Раздел III. Криптографические системы и шифрование

УДК 519.72+004 DOI 10.18522/2311-3103-2025-3-91-99

В.О. Осипян, Е.С. Фурсина, Э.Т. Альгариб

РАЗРАБОТКА АЛФАВИТНОЙ ДИСИММЕТРИЧНОЙ ТРИГРАММНОЙ КРИПТОСИСТЕМЫ НА ОСНОВЕ РЕШЕНИЯ НОРМАЛЬНОЙ СИСТЕМЫ ДИОФАНТОВЫХ УРАВНЕНИЙ 5-Й СТЕПЕНИ РАЗМЕРНОСТИ ШЕСТЬ НАД КОЛЬЦОМ ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ

Целью работы являются разработка математической модели алфавитной криптосистемы на основе общего двухпараметрического решения нормальной системы диофантовых уравнений пятой степени размерности шесть над кольцом целых гауссовых числах и написание программы, демонстрирующей возможности такой криптосистемы. В работе реализована идея К. Шеннона по разработке математической модели криптосистемы, содержащие диофантовы трудности, возникающие при решении нормальных и других многостепенных систем диофантовых уравнений (МСДУ) типа Тарри-Эскотта. К. Шенноном отмечалось, что наибольшей неопределённостью при подборе ключей обладают криптосистемы, содержащие диофантовы трудности. Особенность таких МСДУ заключается в том, что неизвестны общие непереборные методы их решения на основе отрицательного решения 10-й проблемы Гильберта об алгоритмической неразрешимости произвольного диофантова уравнения в целых числах. Отметим также, что диофантовы уравнения представляют собой мощный инструмент в криптографии благодаря своей сложности, однако их использование требует глубокого понимания математического аппарата диофантова анализа при возможных методах решений для предотвращения уязвимостей в таких криптосистемах. Решения являются ключевыми факторами для обеспечения безопасности и надежности криптографических систем, основанных на этих уравнениях. Нами предусмотрено использовать стратегии и подходы в зависимости от значений размерности и степени таких МСДУ для повышения долю стойкости алфавитных систем защиты информации, включая количество параметров, входящих в её общее параметрическое решение, с учётом либо сложности алгоритма решения системы уравнений, либо самого решения, либо и того, и другого одновременно. В работе представлена математическая модель алфавитной дисимметричной триграммной криптосистемы на основе общего двухпараметрического решения нормальной системы диофантовых уравнений пятой степени размерности шесть над кольцом целых гауссовых числах, среди числовых значений параметров которых входят и числовые эквиваленты элементарных сообщений, и ключи, для нахождения которых нелегальному пользователю потребуется поискать общее двухпараметрическое решение нормальной системы диофантовых уравнений. Математическая модель алфавитной дисимметричной триграммной криптосистемы, представленная в работе, содержит диофантовы трудности, поэтому она обладает хорошей криптостойкостью: нелегальный пользователь не сможет сократить множество перебираемых ключей, ему необходимо решить систему диофантовых уравнений в гауссовых числах, что является трудно вычислимой задачей без обладания соответствующих секретных ключей. Также использование вместо посимвольного шифрования открытого текста – трехсимвольное (триграммы) ещё больше повышает криптостойкость системы. Приводится программная реализация указанной криптосистемы средствами языка Python.

Дисимметричная криптосистема; диофантовы трудности; многостепенная система диофантовых уравнений; гауссовы числа; криптосистема на основе решения системы диофантовых уравнений; триграммные криптосистемы.

V.O. Osipyan, E.S. Fursina, E.T. Algarib

DEVELOPMENT OF ALPHABETICAL DISSYMMETRIC TRIGRAM CRYPTOSYSTEM BASED ON SOLVING A NORMAL SYSTEM OF DIOPHANTINE EQUATIONS OF THE 5TH DEGREE OF DIMENSION SIX OVER THE RING OF GAUSSIAN INTEGERS

The aim of the work is to develop a mathematical model of an alphabetic cryptosystem based on a general two-parameter solution of a normal system of Diophantine equations of the fifth degree of dimension six over the ring of Gaussian integers and to write a program demonstrating the capabilities of such a cryptosystem. The paper implements the idea of K. Shannon to develop a mathematical model of a cryptosystem containing Diophantine difficulties encountered in solving normal and other multistep systems of Diophantine equations (MSDE) of the Tarry-Escott type. K. Shannon noted that cryptosystems containing Diophantine difficulties have the greatest uncertainty in selecting keys. The peculiarity of such MSDEs is that general non-exhaustive methods for solving them based on a negative solution to Hilbert's 10th problem on the algorithmic undecidability of an arbitrary Diophantine equation in integers are unknown. It should also be noted that Diophantine equations are a powerful tool in cryptography due to their complexity, but their use requires a deep understanding of the mathematical apparatus of Diophantine analysis with possible methods of solutions to prevent vulnerabilities in such cryptosystems. Solutions are key factors for ensuring the security and reliability of cryptographic systems based on these equations. We provide for the use of strategies and approaches depending on the values of the dimension and degree of such MSDE to increase the share of resistance of alphabetic information security systems (ISS), including the number of parameters included in its general parametric solution, taking into account either the complexity of the algorithm for solving the system of equations, or the solution itself, or both at the same time. The paper presents a mathematical model of an alphabetic dissymmetric trigram cryptosystem based on a general two-parameter solution of a normal system of Diophantine equations of the fifth degree of dimension six over a ring of integer Gaussian numbers, among the numerical values of the parameters of which are both numerical equivalents of elementary messages and keys, for finding which an illegal user will need to look for a general two-parameter solution of a normal system of Diophantine equations. The mathematical model of the alphabetic dissymmetric trigram cryptosystem presented in the paper contains Diophantine difficulties, so it has good cryptographic resistance: an illegal user will not be able to reduce the set of keys being tried, he needs to solve a system of Diophantine equations in Gaussian numbers, which is a difficult-to-calculate problem without having the corresponding secret keys. Also, the use of three-symbol (trigram) encryption of plaintext instead of symbolic encryption of plaintext further increases the cryptographic resistance of the system. A software implementation of the specified cryptosystem using the Python language is provided.

Dissymmetric cryptosystem; Diophantine difficulties; multi-degree system of Diophantine equations; Gaussian numbers; cryptosystem based on solving a system of Diophantine equations; trigram cryptosystems.

Введение. С учетом развития информационных технологий стоит острая необходимость усовершенствовать алгоритмы шифрования и методы защиты конфиденциальных данных для предотвращения возможных кибератак и утечек информации. Одним из важных направлений научных исследований в этой области является поиск новых криптографических решений для повышения безопасности передачи и хранения конфиденциальной информации. Для этого необходимо повышать криптостойкость существующих криптосистем или разрабатывать новые. Как известно, задачи, содержащие диофантовы трудности, являются сложными математическими задачами. Системы защиты информации, в которых используются такие задачи, не дают возможности сократить множество перебираемых ключей [1] Такие криптосистемы обладают наибольшей неопределенностью при подборе ключей [1, 14–21].

В работе рассматривается математическая модель алфавитной дисимметричной криптосистемы (АДК). Дисимметричные криптосистемы обобщают принцип построения криптосистем с открытым ключом: в них часть одного тождества используется в качестве функции прямого преобразования исходного текста в криптотекст, а вторая часть того же тождества используется в качестве функции обратного преобразования криптотекста в исходный текст [2]. Рассматриваемая математическая модель системы защиты инфор-

мации строится на основе двухпараметрического решения нормальной системы диофантовых уравнений 5-й степени размерности шесть в гауссовых числах, взятого из монографии В.О. Осипяна «Разработка методов построения систем передачи и защиты информации» [4]. Комплексные числа, у которых целая действительная часть и целый коэффициент при мнимой части, называются гауссовыми числами [4, 5, 7, 8]. Множество комплексных чисел

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

образует кольцо: это множество замкнуто относительно сложения, вычитания и умножения. Кольцо $\mathbb{Z}[i]$ называют кольцом целых гауссовых чисел.

Математическая модель алфавитной дисимметричной криптосистемы. Нормальная система диофантовых уравнений 5-й степени размерности шесть имеет вид [3–8]:

$$X_1^k + \ ... + \ X_6^k = \ Y_1^k + \ ... \ + \ Y_6^k, \text{ k = 1. .5} \tag{1}$$

или в компактной записи:

$$X_1, \dots, X_6 \overset{5}{=} Y_1, \dots, Y_6,$$

где $X_1, \dots, X_6, Y_1, \dots, Y_6$ – целочисленные неотрицательные переменные.

Её частные решения имеют вид:

$$a_1, \dots, a_6 \overset{5}{=} b_1, , \dots, b_6, \tag{2}$$

где $a_1, \dots, a_6, b_1, \dots, b_6 \in \mathbb{Z}$.

Для некоторых нормальных систем допускается параметризация по одному или нескольким параметрам. Если (2) – частное решение (1), удовлетворяющее следующим 4-м условиям [4]:

$$\sum_{k=1}^{6} a_k b_k (a_k - b_k) = 0, \sum_{k=1}^{6} a_k b_k \left(a_k^2 - b_k^2\right) = 0,$$
$$\sum_{k=1}^{6} a_k b_k \left(a_k^3 - b_k^3\right) = 0, \sum_{k=1}^{6} a_k^2 b_k^2 (a_k - b_k) = 0,$$

то по теореме Осипяна [4] из частного решения нормальной системы диофантовых уравнений можно получить двухпараметрическое (a, b – параметры) решение этой системы в гауссовых числах:

$$\begin{gathered}(aa_1 + bb_1 i)^5 + (aa_2 + bb_2 i)^5 + (aa_3 + bb_3 i)^5 + \\ + (aa_4 + bb_4 i)^5 + (aa_5 + bb_5 i)^5 + (aa_6 + bb_6 i)^5 = \\ = (ab_1 + ba_1 i)^5 + (ab_2 + ba_2 i)^5 + (ab_3 + ba_3 i)^5 + \\ + (ab_4 + ba_4 i)^5 + (ab_5 + ba_5 i)^5 + (ab_6 + ba_6 i)^5.\end{gathered} \tag{3}$$

Таким образом, для разработки АДК мы будем использовать двухпараметрическое решение (3) нормальной системы диофантовых уравнений 5-й степени размерности шесть и наборы частных решений (2) этой системы, которые удовлетворяют вышеприведенным 4-м условиям.

Определим модель произвольной алфавитной криптосистемы в виде следующего кортежа [9–13], предложенного автором [14]:

$$\sum_0 = \langle M^*, \ Q, \ C^*, \ E(m), D(c) | \ V(E(m), D(c)) \rangle,$$

где M^*– множество всех сообщений $m = m_1 m_2 \dots m_k$ (открытых текстов) над буквенным или числовым алфавитом M, $m_1, m_2, \dots, m_k$ – это элементарные сообщения (в частности, буквы или конкатенация букв из алфавита М), на которые разбивается открытый текст m;

Q – множество всех числовых эквивалентов элементарных сообщений m_i;

C^*– множество всех криптотекстов $c = c_1 c_2 \dots c_r$ над алфавитом C;

$E(m)$ – алгоритм прямого преобразования открытого текста m;

$D(c)$ – алгоритм обратного преобразования шифртекста c;

$V(E(m), D(c))$ – связь однозначности между алгоритмами $E(m)$ и $D(c)$: это означает, что каждому элементарному сообщению m соответствует единственный криптотекст c, и наоборот.

Протокол разработки математической модели АДК.

- Выбор алфавита сообщений открытого текста.
- Установление числовых эквивалентов элементарных сообщений и триграмм.
- Выбор частного решения нормальной системы диофантовых уравнений 5-й степени размерности шесть.
- Построение двухпараметрического решения этой системы в гауссовых числах.
- Выбор функций прямого и обратного преобразования и секретного ключа.

Для разработки АДК мы используем алфавит *M*, состоящий из 26 заглавных букв английского языка, а также пробела (в общем случае *M* – алфавит мощности *u,* где *u,* в частности, может являться основанием числовой системы, например, 27-м):

$$M = \{A, B, \dots, Z, \_\}.$$

Далее, определим множество числовых эквивалентов как $Q = \{0,1, \dots 26\}$, где каждой букве алфавита *M* сопоставляется числовой эквивалент от 0 до 25 соответственно, пробелу – 26.

Разбиваем открытый текст $m = m_1 m_2 \dots m_k$ на группы из r букв (так называемые - граммы, обозначаемыми через s_i): в нашем случае $r = 3$. Если последняя группа состоит из одной или двух букв, то к ней добавляется один или два пробела соответственно.

Числовой эквивалент нового элементарного сообщения s_i – триграммы рассчитываем по следующий формуле:

$$q_i(s_i) = q_1 u^2 + q_2 u + q_3 = (q_1 q_2 q_3)_{27}, \quad (4)$$

т.е. как число в 27-м системе счисления, где q_1, q_2, q_3 – соответствующие числовые эквиваленты букв из множества Q, u – основание числовой системы, равное 27 – мощности алфавита *M*.

Используя (3), определим функцию прямого преобразования $E(m)$ для числового эквивалента элементарного сообщения s_i, равное a, в криптотекст c путем переноса слагаемых левой части в правую, кроме одного любого.

Например, так:

$$\begin{gathered} E(s_i) = (aa_1 + bb_1 i)^5 + (aa_2 + bb_2 i)^5 + (aa_3 + bb_3 i)^5 + \\ + (aa_4 + bb_4 i)^5 + (aa_5 + bb_5 i)^5 + (aa_6 + bb_6 i)^5 - \\ -(ab_2 + ba_2 i)^5 - (ab_3 + ba_3 i)^5 - (ab_4 + ba_4 i)^5 - \\ -(ab_5 + ba_5 i)^5 - (ab_6 + ba_6 i)^5 = c. \end{gathered} \quad (5)$$

Тогда функция обратного преобразования $D(c)$ криптотекста c в a соответственно будет иметь вид:

$$D(c) = (ab_1 + ba_1 i)^5 = m \quad (6)$$

$$\Rightarrow a = (\sqrt[5]{m} - a_1 bi)/b_1.$$

Теперь выберём одно частное решение нормальной системы диофантовых уравнений 5-й степени размерности шесть и соответствующее двухпараметрическое решение этой системы в гауссовых числах. Особо отметим, что это частное решение (2) является частью закрытого ключа, т.к. при различных $a_1, \dots, a_6, b_1, \dots, b_6$ получаются разные функции шифрования и дешифрования. Значения b и u также являются частью закрытого ключа K: b и u следуют выбирать достаточно большими числами и некоторым особом способом.

Таким образом, имеем функции криптографических преобразований (5) и (6) и закрытый ключ $K = (u, b, a_1, \dots a_6, b_1, \dots b_6)$.

Для получения криптотекста c вычисляем численный эквивалент a триграммы s_i по формуле (4) – к полученному численному эквиваленту триграммы a применяем (5) с секретным ключом K. В итоге получаем криптотекст c. Применяя к шифртексту c функцию (6) с секретным ключом K получаем численный эквивалент a триграммы s_i. Для получения элементарных сообщений, т.е. букв, необходимо из a получить численные эквиваленты букв q_1, q_2, q_3 по следующему алгоритму [5]:

1) $p = 3$;
2) пока $p > 1$;
3) $a \; mod \; u = q_p$;
4) $a = (a - q_p)/u, p = p - 1$, переходим к шагу 1;
5) $q_p = a$.

Полученные числовые эквиваленты букв $q_1, q_2, q_3 \in Q$ необходимо сопоставить с буквами алфавита M и находить зашифрованную триграмму s_i. Описанные действия проделываются для всех триграмм s_i открытого текста m.

Пример разработки АДК. Рассмотрим пример разработки дисимметричной криптосистемы на основе двухпараметрического решения заданной МСДУ.

Пусть для шифрования и дешифрования открытого текста мы выбрали открытый текст m = DIOPHANT, и следующее частное решение нормальной МСДУ пятой степени:

$$2, 3, 4, 6, 7, 8 \overset{5}{=} 3, 6, 2, 8, 4, 7.$$

Можно убедиться, что данное частное решение удовлетворяет всем четырём условиям, приведенным в начале работы. Следовательно, этот набор можем использовать при параметризации решения нормальный системы диофантовых уравнений пятой степени в гауссовых числах:

$$2a + 3bi, 3a + 6bi, 4a + 2bi, 6a + 8bi, 7a + 4bi, 8a + 7bi \overset{5}{=}$$
$$\overset{5}{=} 3a + 2bi, 6a + 3bi, 2a + 4bi, 8a + 6bi, 4a + 7bi, 7a + 8bi.$$

Пусть $u = 27$, а $b = 7$. На практике значения u и b необходимо выбирать, как уже было сказано выше, достаточно большими числами и некоторым особом способом.

Открытый текст m = DIOPHANT предварительно разбиваем на триграммы: DIO, PHA, NT_. Последнее элементарное сообщение состоит из двух букв, поэтому к нему добавляем пробел. Далее, вычислим числовой эквивалент для первой триграммы s_1 = DIO. Так как числовые эквиваленты букв D, I, O равны $q_1 = 3$, $q_2 = 8$ и $q_3 = 14$ соответственно, то получим значение числового эквивалента первой триграммы s_1 = DIO:

$$a = 3 * 27^2 + 8 * 27 + 14 = 2417.$$

Используя функцию прямого преобразования открытого текста (5) и секретный ключ $K = (27, 7, 2, 3, 4, 6, 7, 8, 3, 6, 2, 8, 4, 7)$ мы получим шифртекст числового эквивалента первой триграммы s_1 = *DIO*:

$$(2 * 2417 + 3 * 7 * i)^5 + (3 * 2417 + 6 * 7 * i)^5 +$$
$$+(4 * 2417 + 2 * 7 * i)^5 + (6 * 2417 + 8 * 7 * i)^5 +$$
$$+(7 * 2417 + 4 * 7 * i)^5 + (8 * 2417 + 7 * 7 * i)^5 -$$
$$-(6 * 2417 + 3 * 7 * i)^5 - (2 * 2417 + 4 * 7 * i)^5 -$$
$$-(8 * 2417 + 6 * 7 * i)^5 - (4 * 2417 + 7 * 7 * i)^5 -$$
$$-(7 * 2417 + 8 * 7 * i)^5 =$$
$$= 20043489617808458000 + 193502429678415870i = c_1$$

Полученное целое комплексное число c_1 представляет собой шифртекст первой триграммы s_1 = *DIO*.

Аналогичным образом вычисляются числовые эквиваленты для остальных триграмм: s_2 = PHA, и s_3 = NT_.

Теперь перейдём к процедуре восстановления открытого текста по полученным криптограммам триграмм. Как и выше, рассмотрим эту процедуру только для первой криптограммы. Чтобы из неё получить числовой эквивалент первой триграммы, необходимо к c_1 применить функцию обратного преобразования (6) с секретным ключом K.

Имеем:

$$(3 * a + 2 * 7 * i)^5 = 20043489617808458000 + 193502429678415870i$$

или

$$(20043489617808458000 + 193502429678415870i)^{1/5} = 7251 + 14i.$$

Решаем простое линейное диофантово уравнение в гауссовых числах, и находим a – числовой эквивалент триграммы s_1 = *DIO*. Имеем:

$$3a + 14i = 7251 + 14i, a = 2417.$$

Таким образом, получили числовой эквивалент первой триграммы $a = 2417$. Далее применяем алгоритм извлечения числовых эквивалентов букв q_1, q_2, q_3 из числового эквивалента первой триграммы:

1) $p = 3$;
2) $3 > 1 => 2417\ mod\ 27 = 14 = q_3$;
3) $a = (2417 - 14)/27 = 89, p = 3 - 1 = 2$;
4) $2 > 1 => 89\ mod\ 27 = 8 = q_2$;
5) $a = (89 - 8)/27 = 3, p = 2 - 1 = 1$;
6) $1 \not> 1 => q_1 = 3$.

Получили $q_1 = 3$, $q_2 = 8$ и $q_3 = 14$, что соответствуют буквам D, I и O первой триграммы s_1.

Таким образом, реализация протокола разработки математической модели алфавитно-дисимметричной триграммной криптосистемы позволит повысить криптостойкость существующих криптосистем при безопасной передаче и хранении конфиденциальной информации.

Программная реализация. В рамках данной программной реализации была написана программа на языке Python, которая выполняет следующие задачи.

Генерация секретного ключа K. Включает следующие подзадачи: определение значения u; выбор значения p; определение наборов $A = (a_1, \dots a_6)$ и $B = (b_1, \dots b_6)$).

Подготовка отрытого текста m. Включает следующие подзадачи: разбиение открытого текста на триграммы; сопоставление буквам открытого текста численных эквивалентов из Q; вычисление числового эквивалента каждой триграммы по формуле вычисления числового эквивалента триграммы (4).

Формирование криптотекста c. Включает следующую подзадачу: формирование криптотекста c при помощи функции прямого преобразования (5) для каждой триграммы s_i.

Извлечение открытого текста m *из криптотекста* c. Включает следующие подзадачи: вычисление из c численные эквиваленты триграмм s_i; получение из s_i численные эквиваленты букв q_1, q_2, q_3, содержащихся в триграмме; сопоставление полученных числовых эквивалентов $q_1, q_2, q_3 \in Q$ буквам алфавита M для нахождения m.

Сохранение всех полученных результатов в файлы формата txt. Включает следующие подзадачи: сохранение K в файл; сохранение c в файл; сохранение m в файл.

Главное окно программы представлено на рис. 1:

Рис. 1. Главное окно программы

Ввод и вывод отрытого текста, криптотекста и секретного ключа осуществляется с помощью файлов формата txt. Для генерации K используется кнопка 1. Для получения c загружается m (кнопка 3) и по кнопке 5 происходит преобразование m в c. Полученный c сохраняется в файл. Для извлечения m из c устанавливается соответствующий K (кнопка 2), выбирается c (кнопка 4) и по кнопке 6 происходит дешифрование c, в итоге получаем m. Полученный m сохраняется в файл. Окна 7-10 служат для вывода служебной информации (расположение файлов, подсказки, ошибки и т. д.).

Файл с полученным криптотекстом представлен на рис. 2.

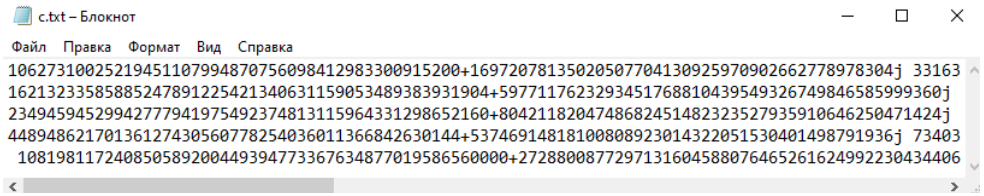

Рис. 2. Криптотекст

Логично использовать данную программную реализацию в качестве криптографического блока других программных продуктов, в которых стоит необходимость обеспечения защиты конфиденциальных данных. Данная программная реализация является учебной версией, которая демонстрирует работу описываемой криптосистемы на простых числовых данных. Соответственно функционал и интерфейс программы организован с целью продемонстрировать возможности алфавитной дисимметричной триграммной криптосистемы на основе двухпараметрического решения нормальной системы диофантовых уравнений 5-й степени размерности шесть в целых гауссовых числах.

Заключение. Сложность диофантовых уравнений, заключающаяся в поиске целочисленных решений, делает их привлекательными для шифрования данных и создания криптографических протоколов. Ключевым моментом является то, что даже зная структуру уравнения, найти конкретное решение может быть крайне затруднительно, особенно при увеличении числа переменных и степени полиномов.

Таким образом, в работе были представлены математическая модель алфавитной дисимметричной триграммной криптосистемы, на основе двухпараметрического решения нормальной системы диофантовых уравнений 5- й степени размерности шесть в гауссовых числах, и программа для шифрования данных на основе этой криптосистемы. Программа, разработанная средствами языка Python, позволяет пользователям генерировать секретный ключ, загружать файлы для шифрования или дешифрования, производить само шифрование или дешифрование и сохранять результат применения криптоалгоритмов в файл.

Данную программную реализацию криптосистемы можно использовать во многих областях, например, ее можно встроить в платежную систему для обеспечения безопасности конфиденциальных финансовых данных пользователей, онлайн-платежей, интернет-банкинга и так далее. Или, например, для защиты конфиденциальных данных непосредственно на компьютерах или серверах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Shannon C.* Communication theory of secrecy systems // Bell System Techn. J. – 1949. – Vol. 28, No. 4. – P. 656-715.
2. *Осипян В.О., Литвинов К.И., Жук А.С.* Разработка математических моделей систем защиты информации на основе многостепенных систем диофантовых уравнений // Экологический вестник научных центров ЧЭС. – 2019. – Т. 16, № 3. – С. 6-15.
3. *Gloden A.* Mehrgradige Gleichungen. – P. Noordhoff: Groningen, 1944.
4. *Осипян В.О.* Разработка методов построения систем передачи и защиты информации: монография. – Краснодар: Кубан. гос. ун-т, 2004. – 180 с.
5. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел: пер. с англ. – М.: Мир, 1987. – 416 с.

6. *Фурсина Е.С., Осипян В.О.* Математическая модель дисимметричной триграммной криптосистемы на основе параметрического решения системы диофантовых уравнений 5-й степени // Матер. VI Всероссийской научно-практической конференции, молодых ученых. – 2024. – Т. 2. – С. 295-299.
7. *Яглом И.М.* Комплексные числа и их применение в геометрии. – М.: Физматгиз, 1963. – 192 с.
8. *Кузьмин Р.О., Фаддеев Д.К.* Алгебра и арифметика комплексных чисел: пособие для учителей. – М.: Учпедгиз, 1939. – 187 с.
9. *Диксон Л.Е.* История теории чисел. Т. 1. – М.: Челси, Нью-Йорк, 1952. – 486 с.
10. *Матиясевич Ю.В.* Диофантовы множества. – М.: УМН, 1972. – 222 с.
11. *Шестопал М.Г., Дорофеева А.В.* Проблемы Гильберта. – М.: Наука, 1969. – 240 с.
12. *Осипян В.О., Григорян Э.С.* Метод параметризации диофантовых уравнений и математическое моделирование систем защиты данных на их основе // Прикаспийский журнал: управление и высокие технологии. – 2019. – Н. 1. – 218 с.
13. *Левина А.Б.* Моделирование криптосистем. – СПб.: Интермедия, 2016. – 144 с.
14. *Осипян В.О.* Разработка математической модели дисимметричной биграммной криптосистемы на основе параметрического решения многостепенной системы диофантовых уравнений // Инженерный вестник Дона. – 2020. – Н. 6. – URL: ivdon.ru/ru/magazine/archive/n6y2020/6534.
15. *Болибрух А.А.* Проблемы Гильберта (100 лет спустя). – М.: МЦНМОБ, 1999. – 24 с.
16. *Болелов Э.А.* Криптографические методы защиты информации. – М.: МГТУ ГА, 2011. – 80 с.
17. *Саломаа А.* Криптография с открытым ключом. – М.: Мир, 1995. – 318 с.
18. *Смарт Н.* Криптография. – М.: Техносфера, 2005. – 528 с.
19. *Матиясевич Ю.В.* Десятая проблема Гильберта. – М.: Наука, 1993. – 12 с.
20. *Осипян В.О., Осипян К.В.* Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004. – 144 с.
21. *Катц Д., Линдел Й.* Введение в современную криптографию. – Чэпмэн энд Холл: CRC, 2014. – 336 с.

REFERENCES

1. *Shannon C*. Communication theory of secrecy systems, *Bell System Techn. J.*, 1949, Vol. 28, No. 4, pp. 656-715.
2. *Osipyan V.O., Litvinov K.I., Zhuk A.S.* Razrabotka matematicheskikh modeley sistem zashchity informatsii na osnove mnogostepennykh sistem diofantovykh uravneniy [Development of mathematical models of information security systems based on multi-degree systems of Diophantine equations], *Ekologicheskiy vestnik nauchnykh tsentrov ChES* [Ecological Bulletin of Scientific Centers of the Black Sea Economic Cooperation], 2019, Vol. 16, No. 3, pp. 6-15.
3. *Gloden A.* Mehrgradige Gleichungen. P. Noordhoff: Groningen, 1944.
4. *Osipyan V.O.* Razrabotka metodov postroeniya sistem peredachi i zashchity informatsii: monografiya [Development of methods for constructing information transmission and protection systems: monograph]. Krasnodar: Kuban. gos. un-t, 2004, 180 p.
5. *Ayerlend K., Rouzen M.* Klassicheskoe vvedenie v sovremennuyu teoriyu chisel [Classical introduction to modern number theory]: transl. from engl. M.: Mir, 1987, 416 p.
6. *Fursina E.S., Osipyan V.O.* Matematicheskaya model' disimmetrichnoy trigrammnoy kriptosistemy na osnove parametricheskogo resheniya sistemy diofantovykh uravneniy 5-y stepeni [Mathematical model of a dissymmetric trigram cryptosystem based on a parametric solution of a system of Diophantine equations of the 5th degree], *Mater. VI Vserossiyskoy nauchno-prakticheskoy konferentsii, molodykh uchenykh* [Proceedings of the VI All-Russian scientific and practical conference of young scientists], 2024, Vol. 2, pp. 295-299.
7. *Yaglom I.M.* Kompleksnye chisla i ikh primenenie v geometrii [Complex numbers and their application in geometry]. Moscow: Fizmatgiz, 1963, 192 p.
8. *Kuz'min R.O., Faddeev D.K.* Algebra i arifmetika kompleksnykh chisel: posobie dlya uchiteley [Algebra and arithmetic of complex numbers: manual for teachers]. Moscow: Uchpedgiz, 1939, 187 p.
9. *Dikson L.E.* Istoriya teorii chisel [History of number theory]. Vol. 1. Moscow: Chelsi, N'yu-York, 1952, 486 p.
10. *Matiyasevich Yu.V.* Diofantovy mnozhestva [Diophantine sets]. Moscow: UMN, 1972, 222 p.
11. *Shestopal M.G., Dorofeeva A.V.* Problemy Gil'berta [Hilbert's Problems]. Moscow: Nauka, 1969, 240 p.
12. *Osipyan V.O., Grigoryan E.S.* Metod parametrizatsii diofantovykh uravneniy i matematicheskoe modelirovanie sistem zashchity dannykh na ikh osnove [Method of parameterization of Diophantine equations and mathematical modeling of data protection systems based on them], *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2019, N. 1, 218 p.

13. *Levina A.B.* Modelirovanie kriptosistem [Modeling of cryptosystems]. Saint Petersburg: Intermediya, 2016, 144 p.
14. *Osipyan V.O.* Razrabotka matematicheskoy modeli disimmetrichnoy bigrammnoy kriptosistemy na osnove parametricheskogo resheniya mnogostepennoy sistemy diofantovykh uravneniy [Development of a mathematical model of a dissymmetric bigram cryptosystem based on a parametric solution of a multi-degree system of Diophantine equations], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2020, N. 6. Available at: ivdon.ru/ru/magazine/archive/n6y2020/6534.
15. *Bolibrukh A.A.* Problemy Gil'berta (100 let spustya) [Hilbert's problems (100 years later)]. Moscow: MTsNMOB, 1999, 24 p.
16. *Bolelov E.A.* Kriptograficheskie metody zashchity informatsii [Cryptographic methods of information protection]. Moscow: MGTU GA, 2011, 80 p.
17. *Salomaa A.* Kriptografiya s otkrytym klyuchom [Public-key cryptography]. Moscow: Mir, 1995, 318 p.
18. *Smart N.* Kriptografiya [Cryptography]. Moscow: Tekhnosfera, 2005, 528 p.
19. *Matiyasevich Yu.V.* Desyataya problema Gil'berta [Hilbert's tenth problem]. Moscow: Nauka, 1993, 12 p.
20. *Osipyan V.O., Osipyan K.V.* Kriptografiya v zadachakh i uprazhneniyakh [Cryptography in tasks and exercises]. Moscow: Gelios ARV, 2004, 144 p.
21. *Katts D., Lindel Y.* Vvedenie v sovremennuyu kriptografiyu [Introduction to modern cryptography]. Chepmen end Kholl: CRC, 2014, 336 p.

Осипян Валерий Осипович – Кубанский государственный университет; e-mail: v.osippyan@gmail.com; г. Краснодар, Россия; кафедра анализа данных и искусственного интеллекта; д.ф.-м.н.; доцент.

Фурсина Елизавета Сергеевна – ООО "БСР"; e-mail: lizafursina@gmail.com; г. Краснодар, Россия; программист 1С.

Альгариб Эман Талиб – Кубанский государственный университет; e-mail: emanalghareeb38@gmail.com; г. Краснодар, Россия; кафедра анализа данных и искусственного интеллекта; аспирант.

Osipyan Valeriy Osipovich – Kuban State University; e-mail: v.osippyan@gmail.com; Krasnodar, Russia; the Department of Data Analysis and Artificial Intelligence; dr. of phys. and math. sc.; associate professor.

Fursina Elizaveta Sergeevna – Limited Liability Partnerships "BSR"; e-mail: lizafursina@gmail.com; Krasnodar, Russia; 1C programmer.

Alghareeb Eman Talib – Kuban State University; e-mail: emanalghareeb38@gmail.com; Krasnodar, Russia; the Department of Data Analysis and Artificial Intelligence; graduate student.

УДК 004.056.55 DOI 10.18522/2311-3103-2025-3-99-110

К.С. Романенко, Е.А. Ищукова, Н.Б. Ельчанинова

ШИФРОВАНИЕ ДАННЫХ В СЭД НА ОСНОВЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ

Рассмотрены вопросы хранения конфиденциальных и персональных данных в системах электронного документооборота. Рассмотрена возможность хранения конфиденциальных и персональных данных в системах электронного документооборота на основе блокчейн технологий. Одной из ключевых характеристик блокчейна является открытость данных. Все транзакции, внесенные в блокчейн, видны всем участникам сети. Это может стать серьезной проблемой при хранении чувствительных данных, таких как личная информация, банковские реквизиты или медицинская история. В связи с этим возникает неизбежный вопрос о безопасном хранении личных данных, поскольку блокчейн-платформа является открытой. Для скрытия информации применяются различные методы, включая гомоморфное шифрование, ZK-SNARK (доказательства с нулевым разглашением), специализированные аппаратные дополнения и другие способы. Ранее авторами был представлен протокол для хранения конфиденциальных данных в блокчейн системах с использованием гибридного шифрования. В работе уделено внимание применению алгоритмов симметричной криптографии в связке с криптографией на эллиптических кривых, поскольку она широко используется в современных блокчейн-платформах, таких как Bitcoin и Ethereum. Причиной выбора эллиптических кривых являются их высокая криптографическая стойкость при относительно малой длине ключа, эффективность вычислений и низкие требования к ресурсам, что особенно важно для децентрализованных сетей с ограниченными вычислительными возможностями узлов. В статье представлены резуль-