ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УДК 519.72+004

МЕТОД ПАРАМЕТРИЗАЦИИ ДИОФАНТОВЫХ УРАВНЕНИЙ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ДАННЫХ НА ИХ ОСНОВЕ[1]

Статья поступила в редакцию 25.02.2019, в окончательной варианте – 08.03.2019.

Осипян Валерий Осипович, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
доктор физико-математических наук, доцент, ORCID 0000-0001- 6558-7998, e-mail: v.osippyan@gmail. Com
Григорян Эвелина Самвеловна, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
бакалавр, e-mail:EvoGrigoryan@mail.ru

Приведен метод параметризации однородных и других многостепенных диофантовых уравнений второй степени специального вида. На их основе разработаны математические модели симметричных и асимметричных систем защиты информации. Предложен оригинальный гибридный метод (SO-метод) разработки систем защиты информации, обобщающий принцип построения криптосистем с открытым ключом, на основе NP-полной задачи о нестандартном рюкзаке и задачи числовых решений диофантовых уравнений заданной размерности и степени. Числовые эквиваленты элементарных сообщений указанных систем – суть числовые решения заданного диофантова уравнения. Криптоанализ описанных математических моделей демонстрирует потенциал применения диофантовых уравнений для разработки систем защиты информации с высокой степенью надёжностью. В отличие от классических асимметричных криптосистем, данный тип математической модели асимметричной криптосистемы позволяет разделять секрет по заданному алгоритму. В частности, такие модели систем допускают существование множества равновероятных ключей, так как соответствующее диофантово множество заданной размерности состоит из счётного количества числовых элементов.

Ключевые слова: система защиты информации, информационная технология, прямое и обратное преобразование данных, симметричная криптосистема, криптосистема с открытым ключом, многостепенное диофантово уравнение, параметризация диофантова уравнения, диофантовы трудности, математическое моделирование

METHOD OF PARAMETRIZATION OF DIOPHANTINE EQUATIONS AND MATHEMATICAL MODELING OF DATA PROTECTION SYSTEMS ON THEIR BASIS

The article was received by editorial board on 25.02.2019, in the final version – 08.03.2019.

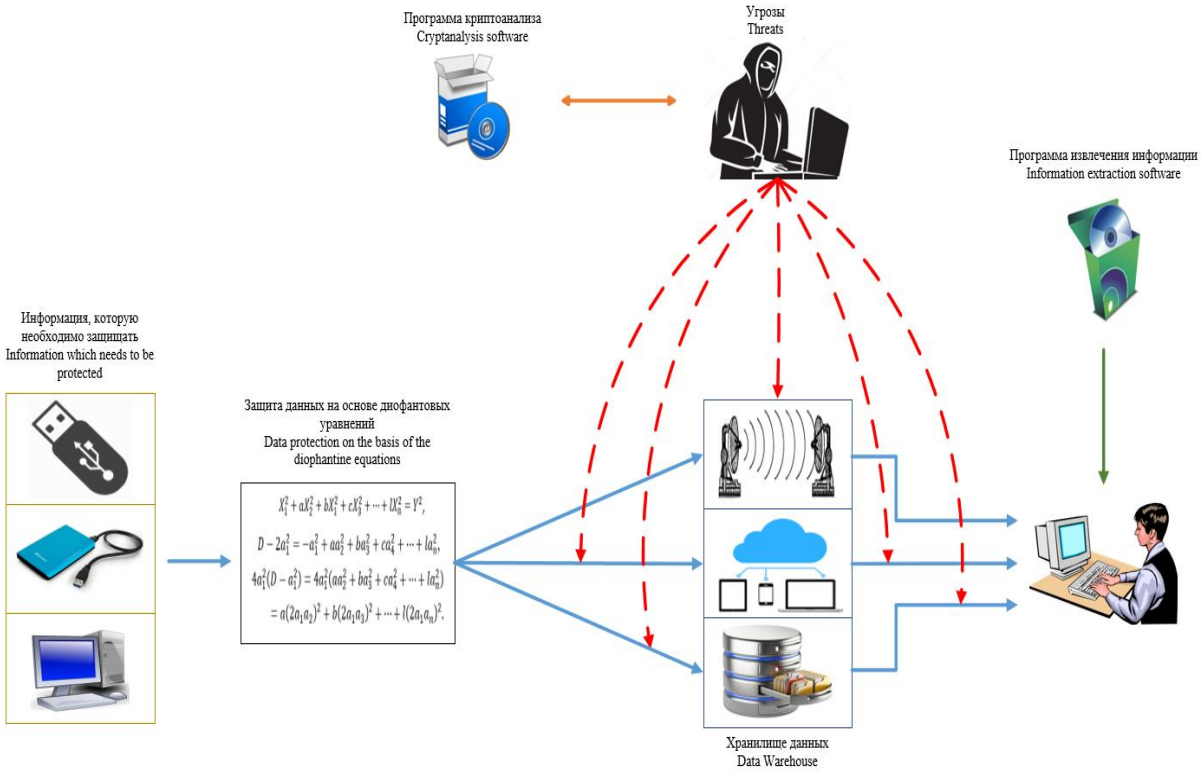
Osipyan Valeriy O., Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
Doct. Sci. (Physics and Mathematics), Associate Professor, ORCID 0000-0001-6558-7998, e-mail: v.osippyan@gmail. Com
Grigoryan Evelina S., Kuban State University, 149 Stavropolskaya St., Krasnodar, 350040, Russian Federation,
bachelor, e-mail: EvoGrigoryan@mail.ru

The method of parametrization of homogeneous and other multi-degree Diophantine equations of the second degree of a special type is given and mathematical models of symmetric and asymmetric information protection systems are developed on their basis. An original hybrid method (SO method) for the development of information protection systems, generalizing the principle of construction of public key cryptosystems, based on NP-complete problem of non-standard backpack and the problem of numerical solutions of Diophantine equations of a given dimension and degree, is proposed. The numerical equivalents of the elementary messages of these systems are the numerical solutions of a given Diophantine equation. Cryptanalysis of the described mathematical models demonstrates the potential of applying Diophantine equations for the development of GIS with a high degree of reliability. Unlike classical asymmetric cryptosystems, this type of mathematical model of asymmetric cryptosystem shares a secret according to a given algorithm. In particular, such models of systems admit the existence of a set of equally probable keys, since the corresponding Diophantine set of a given dimension consists of a countable number of numerical elements.

Key words: information security system, information technology, direct and inverse data transformation, symmetric cryptosystem, public key cryptosystem, multi-degree Diophantine equation, parametrization of Diophantine equation, Diophantine difficulties, mathematical modelling

[1] Работа поддержана грантом РФФИ № 19-01-00596.

Graphical annotation (Графическая аннотация)



Введение. С учетом базовых теоретических положений построения математических моделей эффективных систем защиты информации (СЗИ, криптосистем) мы исходим из необходимости использования для целей защиты сложных математических задач, решение которых потребует от нелегального пользователя большого объема вычислительных ресурсов и работ. К таким задачам, следуя К. Шеннону [26], относятся задачи, содержащие «диофантовы трудности». Их использование препятствует возможности сократить множество перебираемых ключей.

Интенсивное развитие информационно-телекоммуникационных технологий [3] объективно ведет к снижению криптостойкости используемых шифров. Основная идея данной работы состоит в реализации сложной по К. Шеннону криптосистемы защиты информации, содержащей диофантовы трудности, позволяющие смоделировать стойкие системы передачи и защиты информации. Подчеркнем, что К. Шенноном [26] отмечалось, что наибольшей неопределённостью при подборе ключей, обладают СЗИ, содержащие именно диофантовы трудности.

В первой части данной работы приводится метод параметризации однородного многостепенного диофантова уравнения (ДУ) второй степени специального вида, используемые нами при построении математических моделей эффективных СЗИ. Для таких криптосистем передаваемым сообщением является числовое решение заданного диофантова уравнения. Приведены утверждения, которые позволяют описать свойства параметрических решений указанных и других диофантовых уравнений, необходимых для разработки математических моделей СЗИ на их основе.

Во второй части работы приводится авторская математическая модель алфавитной системы защиты данных в виде кортежа; разрабатываются математические модели алфавитных криптосистем защиты информации на основе ДУ второй степени, содержащих диофантовы трудности как для симметричной СЗИ, так и для СЗИ с открытым ключом. В частности, предложены математические модели симметричной биграммной и блочной криптосистем.

Метод параметризации однородного многостепенного диофантова уравнения второй степени. Предварительно приведём некоторые сведения, используемые нами в дальнейшем при построении математической модели СЗИ, содержащей диофантовы трудности.

Как известно [4–6], под ДУ понимают полиномиальное уравнение

$$f(x_1, x_2, \ldots, x_n) = 0, \quad (1)$$

коэффициенты которого суть целые числа, и решение требуется найти тоже в целых или целых неотрицательных числах. Задача решения ДУ типа (1), как правило, заключается в поиске целочисленных решений заданного уравнения или доказательства того, что таких решений нет.

Так, например, ДУ второй степени с одним параметром k (для определённости $k \in N$)

$$X^2 + kY^2 = Z^2$$

обладает следующим общим двупараметрическим решением:

$$X = -a^2 + kb^2,\ Y = 2ab,\ Z = a^2 + kb^2,$$

где a и b – произвольные целые числовые параметры [15].

Ниже мы рассмотрим метод параметризации многостепенного однородного ДУ второй степени специального вида. В монографии Л.Е. Диксона [15 с. 318] приводится (без доказательства) следующее тождество японской исследовательницы Аиды Аммей:

$$(a_1^2 + a_2^2 + \cdots + a_n^2)^2 = (-a_1^2 + a_2^2 + \cdots + a_n^2)^2 + (2a_1a_2)^2 + (2a_1a_3)^2 + \cdots + (2a_1a_n)^2. \quad (2)$$

По утверждению Л.Е. Диксона, это тождество было получено в 1817 г., но опубликовано в Европе лишь в 1897 г., и является обобщением общеизвестного тождества

$$(a_1^2 + a_2^2)^2 = (-a_1^2 + a_2^2)^2 + (2a_1a_2)^2. \quad (3)$$

Если (3) даёт все решения в целых числах уравнения $X^2 + Y^2 = Z^2$, то (2) даёт бесконечное множество решений в целых числах уравнения

$$X_1^2 + X_2^2 + \cdots + X_n^2 = Y^2$$

в виде

$$\begin{cases} X_1 = -a_1^2 + a_2^2 + \cdots + a_n^2, \\ X_r = 2a_1a_r, \quad r = 2,3,\ldots,n, \\ Y = a_1^2 + a_2^2 + \cdots + a_n^2. \end{cases}$$

Рассмотрим следующее многостепенное однородное ДУ второй степени специального вида

$$X_1^2 + aX_2^2 + bX_1^2 + cX_3^2 + \cdots + lX_n^2 = Y^2, \quad (4)$$

где a, b, c, … , l – заданные целые числа. Для получения бесконечного множества целых решений этого уравнения сначала докажем следующее тождество, обобщающее тождество А. Аммей:

$$(a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2)^2 = (-a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2)^2 + (2a_1a_2)^2 + b(2a_1a_3)^2 +$$
$$c(2a_1a_4)^2 + \cdots + l(2a_1a_n)^2. \quad (5)$$

Воспользуемся следующим очевидным тождеством

$$D^2 = (D - 2a_1^2)^2 + 4a_1^2(D - a_1^2).$$

В этом тождестве положим D = $a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2$. Тогда

$$D - 2a_1^2 = -a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2,$$

$$4a_1^2(D - a_1^2) = 4a_1^2(aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2) = a(2a_1a_2)^2 + b(2a_1a_3)^2 + \cdots + l(2a_1a_n)^2.$$

Следовательно, учитывая значения D, $D - 2a_1^2$, $4a_1^2(D - a_1^2)$, получаем тождество (5) и следующее общее параметрическое решение уравнения (4):

$$\begin{cases} X_1 = -a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2, \\ X_r = 2a_1a_r, r = 2,3,\ldots,n, \\ Y = a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2. \end{cases}$$

Из (5) при $a = \mathrm{b} = \mathrm{c} = \cdots = \mathrm{l} = 1$ получается (2).

Согласно тождеству (5), квадрат числа вида

$$a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2$$

всегда можно представить в том же виде. Поэтому мы можем

$$(a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2)^{2^m}$$

представить в виде $A_1^2 + aA_2^2 + bA_3^2 + \cdots + lA_n^2$ и, следовательно, решить в целых числах уравнение

$$A_1^2 + aA_2^2 + bA_3^2 + \cdots + lA_n^2 = Y^{2^m}.$$

Например, для $m = 2$ достаточно возводить в квадрат

$$M = (-a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2)^2 + a(2a_1a_2)^2 + b(2a_1a_3)^2 + c(2a_1a_4)^2 + \cdots + l(2a_1a_n)^2.$$

Тогда пользуясь формулой (5), получаем:

$$M^2 = [-(-a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2)^2 + a(2a_1a_2)^2 + b(2a_1a_3)^2 + c(2a_1a_4)^2 + \cdots + l(2a_1a_n)^2]^2$$
$$+ a(2a_1a_2R)^2 + b(2a_1a_3R)^2 + \cdots + l(2a_1a_nR)^2, \text{где } R = -a_1^2 + aa_2^2 + ba_3^2 + \cdots + la_n^2.$$

Таким образом, бесконечное множество целых решений уравнения

$$X_1^2 + aX_2^2 + bX_3^2 + cX_4^2 + \cdots + lX_n^2 = Y^4$$

получаем по формулам:

$$X_1 = -R^2 + a(2a_1a_2)^2 + b(2a_1a_3)^2 + c(2a_1a_4)^2 + \cdots + l(2a_1a_n)^2,$$

$$X_r = 2a_1a_rR, \qquad r = 2,3,\dots,n, Y = R + 2a_1^2$$

$$R = -a_1^2 + aa_2^2 + ba_3^2 + ca_4^2 + \cdots + la_n^2.$$

В работе Е. Фаукуемберга (“Mathesis”, 2, 3, 1893, с. 235) опубликовано тождество

$$(a_1^2 + a_2^2 + a_3^2 + \cdots + a_i^2 + \cdots + a_n^2)^2 = (a_1^2 + a_2^2 + a_3^2 + \cdots + a_i^2 - a_{i+1}^2 - a_{i+2}^2 \dots - a_n^2)^2 + \sum_{r=1}^{i}\sum_{s=i+1}^{n}(2a_ra_s)^2. \quad (6)$$

Это тождество приводит также Л.Е. Диксон в [15], но без доказательства. Тождество Е. Фаукуемберга доставляет бесконечное множество целых решений уравнения

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 + \cdots + X_k^2 = Y^2, k = 1 + i(n - i)$$

в виде:

$$X_1 = a_1^2 + a_2^2 + a_3^2 + \cdots + a_i^2 - a_{i+1}^2 - a_{i+2}^2 - \cdots - a_n^2,$$

$$X_2 = 2a_1a_{i+1},$$

$$X_3 = 2a_2a_{i+1},$$

. . .

$$X_k = 2a_ia_n.$$

Заметим, что тождество (6) является частным случаем следующего более общего тождества:

$$(a_1^2 + a_2^2 + a_3^2 + \cdots + aa_{i+1}^2 + ba_{i+2}^2 + \cdots + la_n^2)^2 = (a_1^2 + a_2^2 + a_3^2 + \cdots + a_i^2 - aa_{i+1}^2 - ba_{i+2}^2 \dots - la_n^2)^2 + a\sum_{r=1}^{i}(2a_{i+1}a_r)^2 + b\sum_{r=1}^{i}(2a_{i+2}a_r)^2 + \cdots + l\sum_{r=1}^{i}(2a_na_r)^2. \quad (7)$$

Докажем тождество (7). Пусть

$$Q = a_1^2 + a_2^2 + a_3^2 + \cdots + a_i^2,$$

$$P = aa_{i+1}^2 + ba_{i+2}^2 + \cdots + la_n^2.$$

Тогда из тождества $(Q + P)^2 = (Q - P)^2 + 4PQ$

имеем:

$$(Q + P)^2 = (Q - P)^2 + (a_1^2 + a_2^2 + a_3^2 + \cdots + a_i^2)[a(2a_{i+1})^2 + b(2a_{i+2})^2 + \cdots + l(2a_n)^2] = (Q - P)^2 + a\sum_{r=1}^{i}(2a_{i+1}a_r)^2 + b\sum_{r=1}^{i}(2a_{i+2}a_r)^2 + \cdots + l\sum_{r=1}^{i}(2a_na_r)^2,$$

откуда и получаем тождество (7). При $a = b = \cdots = l = 1$ из (7) следует (6).

Тождество (7) доставляет бесконечное множество целых решений ДУ (8):

$$X_1^2 + a(X_2^2 + X_3^2 + \cdots + X_{i+1}^2) + b(X_{i+2}^2 + X_{i+3}^2 + \cdots + X_{2i+1}^2) + \cdots + l(X_{k-i}^2 + X_{k-i+1}^2 + \cdots + X_k^2) = Y^2 \quad (8)$$

в виде:

$$X_1 = a_1^2 + a_2^2 + a_3^2 + \cdots + a_i^2 - aa_{i+1}^2 - ba_{i+2}^2 \dots - la_n^2$$

$$X_2 = 2a_1a_{i+1},$$

$$X_3 = 2a_2a_{i+1},$$

. . .

$$X_k = 2a_ia_n,$$

$$Y = a_1^2 + a_2^2 + a_3^2 + \cdots + aa_{i+1}^2 + ba_{i+2}^2 + \cdots + la_n^2,$$

где $a_1, a_2, a_3, \dots, a_n$ – произвольные целые числа.

Математическая модель алфавитной систем защиты информации. Как известно, математическая модель алфавитной криптосистемы, разработанная автором [6], представляется в виде следующего кортежа:

$$\sum_0 = \langle \mathbf{M}^*, \mathbf{Q}, \mathbf{C}^*, \mathbf{E(m)}, \mathbf{D(c)} \,|\, \mathbf{V(E(m), D(c))} \rangle, \quad (9)$$

где $\mathbf{M}^*$ – множество всех сообщений $\mathbf{m} = \mathbf{m_1}\ \mathbf{m_2} \ldots \mathbf{m_k}$ (открытых текстов) над буквенным или числовым алфавитом **M**;

$\mathbf{m_i}$, $\mathbf{i = 1 \ldots k}$ – элементарные сообщения (в частности, буквы или конкатенации букв из алфавита **M**);

Q – множество всех числовых эквивалентов элементарных сообщений $\mathbf{m_i}$ из $\mathbf{M}^*$;

$\mathbf{C}^*$ – множество всех шифртекстов (криптограмм) $\mathbf{c} = \mathbf{c_1}\ \mathbf{c_2} \ldots \mathbf{c_k}$ над алфавитом **C**, в частности, возможно **M = Q = C**;

E(m) – алгоритм прямого преобразования (шифрования) сообщения **m** в **c**;

D(c) – алгоритм обратного преобразования (дешифрования) шифртекста (криптограммы) **c** в $\mathbf{m} \in \mathbf{M}^*$.

Подчеркнем, что алгоритмы **E(m)** и **D(c)** алфавитной криптосистемы (9) связаны между собой таким образом – **V(E(m), D(c))**, что всегда произвольное сообщение $\mathbf{m} = \mathbf{m_1}\ \mathbf{m_2} \ldots \mathbf{m_k} \in \mathbf{M}^*$ однозначно преобразовывается в соответствующую криптограмму (шифртекст) $\mathbf{c} = \mathbf{c_1}\ \mathbf{c_2} \ldots \mathbf{c_k} \in \mathbf{C}^*$ и обратно. Поэтому по криптограмме **c** всегда однозначно восстанавливается переданное сообщение **m**.

Альтернативным обозначением алгоритмов **E(m)** и **D(c)** для алфавитной криптосистемы (9) является $\mathbf{K_E}$ (или $\mathbf{F_E}$) и $\mathbf{K_D}$ (или $\mathbf{F_D}$) соответственно, как принято считать в классической криптографии [1, 5–7, 9, 15, 22–25]. Мы их назовём иначе ключами (или функциями) шифрования и дешифрования соответственно. Автор не претендует на полноту освещения аналогичных математических моделей алфавитных криптосистем (9). Единственная его цель – формально описать произвольную криптосистему.

Математическая модель симметричной биграммной криптосистемы, содержащей диофантовы трудности. Рассмотрим математическую модель систем защиты данных на основе труднорешаемой задачи нахождения корней ДУ вида (1), для которого алгоритмы *E(m)* и *D(c)* прямого и обратного преобразований строятся на основе решений указанного уравнения. Для наглядности в качестве первого примера рассмотрим ДУ второй степени (10) с коэффициентом k ($k \in$ N) при Y^2

$$X^2 + kY^2 = Z^2, \tag{10}$$

и его следующий класс решений над натуральными числами N в виде:

$$X = -a^2 + kb^2,\ Y = 2ab,\ Z = a^2 + kb^2,\ b > a,$$

где a и b – произвольные натуральные числа (в более общем случае можно рассмотреть его решения над Z или Q).

Рассмотрим математическую модель алфавитной симметричной криптосистемы с проверкой на модификацию сообщения *m,* содержащей диофантовы трудности. Пусть элементами открытого и закрытого текстов являются отдельные заглавные буквы английского 26-буквенного алфавита от A до Z с соответствующими числовыми эквивалентами последовательно от 0 до 25 (если m – элементарное сообщение, то её числовой эквивалент обозначим как q). Очевидно, в общем случае в качестве числовых эквивалентов можно взять некоторую случайную числовую последовательность.

В данном пункте рассмотрим криптосистему, элементарные сообщения которой суть биграммы 27-буквеного алфавита, состоящего из букв A–Z и пробела (с числовым эквивалентом 26 – следующего за эквивалентом для Z), а в качестве числового эквивалента для биграммы $m_i m_{i+1}$, состоящей из двух букв m_i и m_{i+1} с эквивалентами $q_i,\ q_{i+1} \in \{0, 1, \ldots, 26\}$, возьмём целое число

$$27q_i + q_{i+1} \in \{0, 1, \ldots, 728\}.$$

Так, например, биграмме *DI* соответствует целое число 27*3 + 8 = 89.

Примем следующие обозначения:

$$C_L(a, b, v) = (-a^2 + kb^2)^2 + (2ab)^2 + v \tag{11}$$

– функция прямого преобразования биграмм: преобразованная левая часть уравнения (10), v – секретный ключ; $C(m_i m_{i+1})$ – шифр биграммы $m_i m_{i+1}$ (предварительно исходное сообщение m разбиваем на биграммы с добавлением пробела, если m содержит нечётное число элементарных сообщений);

$$C_R(a, b, v) = (a^2 + kb^2)^2 - v \tag{12}$$

– модифицированная правая часть уравнения (10), которая является функцией обратного преобразования.

Заметим, что для практических приложений можно установить «лазейку» v для легального пользователя таким образом, чтобы криптостойкость указанной СЗИ зависела только от выбора ключа v в соответствии с принципом Керкгоффса [1].

Пример 1. Итак, пусть исходное ДУ имеет вид:

$$X^2 + 13Y^2 = Z^2$$

и

$$M = \{A, B, C, \ldots, Y, Z\}$$

– алфавит заглавных букв английского алфавита со множеством числовых эквивалентов элементарных сообщений Q. Пусть сообщение m имеет вид:

$$m = DIOPHANT$$

с числовыми эквивалентными букв, представленных в таблице. Определим, например, открытый ключ v как числовой эквивалент для биграммы $m_i m_{i+1}$.

Таблица – Числовые эквиваленты некоторых английских заглавных букв, соответствующих их порядковым номерам в латинском алфавите

m_i	D	I	O	P	H	A	N	T
q_i	3	8	14	15	7	0	13	19

Так, например, шифр первой биграммы $m_1m_2 = DI$ сообщения m определяем на основе формулы (11) как числовое значение

$$C_L(a, b) = (-a^2 + 13b^2)^2 + 13(2ab)^2 + 27a + b$$

при $a = 3, b = 8$, т.е.

$$C(m_1m_2) = C(DI) = C_L(3, 8) = 707370.$$

Перед нелегальным пользователем стоит трудно вычислимая задача – представить шифр $C_L(3, 8) = 707370$ в виде суммы слагаемых вида (11) с параметрами a, b и установить значения числовых эквивалентов букв D и I, т.е. решить уравнение

$$(-a^2 + 13b^2)^2 + 13(2ab)^2 + 27a + b = 707370.$$

Алгоритм определения тех же значений a, b для легального пользователя сводится на основе (12) к следующему алгоритму:

– $v = 1$, пока $C_R(a, b) - v$ не есть полный квадрат $v = v + 1$;

– после того как $C_R(a, b) - v$ станет полным квадратом, вычислить $t = sqrt(C_R(a, b) - v)$;

– найти a и b из ДУ $C_R(a, b) = t$.

В рассмотренном примере при $v = 89$ имеем следующий полный квадрат:

$$C_R(a, b) = (a^2+13b^2)^2 = 707281 = 841^2,$$

$$a^2+13b^2 = 841$$

или

$$x + 13y = 841.$$

Отсюда находим $x = 9, y = 64$. Следовательно, $a = 3, b = 8$ (как решение последнего ДУ) и биграмму $m_1m_2 = DI$ – как переданное сообщение.

Аналогично поступаем и для других биграмм сообщения m.

Построение математической модели асимметричной криптосистемы на основе уравнения (10) производится на основе механизма, рассмотренного в работе автора [6, с. 158]. При этом алгоритмы $E(m)$ и $D(c)$ определяются аналогичным образом.

Математическая модель блочной криптосистемы, содержащей диофантовы трудности. В предыдущем пункте мы рассмотрели математическую модель симметричной биграммной криптосистемы на основе ДУ второй степени

$$X^2 + kY^2 = Z,^2 k \in \mathrm{N}$$

со следующим общим параметрическим решением:

$$X = -a^2 + kb^2,\ Y = 2ab,\ Z = a^2 + kb^2,\ b > a,$$

где a и b – произвольные натуральные числа.

Аналогично можно реализовать алгоритм построения математической модели криптосистемы блочной структуры, исходя из параметрического решения однородного многостепенного диофантова уравнения второй степени (13):

$$X_1^2 + a_2 X_2^2 + a_3 X_3^2 + \ldots + a_n X_n^2 = Y^2, \qquad (13)$$

со следующим общим параметрическим ($t_1, t_2, \ldots, t_n$ – числовые параметры) решением:

$$X_1 = -t^2_1 + a_2 t^2_2 + a_3 t^2_3 + \ldots + a_n t^2_n,$$

$$X_r = 2t_1 t_r,\ r = 2 \ldots n,$$

$$Y = t^2_1 + a_2 t^2_2 + a_3 t^2_3 + \ldots + a_n t^2_n,$$

где $a_2, a_3, \ldots, a_n$ – произвольные целые числа.

Рассмотрим гибридный метод (SO-метод) разработки СЗИ, обобщающий принцип построения криптосистем с открытым ключом, на основе NP-полной задачи о нестандартном рюкзаке и задачи числовых решений однородного диофантова уравнения второй степени вида (13).

В силу произвольности коэффициентов $a_2, a_3, \ldots, a_n$ сопоставим коэффициентам исходного уравнения (13) сверхрастущий обобщенный рюкзачный вектор $A_p = (a_1, a_2, \ldots, a_n)$ размерности n, $n \geq 3$ с пороговым значением p. Этот вектор состоит из n различных натуральных компонентов a_i, $i = 2. \ . n$ с первым членом $a_1 = 1$. Очевидно, что если рюкзачный вектор p-сверхрастущий, то он инъективен и одновременно возрастающий. Более подробные сведения относительно соответствующих рюкзачных СЗИ и механизма разработки математической модели блочной структуры можно найти в работах авторов [1, 5–8, 21, 23, 24]. Приведём здесь лишь схему и функции прямого и обратного преобразований такой криптосистемы.

Определим для заданного i, $1 \leq i \leq n$ функцию прямого преобразования как:

$$C^i_L(X_1, X_2, \ldots, X_i) = X_1^2 + a_2 X_2^2 + a_3 X_3^2 + \ldots + a_i X_i^2,$$

а функцию обратного преобразования в виде:

$$C^{i+1}_R(X_{i+1}, X_{i+2}, \ldots, X_n, Y) = Y^2 - a_{i+1}X_{i+1}^2 - a_{i+2} X_{i+2}^2 - a_{i+3} X_{i+3}^2 - \ldots - a_n X_n^2.$$

Отметим, в частности, при $i = n$ функция обратного преобразования определяется только правой частью уравнения (13), поэтому мы положим

$$C^{i+1}{}_R(X_{i+1}, X_{i+2}, \ldots, X_n, Y) = C^n{}_R(Y).$$

Как следует из определений функций $C^i{}_L(X_1, X_2, \ldots, X_i)$ и $C^{i+1}{}_R(X_{i+1}, X_{i+2}, \ldots, X_n, Y)$, они дополняют друг друга и их можно рассмотреть как функции нового класса. В отличие от классических асимметричных криптосистем, данный тип математической модели асимметричной криптосистемы позволяет разделять секрет по заданному алгоритму.

Рассмотрим пример ДУ и соответствующие им функции прямого и обратного преобразований.

Так, например, для размерности $n = 5$ и порогового значения $p = 3$ определим обобщенный рюкзачный вектор A_3 как [5]:

$$A_3 = (1, 7, 17, 51, 305),$$

с соответствующим ДУ (13):

$$X_1^2 + 7X_2^2 + 17X_3^2 + 51X_4^2 + 305X_5^2 = У^2, \tag{14}$$

и следующим общим параметрическим решением:

$$X_1 = -t^2{}_1 + 7t^2{}_2 + 17t^2{}_3 + 51t^2{}_4 + 305t^2{}_5,$$
$$X_r = 2t_1 t_r,\ r = 2 \ldots 5,$$
$$Y = t^2{}_1 + 7t^2{}_2 + 17t^2{}_3 + 51t^2{}_4 + 305t^2{}_5,$$

где $t_1, t_2, \ldots, t_5$ – числовые параметры.

Далее для заданного i, например, $i = 5$, аналогично функциям (11, 12), определим функцию прямого преобразования с секретным ключом v как:

$$C^5{}_L(X_1, X_2, X_3, X_4, X_5) = X_1^2 + 7X_2^2 + 17X_3^2 + 51X_4^2 + 305\,X_5^2 + v, \tag{15}$$

а функцию обратного преобразования в виде:

$$C^5{}_R(Y) = У^2 - v. \tag{16}$$

Отметим, что алгоритмы разработок математических моделей криптосистем (симметричной и и с открытым ключом) на основе ДУ (14) ничем не отличаются от соответствующих алгоритмов, приведённых в примере 1. При этом, очевидно, вычислительные затраты у легального и нелегального пользователей не соизмеримы по величине.

Так, для заданного шифра c нелегальному пользователю необходимо решить ДУ (15) второй степени общего вида

$$X_1^2 + 7X_2^2 + 17X_3^2 + 51X_4^2 + 305\,X_5^2 + v = c$$

или в развёрнутом виде уравнение

$$-t^2{}_1 + 7t^2{}_2 + 17t^2{}_3 + 51t^2{}_4 + 305t^2{}_5 + 14t_1 t_2 + 34t_1 t_3 + 102t_1 t_4 + 610t_1 t_5 + v = c,$$

а легальному – уравнение (16)

$$t^2{}_1 + 7t^2{}_2 + 17t^2{}_3 + 51t^2{}_4 + 305t^2{}_5 - v = c,$$

которое сводится к ДУ первой степени и решается одним из указанных в [6] способов.

Таким образом, криптоаналитик, помимо прочих качеств, должен обладать ещё умением решать ДУ заранее заданной степени и сложности. Отметим также, что рассматриваемые примеры являются лишь демонстрацией идеи приложения ДУ в области криптографии. Также очевидно, что указанные модели криптосистем далеки от практического применения, так как многие аспекты прикладной криптографии здесь опущены ради реализации идеи К. Шеннона [26].

В заключение отметим, что приведённая методика построения математических моделей криптосистем с помощью SO-метода позволяет разрабатывать эффективные модели СЗИ для практических приложений на основе параметрических решений ДУ более высоких степеней, что является предметом дальнейшего исследования.

Библиографический список

1. Алферов А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – 2-е изд., испр. и доп. – Москва : Гелиос АРВ, 2002. – 480 с.

2. Виноградов И. М. Основы теории чисел / И. М. Виноградов. – Изд. 9-е, перераб. – Москва : Наука, 1981. – 176 с.

3. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – Москва : Кудиц-Образ, 2001. – 363 с.

4. Матиясевич Ю. В. Диофантовы множества / Ю. В. Матиясевич // Успехи математических наук. – 1972. – Т. 27, вып. 5. – С. 185–222.

5. Осипян В. О. Моделирование систем защиты информации содержащих диофантовы трудности. Разработка методов решений многостепенных систем диофантовых уравнений. Разработка нестандартных рюкзачных криптосистем / В. О. Осипян. – LAMBERT Academic Publishing, 2012. – 344 с.

6. Осипян В. О. Математическое моделирование систем защиты данных на основе диофантовых уравнений / В. О. Осипян // Прикаспийский журнал: управление и высокие технологии. – 2018. – № 1 (41). – С. 151–160.

7. Осипян В. О. Моделирование ранцевых криптосистем, содержащих диофантовую трудность / В. О. Осипян, С. Г. Спирина, А. С. Арутюнян, н В. В. Подколзи// Чебышевский сборник. – 2010.Т. 11, вып. 1. – С. 209–217.

8. Саломаа А. Криптография с открытым ключом / А. Саломаа. – Москва : Мир, 1995. – 318 с.

9. Серпинский В. О решении уравнений в целых числах / В. Серпинский ; пер. с польск. К. Г. Мельникова. – Москва : Физматлит, 1961. – 88 с.

10. Серпинский В. 100 Простых, но одновременно и трудных вопросов арифметики / В. Серпинский. – Москва : Учпедгиз, 1961. – 76 с.

11. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си : пер. с англ. / Б. Шнайер. – Москва : Триумф, 2002. – 816 с.

12. Cassels J. W. S. On a Diophantine Equation / J. W. S. Cassels // Acta Arithmetica. – 1960. – Vol. 6. – P. 47–52.

13. Carmichael R. D. The Theory of Numbers and Diophantine Analysis / R. D. Carmichael. – New York, 1959. – 118 p.

14. Chor B. A knapsack-type public key cryptoystem based on arithmetic in finite fields / B. Chor, R. Rivest // IEEE Transactions on Information Theory. – 1988. – Vol. IT-34. – P. 901–909.

15. Dickson L. E. History of the Theory of Numbers / L. E. Dickson. – New York, 1971. – Vol. 2. Diophantine Analysis.

16. Gloden A. Mehgradige Gleichungen / A. Gloden. – Groningen, 1944. – P. 104.

17. Gurari E. M. An NP-complete number theoretic problem / E. M. Gurari, O. H. Ibarra // Proc. 10th Ann. ACM. Symp. On Theory of computing. – New York, 1978. – P. 205–215.

18. Koblitz N. A Course in Number Theory and Cryptography / N. Koblitz. – New York : Springer-Verlag, 1987. – 235 p.

19. Lenstra A. K. Factoring polynomials with rational coefficients / A. K. Lenstra, H. W. Lenstra, L. Lovasz // Mathematische annalen. – 1982. – Vol. 261. – P. 515–534.

20. Lin C. H. A new public-key cipher system based upon the diophantine equations / C. H. Lin, C. C. Chang, R. C. T. Lee // IEEE Transactions on Computers. – 1995, Jan. – Vol. 44, issue 1.

21. Merkle R. Hiding information and signatures in trapdoor knapsacks / R. Merkle, M. Hellman // IEEE Transactions on Information Theory. – 1978. – Vol. IT-24. – P. 525–530.

22. Mordell L. J. Diophantine equations / L. J. Mordell. – London – New York : Acad. Press, 1969. – 312 p.

23. Osipyan V. O. Buiding of alphabetic data protection cryptosystems on the base of equal power knapsacks with Diophantine problems / V. O. Osipyan // Sinconf 2012 – 5th International Conference on Security of Information and Networks. – Jaipur : ACM, 2012. – P. 124–129.

24. Osipyan V. O. Mathematical modelling of cryptosystems based on Diophantine problem with gamma superposition method / V. O. Osipyan // SIN'15 Proceedings of the 8th International Conference on Security of Information and Networks. – Sochi : ACM, 2015. – P. 338–341.

25. Sierpinski W. Elementary Theory of Numbers / W. Sierpinski. – Warszawa : Hafner Publishing Company, 1964. – 480 p.

26. Shannon C. Communication theory of secrecy systems / C. Shannon // Bell System Techn. J. – 1949. – Vol. 28, № 4. – P. 656–715.

References

1. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. *Osnovy kriptografii* [Bases of cryptography]. 2nd ed. Moscow, Gelios ARV Publ., 2002. 480 p.

2. Vinogradov. I. M. *Osnovy teorii chisel* [Fundamentals of Number Theory]. 9nd ed. Moscow, Nauka Publ., 1981, 176 p.

3. Ivanov M. A. *Kriptograficheskiye metody zashchity informatsii v kompyuternykh sistemakh i setyakh* [Cryptographic methods of information security in computer systems and networks]. Moscow, Kudits-Obraz Publ., 2001, 363 p.

4. Matiyasevich, Yu. B. Diofantovy mnozhestva [Diophantine sets]. *Uspekhi matematicheskikh nauk* [Successes of Mathematical Sciences], 1972, vol. 27, no. 5, pp. 185–222.

5. Osipyan V. O. Modelirovaniye sistem zashchity informatsii soderzhashchikh diofantovy trudnosti. Razrabotka metodov resheniy mnogostepennykh sistem diofantovykh uravneniy. Razrabotka nestandartnykh ryukzachnykh kriptosistem: monografiya [Modeling of systems of protection of information containing the Diophantine difficulties. Development of methods for solving multi-stage systems of Diophantine equations. Development of non-standard knapsack cryptosystems]. LAMBERT Academic Publishing, 2012, 344 p.

6. Osipyan V. O. Matematicheskoe modelirovanie sistem zashchity dannykh na osnove diofantovykh uravneniy [Mathematical modeling of a data protection system based on Diophantine equations]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2018, no. 1 (41), pp. 151–160.

7. Osipyan V. O., Spirina S. G., Arutyunyan A. S., Podkolzin V. V. Modelirovaniye rantsevykh kriptosistem, soderzhashchikh diofantovuyu trudnosti [Simulation of knapsack cryptosystems containing Diophantine difficulty]. *Chebyshevskiy sbornik* [Chebyshev collection], 2010, vol. 11, no. 1, pp. 209–216.

8. Salomaa A. *Kriptografiya s otkrytym klyuchom* [Cryptography with a public key]. Moscow, Mir Publ., 1995, 318 p.

9. Serpinsky W. *O reshenii uravneniy v tselykh chislakh* [On solving equations in integers]. Moscow, Fizmatlit Publ., 1961, 88 p.

10. Serpinsky W. *100 prostykh, no odnovremenno i trudnykh voprosov ariphmetiky* [100 simple, but at the same time difficult questions of arithmetic]. Moscow, Uchpedgiz Publ., 1961, 76 p.

11. Schneier B. *Prikladnaya kriptografiya: Protokoly, algoritmy, iskhodnye teksty na yazyke Si* [Applied cryptography: Protocols, algorithms, source texts in C]. Moscow, Triumph Publ., 2002, 816 p.

12. Cassels J. W. S. On the Diophantine equation. *Acta Arithmetica*, 1960, vol. 6, pp. 47–52.

13. Carmichael R. D. *Theory of numbers and Diophantine Analysis*. New York, 1959. 118 p.

14. Chor B., Rivest R. A knapsack-Type public key cryptoystem based on arithmetic in finite fields of trades. *IEEE on information theory*, 1988, vol. IT-34, pp. 901–909.

15. Dickson L. E. *History of the Theory of Numbers*. New York, 1971, vol. 2: Diophantine Analysis.

16. Gloden A. *Mehgradige Gleichungen*. Groningen, 1944, p. 104.

17. Gurari E. M., Ibarra O. H. An NP-complete number theoretic problem. *Proc. 10th Ann. ACM. Symp. On Theory of computing*, New York, 1978, pp. 205–215.

18. Koblitz N. A Course in Number Theory and Cryptography. New York, Springer-Verlag Publ., 1987. 235 p.

19. Lenstra A. K., Lenstra H. W., Lovasz L. Factoring polynomials with rational coefficients. *Mathematische annalen*, 1982, vol. 261, pp. 515–534.

20. Lin C. H., Chang C. C., Lee R. C. T. A new public-key cipher system based upon the diophantine equations. *IEEE Transactions on Computers*, 1995, Jan., vol. 44, issue 1.

21. Merkle R., Hellman M. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, 1978, vol. IT-24, pp. 525–530.

22. Mordell L. J. *Diophantine equations*. London, New York, Acad. Press, 1969, 312 p.

23. Osipyan V. O. Buiding of alphabetic data protection cryptosystems on the base of equal power knapsacks with Diophantine problems. *Sinconf 2012 – 5th International Conference on Security of Information and Networks*. Jaipur, ACM Publ., 2012, pp. 124–129.

24. Osipyan V. O. Mathematical modelling of cryptosystems based on Diophantine problem with gamma superposition method. *SIN'15 Proceedings of the 8th International Conference on Security of Information and Networks*. Sochi, ACM Publ., 2015, pp. 338–341.

25. Sierpinski W. *Elementary Theory of Numbers*. Warszawa, Hafner Publ. Company, 1964. 480 p.

26. Shannon C. Communication theory of secrecy systems. *Bell System Techn. J.*, 1949, vol. 28, no. 4, pp. 656–715.

УДК 004.056.53

МОДЕЛЬ И ПРОЕКТНЫЕ ДИАГРАММЫ СИСТЕМЫ ЦЕНТРАЛИЗОВАННОЙ ЗАЩИТЫ ПОДСЕТИ ХОСТОВ ПОД УПРАВЛЕНИЕМ UNIX-ПОДОБНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Статья поступила в редакцию 06.03.2019, в окончательном варианте – 05.04.2019.

Горкавенко Владимир Сергеевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, Татищева, 20а,

магистрант, e-mail: slipmetal@mail.ru

Ажмухамедов Искандар Маратович, Россия, г. Астрахань, Татищева, 20а, Астраханский государственный университет,

доктор технических наук, профессор, заведующий кафедрой информационной безопасности, e-mail: iskander_agm@mail.ru

Рассмотрено одно из возможных решений задачи защиты от несанкционированного доступа рабочих станций под управлением unix-подобных операционных систем, находящихся в одной подсети, посредством разработки централизованной системы устранения уязвимостей, позволяющей повысить уровень защищенности. Приведена формализация задачи. Предложено реализовать пять основных этапов, которые будет включать в себя алгоритм поиска и применения решения для устранения диагностированной уязвимости на рабочей станции. Согласно предложенному алгоритму, рабочая станция передает на сервер текст, содержащий информацию о диагностированной уязвимости, затем сервер, согласно информации, полученной от рабочей станции, инициирует поиск решения в базе знаний. Если решение найдено, то сервер передает его на рабочую станцию. Если решение не найдено, тогда централизованная система устранения уязвимостей уведомляет об этом лицо, принимающее решение. После передачи найденного решения для устранения диагностированной уязвимости, сервер инициирует его применение на рабочей станции. Во время применения решений для устранения диагностированных уязвимостей, рабочая станция передает на сервер информацию о процессе их применения. Если они по какой-либо причине не были реализованы, централизованная система устранения уязвимостей уведомляет лицо, принимающее решение о том, что уязвимости не были устранены. Предложено логическое представление централизованной системы устранения уязвимостей, а также диаграмма вариантов использования с описанием взаимодействия внутренних модулей и сервисов. Рассмотрено также одно из возможных решений задачи обеспечения защищенного соединения между рабочей станцией и сервером.

Ключевые слова: операционная система, несанкционированный доступ, информационная безопасность, централизованная защита, unix, linux, ubuntu