right| < \frac{1}{2d^2},$$

следовательно, $\frac{k}{d}$ – подходящая дробь для несекретной дроби $\frac{e}{\mathcal{N}(\mathfrak{N})}$. Таким образом, $\frac{k}{d}$ можно вычислить, используя алгоритм Евклида в $\mathbb{Z}$. Теорема доказана.

Один из известных способов взлома RSA-криптосистемы – это метод повторного шифрования. Пусть $(\mathfrak{N},\ e,\ d)$ – параметры RSA-криптосистемы, $y \equiv x^e (\mathrm{mod}\, \mathfrak{N})$ – зашифрованное сообщение $x \in \mathcal{O}_{K,\mathfrak{N}}$. Для нахождения x вычисляем элементы последовательности $y_i = y^{e^i} (\mathrm{mod}\, \mathfrak{N})$, $i = 1, 2, \ldots$, пока не получим $y_m = y$. Несложно показать, что $y_{m-1} = x$. Итак, параметры RSA-криптосистемы надо выбирать таким образом, чтобы m было достаточно велико.

Следующая теорема дает ответ на вопрос о безопасности RSA-криптосистемы относительно атаки повторным шифрованием. Ее доказательство аналогично доказательству теоремы из [6] для случая квадратичных колец с единственной факторизацией.

Теорема 3. *Пусть* $\mathfrak{N} = \mathfrak{pq}$ *– модуль RSA-криптосистемы в кольце* $\mathcal{O}_K$. *Предположим, существуют различные простые числа r, s и положительные целые k, l такие, что* $\varphi(\mathfrak{p}) = rk$, $\varphi(\mathfrak{q}) = sl$, *и* $r-1$, $s-1$ *имеют разные простые делители* r_1, s_1 *соответственно. Пусть y и e – независимые равномерно распределенные случайные величины со значениями в* $\mathcal{O}_{K,\mathfrak{N}}$ *и* $\mathbb{Z}^*_{\varphi(\mathfrak{N})}$ *соответственно. Тогда для вероятности выполняется неравенство*

$$\mathbb{P}\left(m_{e,y} \ge r_1 s_1\right) \ge \left(1 - r^{-1}\right)\left(1 - s^{-1}\right)\left(1 - r_1^{-1}\right)\left(1 - s_1^{-1}\right),$$

где $m_{e,y}$ *– наименьшее натуральное число такое, что* $y^{e^{m_{e,y}}} \equiv y (\mathrm{mod}\, \mathfrak{N})$.

Доказательство. Оценим вероятность $\mathbb{P}\left\{ rs \middle| \mathrm{ord}_{\mathcal{O}^\times_{K,\mathfrak{N}}}(y) \right\}$. Так как $\mathcal{O}^\times_{K,\mathfrak{N}} \cong \mathcal{O}^\times_{K,\mathfrak{p}} \times \mathcal{O}^\times_{K,\mathfrak{q}}$ и группы $\mathcal{O}^\times_{K,\mathfrak{p}}$, $\mathcal{O}^\times_{K,\mathfrak{q}}$ циклические, то можно записать $y = \left(a^i,\ b^j\right)$, где a и b – примитивные элементы $\mathcal{O}^\times_{K,\mathfrak{p}}$ и $\mathcal{O}^\times_{K,\mathfrak{q}}$ соответственно; i и j – случайные величины со значениями из $\{1, \ldots, rk\}$ и $\{1, \ldots, sl\}$ соответственно. Легко заметить, что

$$\mathrm{ord}_{\mathcal{O}^\times_{K,\mathfrak{N}}}(y) = \mathrm{lcm}\left(\frac{rk}{(rk,\ i)},\ \frac{sl}{(sl,\ j)} \right).$$

Если $r \nmid i$ и $s \nmid j$, то $\operatorname{ord}_{\mathcal{O}^{\times}_{K,\mathfrak{N}}}(y) \vdots rs$. Таким образом,

$$\mathbb{P}\left(rs \middle| \operatorname{ord}_{\mathcal{O}^{\times}_{K,\mathfrak{N}}}(y)\right) \geq \mathbb{P}\{r \nmid i,\ s \nmid j\} = \frac{\varphi(r)k\varphi(s)l}{rksl} = \left(1-\frac{1}{r}\right)\left(1-\frac{1}{s}\right).$$

Так как $e \in \mathbb{Z}^{*}_{rs}$, то аналогично можно получить неравенство

$$\mathbb{P}\left(r_1 s_1 \middle| \operatorname{ord}_{\mathbb{Z}^{*}_{rs}}(e)\right) \geq \left(1-\frac{1}{r_1}\right)\left(1-\frac{1}{s_1}\right).$$

Легко заметить, что $\operatorname{ord}_{W^{\times}_{\mathfrak{N}}}(y) \left| \left(e^{m_{e,y}} - 1\right)\right.$, поэтому

$$\left\{rs \middle| \operatorname{ord}_{\mathcal{O}^{\times}_{K,\mathfrak{N}}}(y)\right\} \subseteq \left\{\operatorname{ord}_{\mathbb{Z}^{*}_{rs}}(e) \middle| m_{e,y}\right\}.$$

Из приведенных выше соотношений следует, что

$$\mathbb{P}\left(m_{e,y} \geq r_1 s_1\right) \geq \mathbb{P}\left(r_1 s_1 \middle| m_{e,y}\right) \geq \mathbb{P}\left(r_1 s_1 \middle| \operatorname{ord}_{\mathbb{Z}^{*}_{rs}}(e),\ rs \middle| \operatorname{ord}_{\mathcal{O}^{\times}_{K,\mathcal{N}}}(y)\right) \geq$$
$$\geq \left(1-r^{-1}\right)\left(1-s^{-1}\right)\left(1-r_1^{-1}\right)\left(1-s_1^{-1}\right).$$

Теорема доказана.

Замечание 1. Для обеспечения безопасности RSA-криптосистемы в кольце с единственной факторизацией $\mathcal{O}_K$ против атаки повторного шифрования необходимо брать такие идеалы $\mathfrak{p}, \mathfrak{q} \subset \mathcal{O}_K$, для которых существуют большие различные простые делители r, s чисел $\varphi(\mathfrak{p})$, $\varphi(\mathfrak{q})$ и большие различные простые делители r_1, s_1 чисел $r-1$, $s-1$.

Теорема 4. *Пусть* $(\mathfrak{N}, e, d)$ *– параметры RSA-криптосистемы в* $\mathcal{O}_K$*, где* $\mathcal{N}(\mathfrak{p})$, $\mathcal{N}(\mathfrak{q})$ *имеют одинаковую битовую длину. Пусть* $ed \leq \left(\mathcal{N}(\mathfrak{N})\right)^2$, $\mathcal{N}(\mathfrak{N}) \geq 107$. *Если d известно, то существует полиномиальный алгоритм (относительно* $\log W$*), который позволяет найти* $\mathcal{N}(\mathfrak{p})$, $\mathcal{N}(\mathfrak{q})$.

Доказательство. Из $ed \equiv 1 \left(\operatorname{mod} \varphi(\mathfrak{N})\right)$ следует $ed = k\varphi(\mathfrak{N}) + 1$ для некоторого $k \in \mathbb{N}$. Предположим, что $\mathcal{N}(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{q})$. Тогда

$$\mathcal{N}(\mathfrak{p}) \leq \left(\mathcal{N}(\mathfrak{N})\right)^{1/2} \leq \mathcal{N}(\mathfrak{q}) < 2\mathcal{N}(\mathfrak{p}) \leq 2\left(\mathcal{N}(\mathfrak{N})\right)^{1/2}.$$

Следовательно,

$$\mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) < 3\left(\mathcal{N}(\mathfrak{N})\right)^{1/2} \leq \frac{\mathcal{N}(\mathfrak{N})}{2}.$$

Из этого неравенства имеем

$$\varphi(\mathfrak{N}) = \left(\mathcal{N}(\mathfrak{p}) - 1\right)\left(\mathcal{N}(\mathfrak{q}) - 1\right) = \mathcal{N}(\mathfrak{N}) + 1 - \mathcal{N}(\mathfrak{p}) - \mathcal{N}(\mathfrak{q}) >$$
$$> \mathcal{N}(\mathfrak{N}) + 1 - \frac{\mathcal{N}(\mathfrak{N})}{2} > \frac{\mathcal{N}(\mathfrak{N})}{2}.$$

Обозначим $\overline{k} = \dfrac{ed-1}{\mathcal{N}(\mathfrak{N})}$. Тогда

$$k - \overline{k} = \frac{\left(\mathcal{N}(\mathfrak{N}) - \varphi(\mathfrak{N})\right)(ed-1)}{\mathcal{N}(\mathfrak{N})\varphi(\mathfrak{N})} = \frac{\left(\mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) - 1\right)(ed-1)}{\mathcal{N}(\mathfrak{N})\varphi(\mathfrak{N})}.$$

Из выражений выше следует, что $k - \overline{k} < 6\left(\mathcal{N}(\mathfrak{N})\right)^{-3/2}(ed-1)$.

Пусть $x = k - \overline{k}$. Также выполнено $\mathcal{N}(\mathfrak{N}) - \varphi(\mathfrak{N}) = \mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) - 1 < 3\left(\mathcal{N}(\mathfrak{N})\right)^{1/2}$. Следовательно, $\varphi(\mathfrak{N}) \in \left[\mathcal{N}(\mathfrak{N}) - 3\left(\mathcal{N}(\mathfrak{N})\right)^{1/2},\ \mathcal{N}(\mathfrak{N})\right]$. Разделим этот интервал на 6 интервалов длиной $\dfrac{\left(\mathcal{N}(\mathfrak{N})\right)^{1/2}}{2}$ с центрами в точках $\mathcal{N}(\mathfrak{N}) - \dfrac{2i-1}{4}\left(\mathcal{N}(\mathfrak{N})\right)^{1/2}$, $i = \overline{1,\ 6}$. Рассмотрим $i \in \{1, \ldots, 6\}$ такое, что

$$\left|\mathcal{N}(\mathfrak{N}) - \frac{2i-1}{4}\left(\mathcal{N}(\mathfrak{N})\right)^{1/2} - \varphi(\mathfrak{N})\right| \leq \frac{1}{4}\left(\mathcal{N}(\mathfrak{N})\right)^{1/2}.$$

Пусть $g = \frac{2i-1}{4}\mathcal{N}(\mathfrak{N})$. Тогда $\left|\mathcal{N}(\mathfrak{N}) - g - \varphi(\mathfrak{N})\right| < \frac{1}{4}\left(\mathcal{N}(\mathfrak{N})\right)^{1/2} + 1$ и $\varphi(\mathfrak{N}) = \mathcal{N}(\mathfrak{N}) - g - y$ для некоторого неизвестного y такого, что $|y| \le \frac{1}{4}\left(\mathcal{N}(\mathfrak{N})\right)^{1/2}$. Далее получим

$$ed - 1 = k\varphi(\mathfrak{N}) = \left(\lceil \bar{k} \rceil + x\right)\left(\mathcal{N}(\mathfrak{N}) - g - y\right).$$

Рассмотрим многочлен

$$f(x, y) = xy - \left(\mathcal{N}(\mathfrak{N}) - g\right)x + \lceil \bar{k} \rceil y - \lceil \bar{k} \rceil\left(\mathcal{N}(\mathfrak{N}) - g\right) + ed - 1,$$

у которого есть корень $(x_0, y_0) = \left(k - \lceil \bar{k} \rceil,\ \mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) + 1 - g\right)$. Имеем $\delta = 1$, где δ из теоремы Копперсмита. Положим $X = 6\left(\mathcal{N}(\mathfrak{N})\right)^{1/2}$, $Y = \frac{1}{4}\left(\mathcal{N}(\mathfrak{N})\right)^{1/2} + 1$. Тогда $|x_0| \le X$ и $|y_0| \le Y$. Пусть W – норма вектора коэффициентов многочлена $f(xX, yY)$, для которой справедливо $W \ge \left(\mathcal{N}(\mathfrak{N}) - g\right)X > 3\left(\mathcal{N}(\mathfrak{N})\right)^{3/2}$. Следовательно,

$$XY = \frac{3}{2}\mathcal{N}(\mathfrak{N}) + 6\left(\mathcal{N}(\mathfrak{N})\right)^{1/2} < W^{2/3} = W^{2/(3\delta)}$$

для $\mathcal{N}(\mathfrak{N}) \ge 107$.

Теперь можно применить теорему Копперсмита и найти корень (x_0, y_0) за полиномиальное относительно $\log W$ время. Данный корень позволяет определить $\mathcal{N}(\mathfrak{p})$, $\mathcal{N}(\mathfrak{q})$. Теорема доказана.

Заметим, что теорема 4 – это аналог известного результата для RSA-криптосистемы в целых числах [15]. Еще одним ограничением на выбор RSA-ключей является то, что RSA-модули должны быть различными для разных пользователей. Покажем, что при реализации аналога RSA-криптосистемы это ограничение сохраняется в определенных кольцах.

Обозначим $\Lambda_K = \sup\limits_{m/n \in F}\left|\frac{m}{n}\right|$, где $\left|\frac{m}{n}\right| = \frac{\upsilon(m)}{\upsilon(n)}$ для $\frac{m}{n} \in F \setminus \{0\}$, $|0| = 0$, F – множество правильных несократимых дробей поля частных K, $\upsilon(m)$ – норма в кольце K.

Теорема 5. *Пусть $\mathbb{K}$ – евклидово кольцо относительно нормы $\upsilon(\cdot)$, $\Lambda_{\mathbb{K}} < 1$, и кольцо вычетов любого элемента $\mathbb{K}$ конечно. Тогда в $\mathbb{K}$ можно рассмотреть реализацию RSA-криптосистемы. Предположим, что два пользователя имеют одинаковые RSA-модули, но разные секретные экспоненты e_1 и e_2, $(e_1, e_2) = 1$. Пусть перехвачены сообщения $c_1 \equiv m^{e_1} (\mathrm{mod}\, N)$ и $c_2 \equiv m^{e_2} (\mathrm{mod}\, N)$, где c_1, c_2, m, $N \in \mathbb{K}$. Тогда сообщение m можно вычислить за полиномиальное относительно $\log\upsilon(N)$ количество арифметических операций в $\mathbb{K}$.*

Доказательство. Условие $(e_1, e_2) = 1$ означает, что существуют $s_1, s_2 \in \mathbb{Z}$ такие, что $e_1 s_1 + e_2 s_2 = 1$. Следовательно, можно вычислить

$$c_1^{s_1} c_2^{s_2} = \left(m^{e_1}\right)^{s_1}\left(m^{e_2}\right)^{s_2} = m^{e_1 s_1 + e_2 s_2} = m.$$

Единственная сложность заключается в том, что одно из чисел s_1, s_2 будет отрицательным. Не нарушая общности, предположим, что $s_2 < 0$. Тогда можно записать $c_2^{s_2} = \left(c_2^{-1}\right)^{|s_2|}$. Требуется найти $c_2^{-1} \bmod N$, что эквивалентно решению уравнения $c_2 x + Ny = (c_2, N)$. Если $(c_2, N) \ne 1$, то известно разложение N на простые множители и сообщение m можно вычислить стандартным способом. В случае $(c_2, N) = 1$ надо решить уравнение $c_2 x + Ny = 1$, что можно сделать с помощью цепочек деления. Из теоремы 2 в работе [16] следует, что $l_n(\mathbb{K}) \le \left[\log_{\Lambda_{\mathbb{K}}^{-1}} n\right] + 2$. Это означает, что длина цепочки с выбором минимального по норме остатка для c_2 и N ограничена логарифмом от их модуля. Следовательно, ее можно найти за полиномиальное относительно $\log\upsilon(N)$ количество арифметических операций в $\mathbb{K}$. Из построения RSA-криптосистемы следует, что $e_1 < \upsilon(N)$ и $e_2 < \upsilon(N)$, поэтому сообщение m можно вычислить за полиномиальное относительно $\log\upsilon(N)$ количество арифметических операций в $\mathbb{K}$. Теорема доказана.

Замечание 2. В [17] показано, что $\Lambda_{\mathbb{K}} < 1$ во всех квадратичных норменно-евклидовых кольцах.

Субэкспоненциальные алгоритмы факторизации в числовых полях

Приведем способ разложения идеала на произведение простых идеалов и таким образом покажем, что задача факторизации идеалов эквивалентна задаче факторизации целых чисел. Данная проблема актуальна и была рассмотрена в [18], где приведен алгоритм по определению степени простого идеала в разложении другого идеала. В настоящей работе строится алгоритм нахождения простых идеалов из разложения идеала и их степеней.

Пусть дан идеал (N) в форме своего 2-представления. Для начала запишем основные шаги алгоритма факторизации.

Шаг 1. Считаем норму идеала равной норме элемента N и раскладываем ее на множители одним из известных алгоритмов для факторизации целых чисел:

$$\mathrm{Nm}(N) = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Следовательно,

$$\left(\mathrm{Nm}(N)\right) = \prod_{i=1}^{k} (p_i)^{\alpha_i}.$$

Шаг 2. Факторизуем идеал (p_i) с помощью теоремы Дедекинда и получаем двухэлементные представления идеалов

$$(p_i) = \prod_{j=1}^{l_i} \left(p_i, f_{i,j}(\theta)\right).$$

Шаг 3. Преобразуем полученные простые идеалы в $\mathbb{Z}$-представление и объединяем равные. В итоге имеем

$$\left(\mathrm{Nm}(N)\right) = \prod_{i=1}^{l} \mathfrak{p}_i^{\beta_i}.$$

Шаг 4. Находим с помощью бинарного поиска степени, в которых $\mathfrak{p}_i$ входит в (N).

Для вычисления нормы идеала (N) необходимо найти определитель матрицы, которая получается при матричном представлении элемента N. Таким образом, справедливо следующее утверждение.

Утверждение 3. Для вычисления нормы идеала (N) необходимо $O\left(\log^2 |N|\right)$ бинарных операций, где $|N|$ обозначает максимальный по модулю элемент матричного представления N.

Предположим, что $\mathcal{O}_K$ фиксировано. Значит, известны индекс $\left[\mathcal{O}_K : \mathbb{Z}[\theta]\right]$ и разложение на простые идеалы всех простых делителей индекса. Следуя второму шагу алгоритма, рассмотрим простое число p и оценим сложность разложения идеала (p) на множители. Также оценим сложность разложения многочлена на множители в $\mathbb{F}_p$. Так как степень многочлена не превосходит константы, сделать это можно с помощью вероятностной версии алгоритма Берлекэмпа за $O\left(\log^3 p\right)$ бинарных операций. В результате разложения получим многочлены, количество которых не превосходит константы, зависящей только от $\mathcal{O}_K$. Тогда вычислить значения многочленов в разложении можно за $O\left(\log^2 p\right)$ операций. Таким образом, доказано следующее утверждение.

Утверждение 4. Разложить идеал (p), используя теорему Дедекинда, можно за $O\left(\log^3 p\right)$ бинарных операций.

Рассмотрим преобразование идеала из 2-представления в $\mathbb{Z}$-представление.

Утверждение 5. Преобразовать 2-представление идеала (p, α) из теоремы Дедекинда в $\mathbb{Z}$-представление можно за $O\left(P(\log p)\right)$ бинарных операций, где $P(T)$ – некоторый полином.

Доказательство. В [19] описан алгоритм преобразования 2-представления в $\mathbb{Z}$-представление. Необходимо найти эрмитову нормальную форму блочной матрицы $\begin{pmatrix} A \\ B \end{pmatrix}$, где $A = \mathrm{diag}(p, \ldots, p)$, а B является матричным представлением элемента α.

В 1979 г. было доказано, что эрмитову нормальную форму матрицы можно найти за строго полиномиальное время [20]. Это означает, что алгоритму необходимо полиномиальное (относительно размеров матрицы) количество арифметических операций над числами, не превосходящими полинома от бинарного представления элементов матрицы. Таким образом, учитывая, что n зависит только от $\mathcal{O}_K$, эрмитову нормальную форму можно вычислить за $O\left(P(\log p)\right)$ бинарных операций, где $P(T)$ – некоторый полином. Утверждение доказано.

Замечание 3. Схемы разделения секрета являются составной частью многих криптографических протоколов. В [21–23] представлены новые эффективные схемы верификации модулярного разделения секрета на основе свойств делимости многочленов с целыми коэффициентами или умножения параметров схемы на подходящие случайные величины. Предложенные протоколы могут быть безопасно использованы для многочленов над произвольными конечными полями без дополнительных ограничений на мощность поля.

Замечание 4. Зная разложение $\left(p_i\right)$ на произведение простых идеалов, можно найти одинаковые идеалы и разложение $\left(\mathrm{Nm}\left(N\right)\right)$ на произведение различных идеалов за $O\left(P\left(\log \mathrm{Nm}\left(N\right)\right)\right)$ бинарных операций, так как $k \le \log \mathrm{Nm}\left(N\right)$ и l_i ограничены константой, зависящей только от $\mathcal{O}_K$. Значит, найти разложение идеала $\left(\mathrm{Nm}\left(N\right)\right)$ на произведение различных простых идеалов можно за полиномиальное относительно $\log \mathrm{Nm}\left(N\right)$ и $\log\left|N\right|$ количество бинарных операций, если разложение $\mathrm{Nm}\left(N\right)$ на множители известно [24–26].

Таким образом, аналог RSA-криптосистемы в некотором смысле не дает никакого выигрыша при использовании в кольцах алгебраических целых числовых полей.

Библиографические ссылки

1. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM.* 1978;21(2):120–126. DOI: 10.1145/359340.359342.

2. Li B. Generalizations of RSA public key cryptosystem. *IACR, Cryptology ePrint Archive* [Preprint]. 2005 [cited 2019 August 23]. Available from: https://arxiv.org/ia.cr/2005/285.

3. Elkamchouchi H, Elshenawy K, Shaban H. Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: *ICCS 2002. Proceedings of the 8th International conference on communication systems; 2002 November 28; Singapore, Singapore. Volume 1.* [S. l.]: IEEE; 2002. p. 91–95. DOI: 10.1109/ICCS.2002.1182444.

4. Koval A, Verkhovsky B. Analysis of RSA over Gaussian Integers Algorithm. In: *ITNG 2008. Proceedings of the Fifth International conference on information technology: new generations; 2008 April 7–9; Las Vegas, Nevada.* Washington: IEEE Computer Society; 2008. p. 101–105. DOI: 10.1109/ITNG.2008.44.

5. El-Kassar AN, Haraty RA, Awad YA, Debnath NC. Modified RSA in the domains of Gaussian integers and polynomials over finite fields. In: *Proceedings of the ISCA 18th International conference on computer applications in industry and engineering; 2005 November 9–11; Honolulu, Hawaii.* [S. l.]: International Society for Computers and their Applications (ISCA); 2005. p. 298–303.

6. Vaskouski M, Kondratyonok N, Prochorov N. Primes in quadratic unique factorization domains. *Journal of Number Theory.* 2016;168:101–116. DOI: 10.1016/j.jnt.2016.04.022.

7. Petukhova KA, Tronin SN. RSA Cryptosystem for Dedekind rings. *Lobachevskii Journal of Mathematics.* 2016;37:284–287. DOI: 10.1134/S1995080216030197.

8. Brunyate A, Clark PL. Extending the Zolotarev – Frobenius approach to quadratic reciprocity. *The Ramanujan Journal.* 2015; 37(1):25–50. DOI: 10.1007/s11139-014-9635-y.

9. Cohen HA. *Course in computational algebraic number theory.* Berlin: Springer; 1996. 545 p.

10. Cohen H. *Advanced topics in computational number theory.* New York: Springer; 1999. 599 p.

11. Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology.* 1997; 10:233–260. DOI: 10.1007/s001459900030.

12. Dedekind R. Über den zusammenhang zwischen der theorie der ideale und der theorie der höheren congruenzen. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen.* 1878;23:3–38.

13. Wikstrom D. On the *l*-Ary GCD-algorithm in rings of integers. In: Caires L, Italiano GF, Monteiro L, Palamidessi C, Yung M, editors. *Automata, Languages and Programming. 32nd International Colloquium, ICALP; 2005 July 11–15; Lisbon, Portugal.* Berlin: Springer; 2005. p. 1189–1201. DOI: 10.1007/11523468_96.

14. Wiener MJ. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory.* 1990;36(3):553–558. DOI: 10.1109/18.54902.

15. Coron JS, May A. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. *Journal of Cryptology.* 2007;20(1):39–50. DOI: 10.1007/s00145-006-0433-6.

16. Vaskouski M, Kondratyonok N. Shortest division chains in unique factorization domains. *Journal of Symbolic Computation.* 2016;77:175–188. DOI: 10.1016/j.jsc.2016.02.003.

17. Васьковский ММ. Полиномиальная эквивалентность вычисления функции Эйлера RSA-модуля и поиска секретного ключа в квадратичных евклидовых кольцах. В: *Международный конгресс по информатике: информационные системы и технологии. Материалы Международного научного конгресса; 31 октября – 3 ноября 2011 г.; Минск, Беларусь. Часть 2*. Минск: БГУ; 2016. с. 427–430.

18. Бабуль ОВ, Васильев ДВ. О факторизации идеалов в кольцах целых алгебраических чисел. *Известия Национальной академии наук Беларуси. Серия физико-математических наук.* 2011;1:32–36.

19. Pohst ME. *Computational algebraic number theory.* Basel: Birkhäuser; 1993. 88 p. DOI: 10.1007/978-3-0348-8589-8.

20. Kannan R, Bachem A. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *SIAM Journal on Computing.* 1979;8(4):499–507. DOI: 10.1137/0208040.

21. Васьковский ММ, Матвеев ГВ. Верификация модулярного разделения секрета. *Журнал Белорусского государственного университета. Математика. Информатика.* 2017;2:17–22.

22. Матвеев ГВ, Матулис ВВ. Совершенная верификация модулярной схемы. *Журнал Белорусского государственного университета. Математика. Информатика.* 2018;2:4–9.

23. Матвеев ГВ. Разделение секрета в кольцах многочленов от нескольких переменных с использованием китайской теоремы об остатках. *Журнал Белорусского государственного университета. Математика. Информатика*. 2019;3:129–133. DOI: 10.33581/2520-6508-2019-3-129-133.

24. Гекке Э. *Лекции по теории алгебраических чисел.* Ольшанский ГИ, Райков ДА, переводчики. Москва: Государственное издательство технико-теоретической литературы; 1940. 261 с.

25. Глухов ММ, Круглов ИА, Пичкур АБ, Черемушкин АВ. *Введение в теоретико-числовые методы криптографии.* Санкт-Петербург: Лань; 2011. 400 с.

26. Koblitz N. *Course in number theory and cryptography.* New York: Springer-Verlag; 1994. 235 p.

References

1. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM.* 1978;21(2):120–126. DOI: 10.1145/359340.359342.

2. Li B. Generalizations of RSA public key cryptosystem. *IACR, Cryptology ePrint Archive* [Preprint]. 2005 [cited 2019 August 23]. Available from: https://arxiv.org/ia.cr/2005/285.

3. Elkamchouchi H, Elshenawy K, Shaban H. Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: *ICCS 2002. Proceedings of the 8th International conference on communication systems; 2002 November 28; Singapore, Singapore. Volume 1.* [S. l.]: IEEE; 2002. p. 91–95. DOI: 10.1109/ICCS.2002.1182444.

4. Koval A, Verkhovsky B. Analysis of RSA over Gaussian Integers Algorithm. In: *ITNG 2008. Proceedings of the Fifth International conference on information technology: new generations; 2008 April 7–9; Las Vegas, Nevada.* Washington: IEEE Computer Society; 2008. p. 101–105. DOI: 10.1109/ITNG.2008.44.

5. El-Kassar AN, Haraty RA, Awad YA, Debnath NC. Modified RSA in the domains of Gaussian integers and polynomials over finite fields. In: *Proceedings of the ISCA 18th International conference on computer applications in industry and engineering; 2005 November 9–11; Honolulu, Hawaii.* [S. l.]: International Society for Computers and their Applications (ISCA); 2005. p. 298–303.

6. Vaskouski M, Kondratyonok N, Prochorov N. Primes in quadratic unique factorization domains. *Journal of Number Theory.* 2016;168:101–116. DOI: 10.1016/j.jnt.2016.04.022.

7. Petukhova KA, Tronin SN. RSA Cryptosystem for Dedekind rings. *Lobachevskii Journal of Mathematics.* 2016;37:284–287. DOI: 10.1134/S1995080216030197.

8. Brunyate A, Clark PL. Extending the Zolotarev – Frobenius approach to quadratic reciprocity. *The Ramanujan Journal.* 2015; 37(1):25–50. DOI: 10.1007/s11139-014-9635-y.

9. Cohen HA. *Course in computational algebraic number theory.* Berlin: Springer; 1996. 545 p.

10. Cohen H. *Advanced topics in computational number theory.* New York: Springer; 1999. 599 p.

11. Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology.* 1997; 10:233–260. DOI: 10.1007/s001459900030.

12. Dedekind R. Über den zusammenhang zwischen der theorie der ideale und der theorie der höheren congruenzen. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen.* 1878;23:3–38.

13. Wikstrom D. On the *l*-Ary GCD-algorithm in rings of integers. In: Caires L, Italiano GF, Monteiro L, Palamidessi C, Yung M, editors. *Automata, Languages and Programming. 32nd International Colloquium, ICALP; 2005 July 11–15; Lisbon, Portugal.* Berlin: Springer; 2005. p. 1189–1201. DOI: 10.1007/11523468_96.

14. Wiener MJ. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory.* 1990;36(3):553–558. DOI: 10.1109/18.54902.

15. Coron JS, May A. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. *Journal of Cryptology.* 2007;20(1):39–50. DOI: 10.1007/s00145-006-0433-6.

16. Vaskouski M, Kondratyonok N. Shortest division chains in unique factorization domains. *Journal of Symbolic Computation.* 2016;77:175–188. DOI: 10.1016/j.jsc.2016.02.003.

17. Vaskouski MM. Polynomial equivalence of computing Euler's function from RSA modulus and searching for private key in euclidean quadratic domains. In*: International congress on computer science: information systems and technologies. Proceedings of the International scientific congress; 2011 October 31 – November 3; Minsk, Belarus. Part 2.* Minsk: Belarusian State University; 2016. p. 427–430. Russian.

18. Babul OV, Vasilyev DV. [Ideals factorization in the number]. *Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics Series.* 2011;1;32–36. Russian.

19. Pohst ME. *Computational algebraic number theory.* Basel: Birkhäuser; 1993. 88 p. DOI: 10.1007/978-3-0348-8589-8.

20. Kannan R, Bachem A. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *SIAM Journal on Computing.* 1979;8(4):499–507. DOI: 10.1137/0208040.

21. Vaskouski MM, Matveev GV. Verification of modular secret sharing. *Journal of the Belarusian State University. Mathematics and Informatics.* 2017;2:17–22. Russian.

22. Matveev GV, Matulis VV. Perfect verification of modular scheme. *Journal of the Belarusian State University. Mathematics and Informatics.* 2018;2:4–9. Russian.

23. Matveev GV. Chinese remainder theorem secret sharing in multivariate polynomials. *Journal of the Belarusian State University. Mathematics and Informatics.* 2019;3:129–133. Russian. DOI: 10.33581/2520-6508-2019-3-129-133.

24. Hecke E. *Vorlesung über die theorie der algebraischen zahlen.* Leipzig: Akademische Verlagsgesellschaft; 1923. 264 p.

Russian edition: Hecke E. *Lektsii po teorii algebraicheskikh chisel.* Ol'shanskii GI, Raikov DA, translators. Moscow: Gosudarstvennoe izdatel'stvo tekhniko-teoreticheskoi literatury; 1940. 261 p.

25. Glukhov MM, Kruglov IA, Pichkur AB, Cheremushkin AV. *Vvedenie v teoretiko-chislovye metody kriptografii* [Introduction to number theoretical methods in cryptography]. Saint Petersburg: Lan'; 2011. 400 p. Russian.

26. Koblitz N. *Course in number theory and cryptography.* New York: Springer-Verlag; 1994. 235 p.

Статья поступила в редколлегию 10.01.2020.
Received by editorial board 10.01.2020.