Список литературы

1. Жарких Л. И. Генератор *z*-матриц молекул. Свидетельство о регистрации программы для ЭВМ № 2015616182 от 2 июня 2015 г. / Л. И. Жарких, А. С. Дегтярев.
2. Жарких Л. И. Автоматизация расчетов основных энергетических и зарядовых характеристик при моделировании межмолекулярных взаимодействий. Свидетельство о регистрации программы для ЭВМ № 2011611798 от 28.02.2011 г. / Л. И. Жарких, Ю. А. Очередко, Н. М. Алыков, А. А. Малев.
3. Степанов Н. Ф. Квантовая механика и квантовая химия / Н. Ф. Степанов. – Москва : Мир, 2001. –519 с.
4. Фирсов Н. Н. Микробиология: словарь терминов / Н. Н. Фирсов. – Москва : Дрофа, 2006. – 256 с.
5. Элькин М. Д. Молекулярное моделирование: методические аспекты / М. Д. Элькин, Г. П. Стефанова, И. А. Крутова, В. И. Коломин // Прикаспийский журнал: управление и высокие технологии. – 2012. – № 4. – С. 103–112 (http://hi-tech.asu.edu.ru/files/4(20)/103-112.pdf).
6. ChemCraft. – Режим доступа: http://www.chemcraftprog.com, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 14.04.2018).
7. MOPAC. – Режим доступа: http://old.psu.ru/science/soft/winmopac, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 14.04.2018).
8. Schmidt M. W. The General Atomic and Molecular Electronic Structure System / M. W. Schmidt, K. K. Baldridge, J. A. Boatz, S. T. Elbert et al. // J. Comput. Chem. – 1993. – Vol. 14. – P. 1347–1363.
9. Shewchuk Jonathan Richard. Second order gradients methods / Shewchuk Jonathan Richard // School of Computer Science. – Carnegie Mellon University Pittsburg, 1994. – Vol. 7. – P. 155–163.
10. Stewart J. J. P. Optimization of Parameters for Semiempirical Methods / J. J. P. Stewart // J. Comput. Chem. – 1989. – Vol. 10, № 2. – P. 209–220.

References

1. Zharkix L. I., Degtyarev A. S. *Generator z-matricz molekul* [Generator of z-matrices of molecules]. Svidetel`stvo o registracii programmy` dlya E`VM №2015616182 ot 2 iyunya 2015 g. [Certificate of registration of the computer program no. 2015616182 dated June 2, 2015].
2. Zharkix L. I., Ocheredko Yu. A., Aly`kov N. M., Malev A. A. *Avtomatizaciya raschetov osnovny`kh e`nergeticheskikh i zaryadovy`kh kharakteristik pri modelirovanii mezhmolekulyarny`kh vzaimodejstvij* [Automation of calculations of the main energy and charge characteristics in the modeling of intermolecular interactions] Svidetel`stvo o registratsii programmy` dlya E`VM №2011611798 ot 28.02.2011g. [Certificate of registration of the computer program no. 2011611798 from 28.02.2011]
3. Stepanov N. F. *Kvantovaya mekhanika i kvantovaya khimiya [*Quantum mechanics and quantum chemistry]. Moscow, Mir Publ., 2001. 519 p.
4. Firsov N. N. *Mikrobiologiya: slovar` terminov* [Microbiology: a glossary of terms]. Moscow, Drofa Publ., 2006. 256 p.
5. E`l`kin M. D., Stefanova G. P., Krutova I. A., Kolomin V. I. Molekulyarnoe modelirovanie: metodicheskie aspekty` [Molecule modelling: methodical aspects]. *Prikaspijskij zhurnal: upravlenie i vy`sokie tekhnologii* [Caspian Journal: Control and High Technologies], 2012, no. 4, pp. 103–112 (http://hi-tech.asu.edu.ru/files/4(20)/103-112.pdf).
6. *ChemCraft*. Available at: http://www.chemcraftprog.com (accessed: 14.04.2018).
7. *MOPAC*. Available at: http://old.psu.ru/science/soft/winmopac (accessed: 14.04.2018).
8. Schmidt M. W., Baldridge K. K., Boatz J. A., Elbert S. T. et al. The General Atomic and Molecular Electronic Structure System . *J. Comput. Chem.*, 1993, vol. 14, pp. 1347–1363.
9. Shewchuk Jonathan Richard. Second order gradients methods. *School of Computer Science*. Carnegie Mellon University Pittsburg, 1994, vol. 7, pp. 155–163.
10. Stewart J. J. P. Optimization of Parameters for Semiempirical Methods. *J. Comput. Chem.*, 1989, vol. 10, no. 2, pp. 209–220.

УДК 519.72

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ДИОФАНТОВЫХ УРАВНЕНИЙ

Статья поступила в редакцию 27.03.2018, в окончательном варианте – 12.06.2018.

Осипян Валерий Осипович, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,

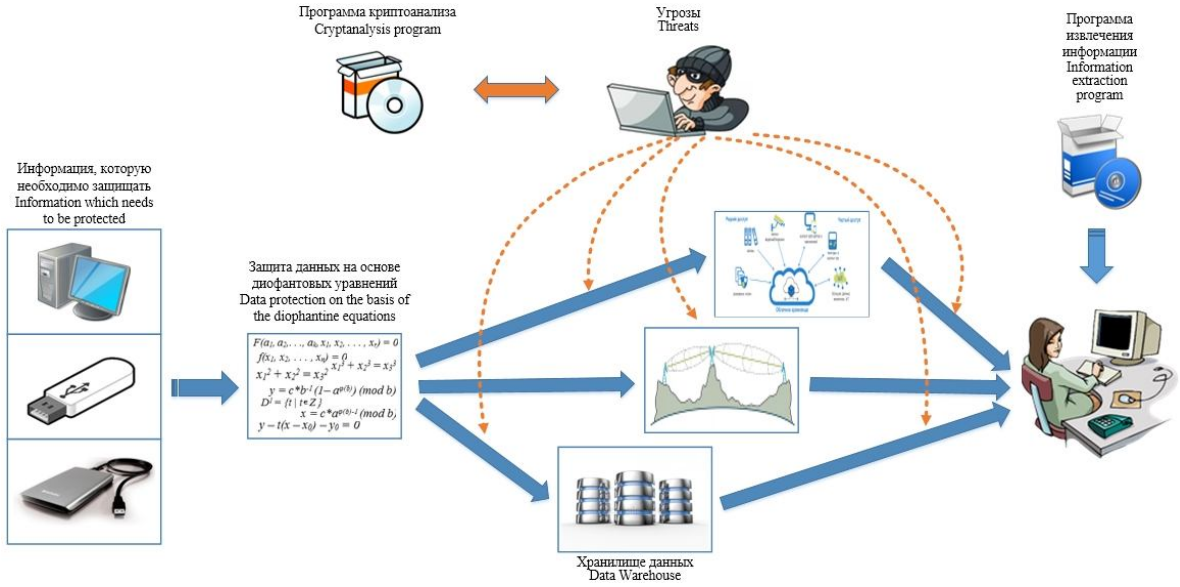
доктор физико-математических наук, доцент, ORCID 0000-0001-6558-7998, e-mail: v.osippyan@gmail. com

Показана объективная необходимость совершенствования систем защиты информации в условиях развития информационно-телекоммуникационных технологий. Представлены математические модели систем защиты информации, разработанные на основе линейного неоднородного и квадратного однородного диофантова уравнений. Исходным сообщением служит некоторое решение заданного диофантова уравнений, а шифртекстом – его правая часть. Изучается задача нахождения диофантова представления заданного множества с целыми числовыми компонентами. Приведены теоремы, которые позволяют описать свойства параметрических решений диофантова уравнений, необходимых для

разработки математических моделей систем защиты информации на их основе. Криптоанализ описанных математических моделей, несмотря на имеющиеся уязвимости, демонстрирует потенциал применения ДУ для разработки систем защиты информации с высокой степенью надёжностью. В частности, такие модели позволяют строить как симметричные систем защиты информации, так и системы с открытом ключом. Такие системы допускают существование множества равновероятных ключей, так как соответствующее диофантово множество заданной размерности состоит из счётного количества числовых элементов.

Ключевые слова: системы защиты информации, информационные технологии, шифрование информации, симметричная криптосистема, криптосистема с открытым ключом, линейное диофантово уравнение, диофантовы трудности, диофантово множество

Графическая аннотация (Graphical annotation)



MATHEMATICAL MODELING OF THE DATA PROTECTION SYSTEMS BASED ON DIOPHANTINE EQUATIONS

The article was received by editorial board on 27.03.2018; in its final version – 12.06.2018.

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

The objective need for improving data protection systems in conditions of information and telecommunication technologies development is showed. Mathematical models of the DPS developed on the basis of linear inhomogeneous and square homogeneous Diophantine equations are presented. A solution to the given Diophantine equations serves as the original message and the ciphertext is its right part. The problem of finding the Diophantine representation of the given set with the entire numerical components. The authors present the theorems, which let describe the characteristics of the Diophantine equations parameter solutions, necessary for data protection systems mathematical models development on their basis. The cryptanalysis of the described mathematical models, despite their vulnerability, demonstrates the potential of applying Diophantine equations for the development of data protection systems with a high degree of reliability. In particular, such models allow to build both symmetrical data protection systems and systems with an open key. Such systems admit the existence of numerous equi-probable keys, as the corresponding Diophantine set of a given dimension consists of enumerable quantity of numeric elements.

Keywords: data protection systems, information technologies, information encryption, symmetric cryptosystem, cryptosystem with an open key, linear Diophantine equation, Diophantine compilations, Diophantine set

Введение. Интенсивное развитие информационно-телекоммуникационных технологий объективно ведет к снижению криптостойкости используемых шифров, применяемых в системах защиты информации (СЗИ, криптосистем). При этом термин «криптостойкость» мы понимаем как время, необходимое для взлома шифра в автоматическом или полуавтоматическом режиме. Основные причины следующие: увеличение мощностей вычислительных машин, включая скорости выполнения операций; развитие суперком-

пьютеров (оно позволяет распараллелить вычисления и, тем самым, сократить общее время перебора вариантов); совершенствование традиционных и перспективных алгоритмов криптоанализа; использование в системах криптоанализа элементов «искусственного интеллекта», позволяющих оптимизировать процесс подбора оптимальных алгоритмов и пр. Поэтому актуальна разработка новых алгоритмов криптозащиты, основанных на использовании сложных математических задач, решение которых потребует от нелегального пользователя (НП) большого объема вычислительной работы. К таким задачам, в соответствии с работами К. Шеннона [26], относятся задачи, содержащие «диофантовы трудности». Их использование препятствует возможностям для НП сократить множество перебираемых ключей.

Основная идея данной работы состоит в реализации сложной, по К. Шеннону, криптосистемы защиты информации, содержащей диофантовы трудности. Это позволяет смоделировать стойкие системы передачи и защиты информации (К. Шенноном отмечалось, что наибольшей неопределённостью при подборе ключей, обладают СЗИ, содержащие диофантовы трудности).

В первой части работы приведены основные понятия, факты и определения из теории диофантова анализа [2, 9–11], используемые нами при построении математических моделей (ММ) эффективных СЗИ. Для таких криптосистем передаваемым сообщением является некоторое решение заданного диофантова уравнения (ДУ), а шифртекстом – свободный член этого уравнения. Приведены теоремы, которые позволяют описать свойства параметрических решений ДУ, необходимых для разработки математических моделей СЗИ на их основе.

Приводится авторская ММ алфавитной системы защиты данных в виде кортежа; разрабатываются ММ алфавитных криптосистем защиты информации на основе ДУ первой и второй степеней, содержащих диофантовы трудности (для двух типов СЗИ – симметричной и с открытым ключом).

Основные понятия, определения и факты из диофантова анализа. Предварительно приведём некоторые факты, используемые нами в дальнейшем при построении ММ СЗИ, содержащей диофантовы трудности.

Как известно [9–11, 13, 23], под диофантовым уравнением понимают полиномиальное уравнение

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

коэффициенты которого суть целые числа, и решения требуется найти тоже в целых или целых неотрицательных числах. Задача решения ДУ вида (1), как правило, заключается в поиске целочисленных решений заданного уравнения или доказательстве того, что таких решений нет. Так, например, ДУ второй степени с тремя неизвестными

$$x_1^2 + x_2^2 = x_3^2$$

обладает общим двупараметрическим решением вида:

$$x_1 = a^2 - b^2,\ x_2 = 2ab,\ x_3 = a^2 + b^2,$$

где a и b – параметры, а уравнение

$$x_1^3 + x_2^3 = x_3^3$$

– нет.

Наряду с отдельными ДУ вида (1) часто рассматривают семейства диофантовых уравнений вида [4]

$$F(a_1, a_2, \ldots, a_k, x_1, x_2, \ldots, x_r) = 0, \quad (2)$$

зависящие от k параметров $a_1, a_2, \ldots, a_k$ и r неизвестных переменных $x_1, x_2, \ldots, x_r$ так, что $k + r = n$. Каждое такое семейство определяет некоторое множество D^k упорядоченных наборов из k чисел – множество тех целых значений параметров$a_1, a_2, \ldots, a_k$, при которых уравнение (2) разрешимо относительно неизвестных переменных $x_1, x_2, \ldots, x_r$ (иногда – в целых неотрицательных числах):

$$D^k = \{(a_1, a_2, \ldots, a_k) \mid F(a_1, a_2, \ldots, a_k, x_1, x_2, \ldots, x_r) = 0\}. \quad (3)$$

Такое множество (3) называют диофантовым; число k называют его размерностью, а соответствующее уравнение (2) – его диофантовым представлением [4]. Другими словами, множество, имеющее диофантово представление, будем называть диофантовым.

Например, уравнение $13a + 6x = 14$ является диофантовым представлением и оно содержит один параметр a, одно неизвестное x. Это ДУ имеет следующее общее параметрическое решение:

$$a = 2 - 6t,\ x = -2 + 13t,\ t \in Z.$$

Здесь имеем соответственно следующее диофантово счётно-бесконечное множество размерности один:

$$D^1 = \{2 - 6t \mid t \in Z\} = \{\ldots 26, 20, 14, 8, 2, -4, -10, -16, -22, -28, \ldots\}$$

– множество тех значений параметра t, при которых исходное уравнение разрешимо относительно неизвестного x. Очевидно, что данное диофантово множество D^1 состоит из бесконечного числа элементов. Причём если $t \le 0$, то мы имеем следующие натуральные решения:

$$D^1 = \{2, 8, 14, 20, 26, \ldots\}$$

– элементы которого образуют арифметическую прогрессию с первым членом $a_1 = 2$ и разностью прогрессии $d = 6$.

В простейших случаях диофантовость множества очевидна. Например, диофантовым является множество всех чётных (нечетных) чисел, так как они удовлетворяют ДУ $t_1 = 2x$ ($t_1 = 2x+1$). В этом случае множество

$$D^1 = \{t_1 = 2x\ (t_1 = 2x+1)\ | x \in Z\}$$

размерности один имеет диофантово представление или, что то же самое:

$$D^1 = Z_0 = \{a|2x=a\},\ D^1 = Z_1 = \{a|2x+1=a\}.$$

В общем случае, часто достаточно сложно ответить на такие естественные вопросы [4]: диофантово ли множество всех простых чисел, чисел Фибоначчи; диофантово ли множество всех совершенных чисел или других множеств.

Так, например, для ДУ

$$t_1 + 5x_1 = 101$$

с одним параметром t_1 и одним неизвестным x_1 имеем следующее счётное диофантово множество

$$D^1 = \{101–5x_1 \mid x_1 \in Z\}$$

– множество тех значений параметра t_1, при которых оно разрешимо относительно неизвестного x_1. В частности, оно содержит следующие элементы:

$$46, 66, 36, 71, 31$$

и, соответствующие значения для неизвестного x_1**:**

$$11, 7, 13, 6, 14,$$

то есть следующие пары:

$$(101–5x_1, x_1),\ x_1 \in Z.$$

Возвращаясь к предыдущему уравнению

$$13x + 6y = 14,$$

приведём следующую его параметризацию:

$$x = 2 – 6t,\ y = – 2 +13t,\ t \in Z,$$

и – соответствующее диофантово множество:

$$D^1 = \{t \mid t \in Z\},\ S = \{(2 – 6t, – 2 +13t) \mid t \in Z\}.$$

Отметим, что отдельные численные решения приведенных ДУ в целых (или целых положительных) числах можно получить, например, с использованием средства «Поиск решения», имеющегося в Microsoft Excel. Такой подход позволяет эффективно определить факт отсутствия решения у анализируемого ДУ. Однако гарантированно обеспечить нахождение всех решений (из числа имеющихся). Такой подход обычно не позволяет – даже при использовании нескольких вариантов с различными начальными приближениями. Вопрос о том, можно ли использовать средство «Поиск решения» для выявления решений ДУ в параметрической форме, нуждается в отдельном обсуждении.

Рассмотрим теперь следующую обратную задачу относительно десятой проблемы Д. Гильберта [4].

Обратная задача о разрешимости диофантова уравнения. Имеется некоторое множество целых числовых значений и требуется узнать, является ли оно диофантовым. Другими словами, можно ли найти диофантово представление заданного множества с целыми числовыми компонентами.

Для простоты изложения рассмотрим случай одного решения: необходимо построить такое ДУ, среди решений которого содержится заранее заданное значение.

Так, например, единственный элемент одноэлементного множества $D^2 = \{(3, 5)\}$ является одним из множества решений ДУ

$$3x + 5y = c,$$

где c – некоторый параметр.

В самом деле, из общего решения $x = 2c – 5r,\ y = 3r – c$ при $r = 13,\ c = 34$ получаем следующее частное решение (3, 5), принадлежащее D^2. Является диофантовым также множество D^2 размерности два, состоящее из следующих пар целых числовых значений:

$$D^2 = \{(0, 6), (1, 19), (2, 32), (3, 45), (4, 58), (5, 71), (6, 84)\}.$$

Очевидно, здесь уравнение $13x – y + 6 = 0$ содержит указанное множество значений D^2, следовательно, оно диофантово.

В общем случае, если $D^2 = \{(x_0, y_0)\}$, то соответствующее уравнение можно задать, например, с помощью следующего ДУ:

$$y – t(x – x_0) – y_0 = 0,$$

где t – параметр, а x и y переменные величины.

В силу её важности, приведём следующую известную теорему относительно решений линейного ДУ [9–14].

Теорема 1. Если c не делится на $d = (a, b)$, являющегося наибольшим общим делителем чисел a и b, то ДУ

$$ax + by = c$$

не разрешимо в целых числах.

Если же c делится на $d = (a, b)$, то оно разрешимо в целых числах. Причём если (x_0, y_0) – одно частное решение этого уравнения, то все его решения находятся по формулам:

$$x = x_0 + t*b/d,\ y = y_0 – t*a/d,\ t \in Z.$$

Известны различные методы решения такого уравнения, в частности, с помощью функции Эйлера $\varphi(n)$ – в виде:

$$x = c*a^{\varphi(b)-1} (mod\ b),$$
$$y = c*b^{-1} (1 - a^{\varphi(b)}) (mod\ b).$$

Следствие. Аналогично решается линейное ДУ от n неизвестных переменных:

$$a_1x_1 + a_1x_1 + \ldots + a_1x_1 = c. \quad (4)$$

Теорема 2. Если $d = (a, b) = 1$, то одним из корней ДУ

$$a\,x + b\,y = c$$

является (a, b), где $c = a^2 + b^2$.

Доказательство. В самом деле, на основании теоремы Евклида имеем: всегда найдутся целые числа x_0 и y_0 такие, что $ax_0 + by_0 = 1$. Отсюда при $x_0 = a$ и $y_0 = b$ следует утверждение теоремы $ax_0 + by_0 = a^2 + b^2$.

Так, например, уравнение $7x + 13y = 170$ имеет своим решением
$x_0 = 7, y_0 = 11$.

В более общем случае можно доказать следующую теорему.

Теорема 3. Непустое множество

$$S = \{ax + by | a, b, x, y \in NU\{0\}\} \neq \varnothing$$

– множество натуральных чисел вида $ax + by$, где a и b параметры, а x, y переменные величины, является счётным множеством мощности $\aleph$ (алеф-нуль: мощность множества всех натуральных чисел).

Так, например, множество натуральных чисел вида $7x + 13y$ мощности $\aleph$ состоит из

$$S = \{7, 13, 14, 20, 21, 26, 27, 28, 33, \ldots, 90, 93, 100, \ldots\}.$$

Здесь в качестве базиса или генераторами являются $e_1 = 7, e_2 = 13$. Следовательно, уравнение

$$7x + 13y = s_0 \in S$$

имеет единственное натуральное решение для любого $s_0 \in S$ и не имеет решений – в противном случае.

В качестве практического приложения, рассмотрим демонстрационную задачу определения числа и месяца рождения конкретного человека (например, автора данной статьи), зашифрованных с помощью ДУ. При этом естественными ограничениями являются следующие: число в месяце – от 1 до 31; номер месяца – от 1 до 12.

Задача. Определить день d и месяц m рождения автора данной статьи, если известно, что

$$31d + 12m = 413. \quad (5)$$

Данную задачу можно применить для любого w **(**в нашем случае $w = 413$**),** рассмотрев ДУ

$$31d + 12m = w, \quad (6)$$

со следующими ограничениями относительно d: $1 \le d \le 31$; m: $1 \le m \le 12$; w: $43 \le w \le 1105$ (при минимальных и максимальных значений d и m соответственно).

Очевидно, общее параметрическое решение уравнения (6) имеет вид:

$$d = -5w + 12t,$$
$$m = 13w - 31t.$$

Тогда для $w = 413$ определим целые значения параметра t, при которых выполняется уравнение (6).

Имеем:

$d = -5*413 + 12*t = -2065 + 12*t > 0$, откуда $t > 172$.
$m = 13*413 - 31*t = 5369 - 31*t > 0$, откуда $t <= 173$,

Таким образом, получаем $t = 173$. Следовательно,

$$d = -2065 + 12*173 = 11,$$
$$m = 5369 - 31*173 = 6.$$

Следовательно, искомое решение соответствует $d = 11$ (т.е. числу в месяце) и $m = 6$ (т.е. месяцу июнь).

Ниже мы рассмотрим математически модели СЗИ, взяв за основу эту простую идею.

Разработка математических моделей алфавитных СЗИ на основе диофантовых уравнений. Символически ММ модель алфавитной системы защиты информации, разработанную автором, представляется в виде следующего кортежа:

$$\sum_0 = \left\langle M^*, Q, C^*, E(m), D(c) \,|\, V(E(m), D(c)) \right\rangle, \quad (8)$$

где M^* – множество всех сообщений $m = m_1m_2 \ldots m_k$ (текстов) над буквенным или числовым алфавитом M. Здесь $m_i, i = 1 \ldots k$ – элементарные сообщения (в частности, буквы или конкатенация букв из алфавита M); Q – множество всех числовых эквивалентов элементарных сообщений m_i из M^*; C^* – множество всех текстов $c = c_1c_2 \ldots c_k$ над алфавитом C, полученных на основе алгоритма $E(m)$ – прямого преобразования сообщения m в c; $D(c)$ – алгоритм обратного преобразования текста c в $m \in M^*$.

Подчеркнем, что алгоритмы $E(m)$ и $D(c)$ алфавитной СЗИ (8) связаны между собой таким образом – $V(E(m), D(c))$, что всегда произвольное сообщение $m = m_1m_2 \ldots m_k \in M^*$ однозначно преобразовыва-

ется в соответствующий текст $c = c_1c_2 \ldots c_k \in C^*$ и, обратно: по c всегда можно однозначно восстановить переданное сообщение m.

Альтернативным обозначением алгоритмов $E(m)$ и $D(c)$для алфавитной системы (8) являются K_E (или F_E) и K_D (или F_D) соответственно – как принято считать в классической литературе по СЗИ [1, 3, 8, 19]. Мы иначе назовём их ключами (или функциями) прямого преобразования и обратного преобразования соответственно. С учетом ограниченности объема статьи ММ, аналогичные (8), и алфавитные СЗИ рассматриваются лишь фрагментарно.

Прежде всего, заметим, что прямое преобразование открытого текста m, состоящего из одного элементарного сообщения m_1 или представляющего конкатенацию сообщений m_1m_2, осуществляется путем равномерного увеличения длины ключа этого преобразования. Так, например, пусть в качестве элементарного сообщения выступает одна буква m_1 с числовым эквивалентом c_1, длины n. Тогда конкатенации m_1m_2 будет соответствовать числовой эквивалент c_1c_2 – длины $2n$, имеющий блоковую структуру.

Математическая модель СЗИ на основе задачи об обобщенном рюкзаке. Как известно [5–8,12,15,19, 22], в основе всех стандартных рюкзачных СЗИ (РСЗИ) лежит *NP*-полная задача [18, 21] об укладке рюкзака или ранца K_S. Криптостойкость таких СЗИ зависит от первоначального способа кодирования самих букв и процедуры дальнейшего прямого преобразования открытого текста.

Для построения лёгкого подкласса стандартных РСЗИ на основе «сверхрастущего рюкзака» Р. Меркль и М. Хеллман [22] предложили «замаскировать» рюкзак с помощью линейного преобразования последнего посредством сильного модульного умножения.

В протоколе Шора-Ривеста [15], в отличие от протокола Меркля-Хеллмана, рюкзак представляет собой набор логарифмов в мультипликативной группе расширенного поля и обладает повышенной плотностью по сравнению с рюкзаком Меркля-Хеллмана.

После вскрытия с помощью алгоритма полиномиальной сложности Ленстры-Ленстры-Ловаша [20] оригинальной схемы Меркля-Хеллмана многие эксперты стали скептически относиться к криптостойкости таких систем. Одновременно было предложено множество других усложнённых вариантов РСЗИ [19], в частности, рюкзаки Грэм-Шамира, основанные на принципе укладки стандартного рюкзака. Среди них в настоящее время существуют всё ещё не вскрытые РСЗИ [19].

Приведём авторскую формулировку [6] математической модели задачи об обобщенном (нестандартном) рюкзаке K_G, обобщающей известную – стандартную K_S.

Пусть $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$ – обобщенный рюкзачный вектор размерности n, $n \geq 3$ из n различных натуральных компонентов a_i, $i = 1. \ldots n$ и (A, v) – его вход [6], где v также некоторое натуральное число (в частности, нуль). Для простоты изложения будем считать, что значения компонент рюкзачного вектора **A** расположены в возрастающем порядке.

Пусть, далее, $Z_p = \{0, 1, \ldots, p-1\}$ – множество коэффициентов повторений компонент рюкзачного вектора **A** при определении его входа **(A, v)**, где $p = 2$ (стандартный рюкзак) или $p > 2$ (нестандартный, обобщённый рюкзак). Все входы **(A, v)**, для любого допустимого значения v, должны обладать не более чем одним решением – с повторениями или без него. Такие рюкзачные векторы будем называть инъективными.

Рюкзачный вектор $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$ назовём обобщённо сверхвозрастающим p-го порядка, если для любого $j = 2 \ldots n$ имеет место неравенство:

$$a_j > \sum_{k=1}^{J-1} (p-1)\, a_k .$$

Очевидно, если рюкзачный вектор сверхрастущий, то он инъективен и одновременно возрастающий. Соответствующие рюкзачные СЗИ можно найти в работах автора [5–7, 24, 25].

Рассмотрим другое возможное решение относительно входа обобщенного рюкзака K_G на основе указанного выше линейного ДУ (4):

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$$

или

$$A*X = c, \tag{9}$$

где $\mathbf{A} = (\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n})$ – обобщённо сверхвозрастающий вектор коэффициентов p-го порядка этого уравнения, а $\mathbf{X} = (\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n})$ – его решение. Очевидно, из равенства (9) следует равенство

$$A*(w*X) = w*c,$$

где w – любое натуральное число, такое что

$$u*w = 1(\mathrm{mod}m),$$

для некоторого модуля $m > a_n$ и натурального числа u.

Пусть M – произвольный алфавит, например, заглавные буквы английского языка:

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

с множеством числовых эквивалентов элементарных сообщений в виде
p-ичных (например, $p=3$) равномерных блоков:

$$Q = \{1_p, 2_p, \dots, 26_p\}.$$

Для $p = 3$ имеем:

$$Q = \{001, 002, 010, 011, \dots, 222\}.$$

Определим алгоритм прямого преобразования $E(m)$ на основе следующего открытого вектора

$$\mathbf{B} = (b_1, b_2, \dots, b_n),$$

как

$$c = E(m) = B*Q,$$

где $b_i = u*a_i \ (mod\ m)$.

Отметим, что c представляет собой правую часть уравнения (9), а алгоритм обратного преобразования $D(c)$ сообщения c в m имеет вид:

$$m = D(c)*w = A*Q.$$

Выполнение связи $V(E(m), D(c))$ – очевидно.

Так, например, если сообщение m имеет вид: $m = DIOPHANT$ с числовыми эквивалентами, представленными в таблице, то биграмме DI будет соответствовать числовой эквивалент $(0, 1, 1, 1, 0, 0)$.

Пусть секретный вектор порядка $p = 3$ имеет вид:

$$\mathbf{A} = (1, 2, 7, 21, 63, 189),$$

а u и w выберем, например, в виде

$$u = 13, w = 147, m = 191,$$

т.е. так, чтобы выполнялось сравнение:

$$13*147 = 1 \ (mod\ 191).$$

Тогда открытый вектор определим как:

$$\mathbf{B} = (147, 103, 74, 31, 93, 88).$$

Таблица – Числовые эквиваленты некоторых английских заглавных букв.

m_i	D	I	O	P	H	A	N	T
q_i	4	9	15	16	8	1	14	20

Имеем для биграмма DI следующее прямое преобразование:
c= E(m) = B*Q = E(DI) = (147, 103, 74, 31, 93, 88)*(0, 1, 1, 1, 0, 0) = 208 и следующее ДУ, которое должен решить нелегальный пользователь для «вскрытия» зашифрованной информации:

$$147x_1 + 103x_2 + 74x_3 + 31x_4 + 93x_5 + 88x_6 = 208.$$

Для обратного преобразования легальному пользователю необходимо решить ДУ:

$$x_1 + 2x_2 + 7x_3 + 21x_4 + 63x_5 + 189x_6 = 208$$

и получить решение

$$(x_1,x_2,x_3,x_4,x_5,x_6) = (0, 1, 1, 1, 0, 0).$$

В самом деле,
$m = D(c)*w = A*Q = 208*13 \ (mod\ 191) = 30 = 0*1+1*2 + 1*7 + 1*21 + 0*63 +0*189 = (1, 2, 7, 21, 63, 189)*(0, 1, 1, 1, 0, 0)$. Отсюда следует, что было передано биграмма DI. Аналогично поступаем и для других биграмм.

Данная СЗИ более криптостойка по сравнению с СЗИ Меркла-Хеллмана, так как количество всевозможных ключей, которые необходимо будет перебрать в случае, когда неизвестен ключ, равно $N(k) = p^n$. Для СЗИ Меркла-Хеллмана количество всевозможных ключей равно $N(k) = 2^n$, т.е. является в разы меньшей величиной.

Математическая модель алфавитной системы защиты информации, содержащей диофантовы трудности. Рассмотрим ММ асимметричной системы защиты данных на основе трудно решаемой задачи нахождения корней ДУ (1), для которой алгоритмы $E(m)$ и $D(c)$ прямого и обратного преобразований строятся на основе решений указанного уравнения. Здесь, для наглядности и простоты, в качестве примера рассмотрим ДУ

$$x^2 + y^2 = z^2 \qquad (9)$$

второй степени (5) и его следующий класс решений над натуральными числами N в виде:

$$x = a^2 - b^2, y = 2ab, z = a^2 + b^2,$$

где a и b – произвольные натуральные числа (в более общем случае можно рассмотреть его решения над Z или Q [9, 14, 16]).

Рассмотрим ММ алфавитной асимметричной криптосистемы с проверкой на модификацию сообщения m, содержащей диофантовы трудности. Пусть, так же как и выше,

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

– алфавит заглавных букв английского языка с множеством числовых эквивалентов элементарных сообщений Q и сообщение m имеет вид: $m = DIOPHANT$ с числовыми эквивалентами, представленными в таблице.

Примем следующие обозначения:

$$C_L(a, b) =(a^2 – b^2)^2 +(2ab)^2 \quad (10)$$

– функция прямого преобразования биграмм (открытый ключ), являющаяся левой частью уравнения (9); $C(m_im_{i+1})$ – шифр биграммы m_im_{i+1}, например, DI для нашего сообщения m. Предварительно разбиваем сообщение m на биграммы с добавлением пробела, если m содержит нечётное число элементарных сообщений, в частности, букв.

$$C_R(a, b) = (a^2+b^2)^2$$

– правая часть уравнения (9), представляющего собой функцию обратного преобразования (лазейка для легального пользователя).

Так, например, шифр первой биграммы $m_1m_2= DI$ сообщения m определяем на основе (9) как числовое значение $C_L(a, b)$ при $a = 4, b = 9$:

$$C(m_1m_2) = C(DI) = C_L(4, 9) = 9409.$$

Перед нелегальном пользователем стоит трудная вычислительная задача – представить шифр $C_L(4, 9) = 9409$ в виде суммы двух слагаемых вида (10) с параметрами a, b и установить значения числовых эквивалентов букв D и I. Иными словами ему необходимо решить диофантово уравнение второй степени с двумя параметрами a и b:

$$(a^2 – b^2)^2 +(2ab)^2 = 9409.$$

В тоже время для легального пользователя алгоритм определения тех же значений a, b сводится к решению уравнения:

$$C_R(a, b) = (a^2+b^2)^2 =9409$$

или

$$(a^2+b^2)= 9409^{0,5}= 97,$$

Осюда он находит $a = 4, b = 9$ – как решение последнего ДУ.

Аналогично поступаем и для других биграмм сообщения m.

Теперь рассмотрим ММ асимметричной криптосистемы на основе того же уравнения (9).

Определим значение модуля $R = R(a, b)$ как число, большее чем $z^2 = (a^2+b^2)^2$, например, $z^2 + 1$ для двух наибольших числовых эквивалентов букв a и b. Далее, определим открытый $(OK = w)$ и секретный $(PK = u)$ ключи таким образом, чтобы выполнялось условие:

$$(w, u) = 1 (modR).$$

В данном случае в качестве функции прямого преобразования, определим $C_L(a, b, w)$ как:

$$C_L(a, b, w)=w^2*((a^2 –b^2)^2 +(2ab)^2)(mod R)=w^2*C_L(a, b).$$

Функцию дешифрования определим как

$$C_R(a, b, u) =u^2* C_L(a, b, w) (mod R).$$

Поскольку $(w, u) = 1 (modR)$, то при обратном преобразовании учтём, что

$$C_R(a, b, u) = u^2* w^2* C_L(a, b) (mod R) = (a^2 +b^2)^2(mod R).$$

Следовательно,

$$a^2+b^2= u (C_L(a, b, w))^{1/2} (mod R) = (C_L(a, b))^{1/2} (mod R),$$

– что так же сводится к ДУ.

Теперь рассмотрим тот же простой пример для приведённой выше ММ симметричной СЗИ. Пусть для того же сообщения

$$m = DIOPHANT$$

имеем те же числовые эквиваленты букв и разбиение на биграммы m_im_{i+1}:

$$q_D= 4, q_A= 1, q_I= 9, q_O= 15, q_P= 16, q_H= 8, q_N= 14, q_T= 20,$$

то есть

$$Q = \{4, 9, 15, 16, 8, 1, 14, 20\}.$$

Так, для биграммы $m_1m_2 = DI$ определим модуль как

$$R = R(a, b) = (a^2 +b^2)^2+ 1 = R(16, 20) + 1 =$$
$$(256 + 400)^2 + 1 = 656^2 + 1 = 430337.$$

Далее, аналогично определяются w и u таким образом, чтобы выполнялось условие

$$(w, u) = 1 (mod430337).$$

Очевидно, вычислительные затраты у легального и нелегального пользователей не соизмеримы по величине. При этом криптоаналитик, помимо прочих качеств, должен обладать ещё умением решать ДУ заранее заданной сложности. Отметим также, что рассматриваемый пример является лишь демонстрацией идеи приложения ДУ в области криптографии. Также очевидно, что указанные модели криптосистем далеки от практического применения, т.к. многие аспекты прикладной криптографии здесь опущены ради реализации идеи К. Шеннона [26].

В заключение отметим, что приведённая методика позволяет разрабатывать СЗИ для практических приложений на основе ДУ, в частности, на основе многостепенных систем диофантовых уравнений высоких степеней [5, 14, 16,17, 23], что является предметом дальнейшего исследования.

Список литературы

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 мат. 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: монография / В. О. Осипян. – LAP, 2012. – 344 с.
6. Осипян В. О. Об одном обобщении рюкзачных криптосистем / В. О. Осипян // Изв. вузов. Сев.-Кавк. регион. Техн. науки. – 2003. – Приложение № 5. – С. 18–25.
7. Осипян В. О. Моделирование ранцевых криптосистем, содержащих диофантовую трудность / В. О. Осипян, С. Г. Спирина, А. С. Арутюнян, В. В. Подколзин // Чебышевский сборник. – 2010. – Т. XI, 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. – Москва, 1961. – 88 с.
10. Серпинский В. 100 Простых, н одновременно и трудных вопросов арифметики / В. Серпинский. – Москва, 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. – № 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 Number / L. E. Dickson // Diophantine Analysis. – N.Y., 1971. – vol. 2.
16. Gloden A. Mehgradige Gleichungen / Gloden A. – 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 // 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 ACM. – 2015. – P. 338–341.
25. Sierpinski W. Elementary Theory of Numbers / W. Sierpinski. – 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* [Foundations of cryptography]. 2nd ed. Moscow, Helios ARV Publ., 2002. 480 p.
2. Vinogradov I. M. *Osnovy teorii chisel* [Fundamentals of number theory]. Ed. 9th., rev. Moscow, Nauka publ., 1981. 176 p.
3. Ivanov M. A. *Kriptograficheskiye metody zashchity informatsii v komp'yuternykh sistemakh i setyakh* [Cryptographic methods of information protection in computer systems and networks]. Moscow, Kudits-Obraz Publ., 2001. 363 p.
4. Matiyasevich Yu. B. Diaphantovy mnozhestva [Diophantine sets]. *Uspechi matematicheskikh nauk* [Successes of Mathematical Sciences], 1972, Vol. 27, iss. 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*

[Modeling of information security systems containing Diophantine difficulties. Development of methods for solving multi-step systems of Diophantine equations. Development of non-standard backpacking cryptosystems]. LAP, 2012. 344 p.

6. Osipyan V. O. Ob odnom obobshchenii ryukzachnykh kriptosistem [On a generalization of backpack cryptosystems]. *Izv. vuzov. Sev.-Kavk. region. Tekhn. nauki* [Proceedings of Universities. North-Caucasus Region. Techn. Science], 2003. Application no. 5, pp. 18–25.

7. Osipyan V. O., Spirina S. G., Arutyunyan A. S., Podkolzin V. V. Modelirovaniye rantsevykh kriptosistem, soderzhashchikh diofantovuyu trudnost [Simulation of knapsack cryptosystems containing Diophantine difficulty]. *Chebyshevskiy sbornik* [Chebyshevsky Proceedings], 2010, vol. XI, iss. 1. pp. 209–216.

8. Salomaa A. *Kriptographiya s otkrytym klyuchom* [Public Key cryptography]. Moscow, World Publ., 1995. 318 p.

9. Sierpinski W. *O reshenii uravneniy v tcelix chislax* [On the solution of equations in integers]. Moscow, 1961. 88 p.

10. Serpinsky W. 100 prostix, no odnovremenno i trudnix voprosov ariphmetiky [100 Simple, but at the same time difficult questions of arithmeti]. Moscow, 1961. 76 p.

11. . Schneier B. *Prikladnaya Kriptographiya* [Applied cryptography: Protocols,algorithms, source texts in C: TRANS]. Moscow, Triumph, 2002 . 816 p.

12. Cassels J. W. S. On the Diophantine equation. *Acta Arithmetica*. –1960. – no. 6, pp. 47–52.

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

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. 34, pp. 901–909.

15. . Dickson L. E. *History of theory of numbers. Diophantine Analysis*. N.Y., 1971, vol. 2.

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

17. Gurari M. E., Soloviev O. N. NP-complete set of theoretical problems: Sat. Doc.*10th Anne. AFM. Symp. On the theory of computing*. New York, 1978, pp. 205–215.

18. Koblitz N. *A course in number theory and cryptography*. New York, Springer-Verlag, 1987. 235 p.

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

20. Lin S. H., Cheng S. S., Li R. T. S. new public key encryption system based on Diophantine equations. *IEEE transactions on computers*, 1995, Jan., vol. 44, iss. 1.

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

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

23. . Osipyan V. O. Construction of alphabetical cryptosystems of data protection on the basis of equal power packs with Diophantine problems. *ACM*, 2012, pp. 124–129.

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

25. Serpinsky W. *Elementary Theory of numbers*. Hafner Publishing, 1964, 480 p.

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