DOI: 10.18372/2225-5036.25.14458

MODIFICATION OF RC5 CRYPTOALGORYTHM FOR ELECTRONIC DATA ENCRYPTION SYSTEMS

Tetiana Zhovnovach[1], Andriy Sagun[2], Vladyslav Khaidurov[3] , Hanna Martyniuk[4], Tetiana Scherbak[4]

[1]*Cherkasy State Technological University, Ukraine*
[2]*Cherkasy branch of the European University, Ukraine*
[3]*Kiev International University, Ukraine*
[4]*National Aviation University, Ukraine*

ZHOVNOVACH Tetiana Anatoliivna, Senior Lecturer

Year and place of birth: 1974, Poltava, Ukraine.
Education: Cherkasy National University named after Bogdan Khmelnytsky, 1996.
Position: Senior Lecturer of the Department of Mathematical, Informational and Social-Humanitarian Disciplines.
Scientific interests: economic development of the countries of the world, information space security, linguistic systems and processors.
Publications: more than 20 scientific publications.
E-mail: z.ta@ukr.net.
Orcid ID: 0000-0003-1037-4383.

SAGUN Andriy Viktorovych, PhD, Associate Professor

Year and place of birth: 1973, Cherkassy, Ukraine.
Education: Cherkasy State Technological University, 1998.
Position: Associate Professor of the Department of Informatics, Information Security and Documentation at Cherkasy State Technological University.
Scientific interests: Modeling of information security systems based on PLC. Administration of security systems, mathematical modeling of information security systems.
Publications: more than 40 scientific and methodical publications.
E-mail: avd29@ukr.net.
Orcid ID: 0000-0002-5151-9203.

KHAIDUROV Vladyslav Volodymyrovych, PhD.

Year and place of birth: 1989, Cherkassy, Ukraine.
Education: Cherkasy National University named after Bogdan Khmelnitsky, 2012.
Position: Senior Lecturer of the Department of Computer Science of Kyiv International University.
Scientific interests: information protection, software development, mathematical and computer modeling of complex objects and processes.
Publications: more than 30 scientific publications.
E-mail: allif0111@gmail.com.
Orcid ID: 0000-0002-4805-8880.

MARTYNIUK Hanna Vadymivna, PhD

Year and place of birth: 1989, Kherson, Ukraine.
Education: National Aviation University, 2011.
Position: Associate Professor of the Information Security Department.
Scientific interests: information assurance of noise measurement; statistical models of information signals; statistical methods for measuring the characteristics of random processes and fields; methods of signal simulation and measurement data.
Publications: more than 35 scientific publications, including monograph and patent for invention.
E-mail: ganna.martyniuk@gmail.com.
Orcid ID: 0000-0003-4234-025X.

SCHERBAK Tetiana Leonidivna, PhD, Associate Professor

Year and place of birth: 1973, Kyiv, Ukraine.
Education: Kyiv Polytechnic Institute, 1996.
Position: Associate Professor of the Information Security Department.
Scientific interests: technical information security systems.
Publications: more than 20 scientific publications.
E-mail: tais2004@i.ua.
Orcid ID: 0000-0003-1170-8154.

Abstract. *Encryption of electronic data requires the use of cryptanalysis functions. Information, like any value, is attacked by various scammers. The level of information security depends primarily on the security of the channels through which information from the company's information base can get into the network. To date, there are specially designed software tools that can block these channels and reduce the risk of leakage, theft or unauthorized access to information. The problem is that with an increase in the number of violations, their detection is reduced. The relevance of threats to the integrity and confidentiality of information requires careful attention to the task of protecting it. 20 years ago, the task of ensuring information security was solved with the help of cryptographic protection, the establishment of firewalls, and access control. Now these technologies are not enough, any information that has financial, competitive, military or political value is at risk. An additional risk is the possibility of intercepting the management of critical information infrastructure facilities. Particularly relevant is the increased stability of block algorithms, in particular, RC5, which is part of various open cryptographic libraries - OpenSSL, OpenVPN, etc. Improve the cryptographic stability of block diagrams and cryptographic algorithms by various methods. The article discusses the choice of shift functions for modifying the classic RC5 algorithm to increase the cryptographic stability of RC5 algorithm. For confirmation of efficiency modeling of the cryptographic system realized on the basis of modification of cryptographic algorithm RC5 was carried out and the time and qualitative characteristics of the work of the modified algorithm were obtained.*

Keywords: *encryption, cryptographic algorithm RC5, block ciphers, bitwise shift function, OpenSSL library, OpenVPN.*

Introduction

Existing electronic information security systems can protect the basic properties of information: confidentiality, integrity and availability. A deliberate encroachment on the change of any of these properties is classified as an attack on information [4].

What are the possible consequences of attacks on information? First of all, these are economic losses [4]:

- disclosure of commercial information can lead to serious direct competitive losses on the market;
- the news of theft of a large amount of information usually results in serious reputational losses;
- competitors can take advantage of theft of information, if it left unnoticed, in order to realize fictitious or knowingly unprofitable agreements on behalf of the management of the organization;
- the substitution of information both during the transfer stage and at the stage of storage in the firm can lead to huge losses;
- repeated successful attacks on an enterprise or organization that provides any type of information service reduces trust in the firm in customers, which affects the amount of revenue.

Cryptographic algorithms are used both in the scheme of symmetric and asymmetric cryptography, in particular in systems of electronic digital signature (EDS).

At different stages of creation or transmission, electronic data is protected by various encryption systems. It is known that a significant amount of information security systems when implementing authentication mechanisms, encryption uses open-source cryptographic tools that allow encryption, create keys and certificates of asymmetric cryptography, test and install secure connections. These packages include the OpenSSL package [https://ru.wikipedia.org/wiki/ OpenSSL] and is embedded in many of the major products of RSA Data Security Inc., including BSAFE, JSAFE, and S / MAIL and OpenVPN [https: // openvpn.net/index.php/open-source/downloads.html]. Consequently, the task of modifying of the cryptographic algorithm RC5 in order to increase its cryptostability and speed of operation is relevant.

The purpose of this work is to increase the efficiency of the RC5 classical algorithm by modifying its key parameters, which enhances the protection of electronic information for various applications (electronic document files, graphical files, text files) by choosing nonlinear shifting functions that are repeatedly used in single-key encryption in the proposed work modification of cryptographic algorithm RC5 based on the choice of bitwise shift functions. The abbreviation RC stands for different sources, either Rivest Cipher, or Ron's Code, that is, collectively - the "Rhone Rives the cipher" [1; 3].

Part of the basic parameters of the RC5 algorithm is variabled [1]. It is known that in the algorithm in addition to the secret key, the parameters of the algorithm have the following values:

- the size of the word w (in bits). Algorithms RC5 encode blocks in two words (A and B), and the valid values of w are natural numbers 16, 32 or 64, and 32 is the recommended value;
- number of rounds of algorithm R – as permissible, use of any integer from 0 to 255 inclusive;
- the size of the secret key in bytes b – any integer value from 0 to 255 inclusive.

For two blocks A and B in a binary representation, the classical algorithm has the following strategy. Before the first round, the operations of overlaying the extended key S (detailed formulation of the extended key S are given in [1]) are performed on the encrypted data:

$$A = \left(A + S_0\right) \bmod 2^w,\ B = \left(B + S_1\right) \bmod 2^w.$$

Each round performs the following actions [1; 3]:

$$A = \left(\left(A \oplus B\right) << B\right) + S_{2i},$$

$$B = \left(\left(B \oplus A\right) << A\right) + S_{2i+1}.$$

Decryption is performed in reverse order, given that the given cryptographic algorithm is symmetric.

Analysis of existing research

The most common methods for protecting the privacy of electronic data are steganographic and cryptographic transformations [1; 4]. Of course, the principle of their work varies significantly. Quite often, in practice, different combinations of steganographic and cryptographic systems are used.

At the time of presenting this work, virtually necessary cryptostability for this algorithm is achievable even after performing 6 rounds of linear cryptanalysis, and a differential cryptanalysis starting with 15 rounds no longer makes sense, since there are only 264 possible open texts [https://ru.wikipedia.org / wiki / RC5], then due to the rapid development of cloud computing systems, the computational capabilities of cryptanalysis are also increasing.

The main part of the study

The task of the work is to modify the known cryptographic algorithm RC5 based on the selection of bitwise shift functions during the encryption of the binary representation of arbitrary electronic information.

In platforms where the operation of a cyclic shift on a variable number of bits is executed at a different number of processor cycles, an attack on the execution time on the RC5 algorithm is possible. Two variants of such attack were formulated by cryptographic analysts Howard Haze and Helen Handshuk [1]. They found that the key can be calculated after performing about 220 crypt operations with high-precision runtime metrics and then from 228 to 240 test encryption operations. The easiest way to combat such attacks is to force the offsets to perform a constant number of cycles (for example, during the time of the slowest shift).

The work of one round of a modified algorithm using a certain function of the bitwise shift *f* can be represented as the following structural scheme (Fig. 1).

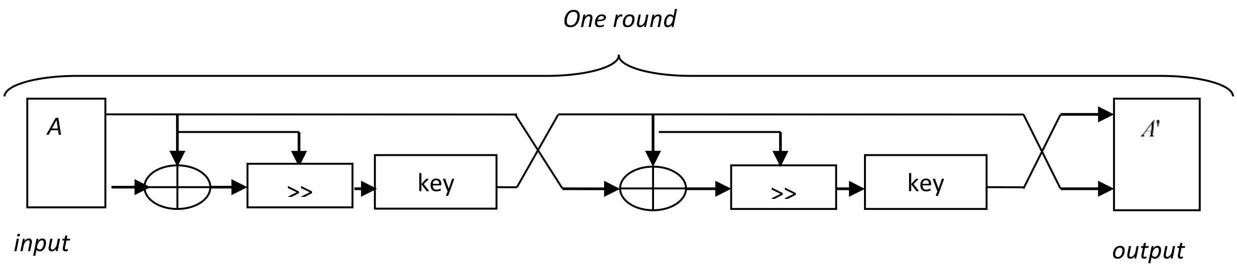


Fig. 1. The block diagram of one round of the modified cryptographic algorithm RC5 using the bitwise shift function *f*

Method of solving the problem

In accordance with the scheme in Fig. 2, it is possible to write the formulas of the modified block cryptographic algorithm for encryption of data in the form:

$$A_{i+1} = \left(\left(A \oplus B\right) << f\right) + S_{2i},$$

$$B_{i+1} = \left(\left(B \oplus A\right) << f\right) + S_{2i+1}.$$

The following functions were selected as test functions.

<u>First function:</u>

$$f\left(K, r\right) = r + \left[w \sin\left(wr \sum_{s=1}^{w} L_{bit_s} \right) \right], \qquad (1)$$

where r – round number, w – half length of the encoded block, $m = r^2 \bmod w$, $\left[x\right]$ – whole part of the number x, L_{bit} – binary representation of a character L_m coded word K, which has a length w in a binary representation.

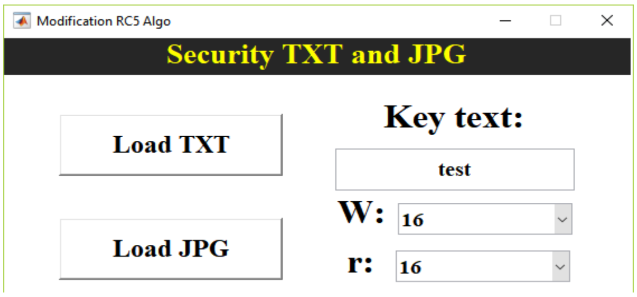
<u>Second function:</u>

$$f\left(K, r\right) = rw \exp\left(1 + \frac{r}{\left| w \sin\left(wr \sum_{s=1}^{w} L_{bits_{m_s}} \right) \right|} \right). \qquad (2)$$

<u>Third function:</u>

$$f\left(K, r\right) = r\, th\left(w \sin\left(wr \sum_{s=1}^{w} L_{bits_{m_s}} \right) \right). \qquad (3)$$

During the work, a program was developed in the MatLab environment, which has the ability to protect (encrypt and decrypt) text and graphics information. The graphical interface of the main module is shown in Fig. 2.


Modification RC5 Algo

Security TXT and JPG

Load TXT

Load JPG

Key text: test

W: 16

r: 16

Fig. 2. The user interface of the main module for the protection of electronic documents

To simulate the work of the developed modification of the cryptographic algorithm, an application software package MatLab is used to find solutions to real applications of various technical problems of different origin. It can be used as a tool for processing signals, images and videos for the purpose of protecting certain electronic information.

The main module of the program consists of the main blocks: the user interface, a subroutine for integrated protection of the graphic file, a subroutine for forming a protected image and its recording in the current folder, a subroutine for extracting and decrypting the information in the graphic container. Detailed information about the program modules is shown in Fig. 3.

Fig. 4 and Fig. 5 show the results of the program of protection of text and graphic documents of electronic document circulation.

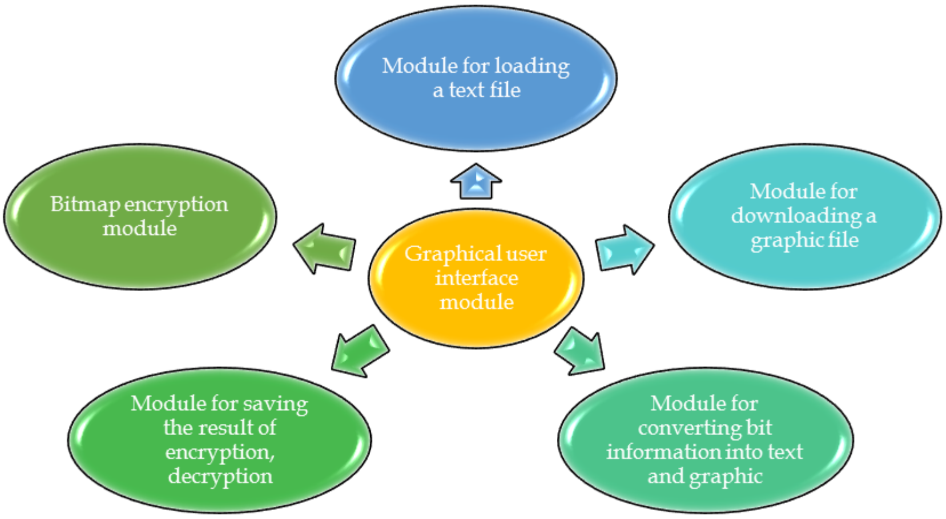

Module for loading a text file
Bitmap encryption module
Graphical user interface module
Module for downloading a graphic file
Module for saving the result of encryption, decryption
Module for converting bit information into text and graphic

Fig. 3. The main modules of the developed application in the Matlab environment

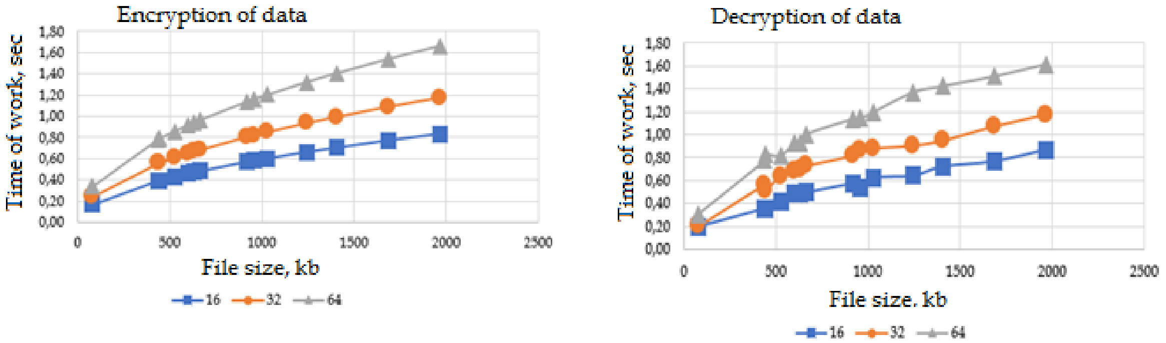


Fig. 4. Results of the program for encryption (left) and decryption (right) text information at *r=16*

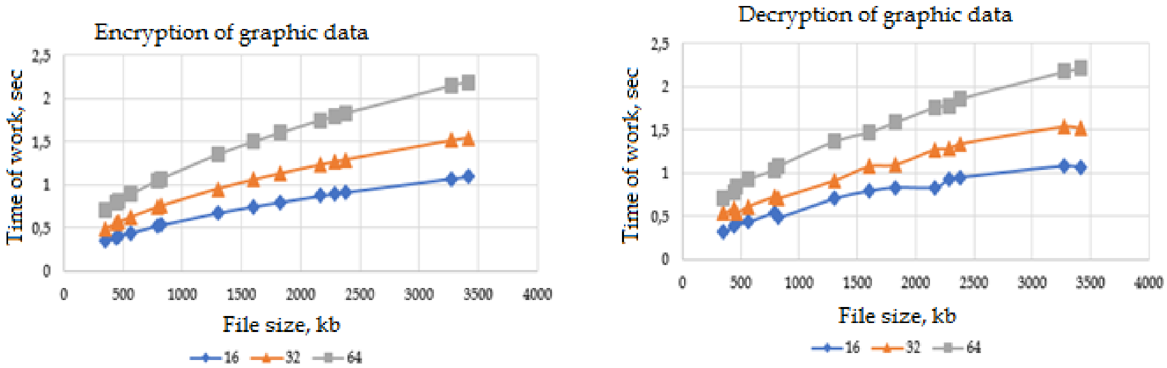


Fig. 5. Results of the program for encryption (left) and decryption (right) graphic information at *r=16*

Table 1 presents the results of studies of the resistance of the RC5 algorithm (16 bits and 32 bits) for functions (1)–(3) to differential cryptanalysis (the number of elementary operations).

Based on the obtained results, it can be argued that the modified RC5 algorithm works very fast with files of sufficiently large volumes. It should also be noted that the choice of the bitwise shift does not significantly affect the time of encryption and decryption of text and graphic information.

Determination of additional bits when encoding the cryptoalgorythm. Due to the fact that the modified cryptographic algorithm RC5 is a block algorithm, we define how many additional bits should be added to a message of 106 characters long if the Unicode characters with codes U + 0000 to U + 007F are used for encoding.

Table 1

Resistance of the RC5 algorithm to differential cryptanalysis

RC5 Method	16 bits	32 bits
Classic	2^{27}	2^{37}
Function (1)	2^{31}	2^{39}
Function (2)	2^{28}	2^{40}
Function (3)	2^{33}	2^{42}

Solution: Define that the character encoding in the case of UTF-8 use is one byte (taking into account zero in the older bit) and fully matches the 7-bit US-ASCII encoding [4]. So, encoding one character will require 8 bits. Thus, an encoded message of 106 characters contains 848 bits.

In the implemented test model, the cryptographic algorithm works with blocks of 64-bit length, that is, the original text must be divided by 64. If the letters M and m are denoted by the letters, respectively, of the useful message and the length of the complementary bits, then:

$$M + m \equiv 0\left(\mathrm{mod}\,64\right) \Rightarrow m \equiv -848\left(\mathrm{mod}\,64\right) \equiv 48\left(\mathrm{mod}\,64\right)\cdot$$

So, at the end of the open text you should add 16 extra bits. In this case, the total length of the message will be 896 bits or 13 blocks of 64 bits, which corresponds to 14 rounds of the algorithm to create 14 blocks of encrypted text.

Cryptographic stability of the algorithm. Theoretically, the cryptostability of the RC5 algorithm, documented by the linear cryptanalysis method, shows that the algorithm is reliable after 6 rounds. While differential cryptographic analysis requires 2^{24} selected open source texts for a 5 rounds algorithm, 2^{45} - for 10 rounds, 2^{53} - for 12 rounds, 2^{68} – for 15 rounds. Due to what exists 2^{64} possible different open texts [3], then cryptographic analysis is not possible for 15 or more rounds.

Determine the cryptographic stability of the modified cryptographic algorithm (the possibility of obtaining open text corresponding to the intercepted ciphertext) under the condition that:

1) he works in substitution / reshaping mode;
2) block size n = 64 bits;
3) encrypted text contains 12 units of information capacity;
4) speed of blocking by cryptographic analyst 108 blocks per second.

Indeed, for the substitution mode, each open-text bit can be replaced by "0" or "1" -the original open text and encrypted text may have different number of units.

Under given conditions, it's not known how many units are in plain text, which requires checking all possible blocks, the number of which is equal to 2^{64}. Consequently, for the given speed, the execution time of the cryptanalysis will be: t=$2^{64}/10^{8}$. In order to avoid the case of a computing device in operations with high degree indices, we use the properties of the natural logarithm:

$$\ln t = 64\ln 2 - 8\ln 10 = 25{,}94,$$

where:

$$t \approx e^{26} \approx 195729609426(s) \approx 54369336(h) \approx 2265389(d) \approx 6206(y).$$

If cryptanalysis is available at the disposal of the best computing power, the cryptanalysis time can be significantly reduced.

For cryptanalysis permutation mode, it is known that there are exactly 10 units in the open text. When using a brut force attack, only those 64-bit blocks that have exactly 10 units are used. The total number of such blocks can be estimated by the expression:

$$C_{64}^{10} \approx 151{*}10^{9}\cdot$$

Thus, it can be said that the modification of the RC5 cluster algorithm using the selected bitwise shift functions makes it more stable than cryptographic analysis.

Conclusions

The use of the modification described in the RC5 algorithm in the work makes it possible to protect the protection of electronic files of various origin. It should be noted that taking into account the improvements of the RC5 basic algorithm by choosing nonlinear displacement functions (1), (2) and (3), we obtain a much more stable algorithm in relation to the classical one. Additional bits are determined at coding in a cryptographic algorithm and the cryptographic stability of the algorithm is calculated under certain conditions.

The resulting modification of the cryptographic algorithm RC5 is theoretically more cryptic than traditional, which allows to increase the cryptographic stability of existing applied cryptosystems.

References

[1]. [Electronic resource]. Online: http://cseweb. ucsd. edu/~mihir/papers/gb.pdf.

[2]. [Electronic resource]. Online: http:// cryptography.ru/wp-content/ uploads/ 2014/11/ varn_ lectures_long.pdf

[3]. L. Babenko, Ye. Ishchukova, *Sovremennyye algoritmy blochnogo shifrovaniya i metody ikh analiza*, M.: Gelios ARV, 2006, 376 p.

[4]. O. Logachov, A. Sal'nikov, S. Smyshlyayev, V. Yashchenko, *Bulevy funktsii v teorii kodirovaniya i kriptologii. Izdaniye vtoroye, dopolnennoye,* MTSNMO, M., 2012.

UDC 004.056.55 (045)

Жовновач Т.А., Сагун А.В., Хайдуров В.В., Мартинюк Г.В., Щербак Т.Л. Модифікація криптоалгоритму RC5 для систем шифрування електронних даних

Анотація. *Шифрування електронних даних вимагає застосування стійких до криптоаналізу функцій. Інформація, як будь-яка цінність, піддається посяганням з боку різних шахраїв. Концентрація інформації в комп'ютерних системах змушує мати великі зусилля для її захисту. Національна безпека, державна таємниця, комерційна таємниця - всі ці аспекти вимагають посилення контролю над інформацією в комерційних і державних організаціях. Рівень інформаційної безпеки залежить в першу чергу від захищеності каналів, по яких дані з інформаційної бази компанії можуть потрапити в мережу. На сьогоднішній день існують спеціально розроблені програмні засоби, здатні перекрити ці канали і знизити ризик витоку, викрадення або несанкціонованого доступу до інформації. Проблемою стає те, що з ростом числа порушень знижується їх розкриття. Актуальність загроз цілісності і конфіденційності інформації вимагає відповідального ставлення до завданню* *її захисту. 20 років назад завдання забезпечення безпеки інформації вирішувалася за допомогою засобів криптографічного захисту, встановлення міжмережевих екранів, розмежування доступу. Зараз цих технологій недостатньо. Будь-яка інформація, що має фінансову, конкурентну, військову чи політичну цінність, опиняється під загрозою. Додатковим ризиком стає можливість перехоплення управління критичними об'єктами інформаційної інфраструктури. Тому особливо актуальним є завдання підвищення стійкості блочних алгоритмів, зокрема, RC5, який входить до складу різних відкритих криптографічних бібліотек – OpenSSL, OpenVPN тощо. Підвищувати криптографічну стійкість блокових схем та криптоалгоритмів можна різними методами. У статті розглядається вибір функцій зсувів для модифікації класичного алгоритму RC5 з метою підвищення криптографічної стійкості останнього. Для підтвердження ефективності проведено моделювання криптографічної системи, реалізованої на базі модифікації криптоалгоритму RC5 та отримані часові та якісні характеристики роботи модифікованого алгоритму.*

Ключові слова: *шифрування, криптографічний алгоритм RC5, блочні шифри, функція побітового зсуву, бібліотека OpenSSL, OpenVPN, прикладний програмний пакет MatLab.*

Жовнович Т.А., Сагун А.В., Хайдуров В.В., Мартинюк А.В., Щербак Т.Л. Модификация криптоалгоритма RC5 для систем шифрования электронных данных

Аннотация. *Шифрование электронных данных требует применения стойких к криптоанализу функций. Особенно актуальным является повышение стойкости блочных алгоритмов. Информация, как любая ценность, подвергается посягательствам со стороны различных мошенников. Концентрация информации в компьютерных системах вынуждает наращивать усилия по её защите. Национальная безопасность, государственная тайна, коммерческая тайна – все эти юридические аспекты требуют усиления контроля над информацией в коммерческих и государственных организациях. Уровень информационной безопасности зависит в первую очередь от защищенности каналов, по которым сведения из информационной базы компании могут попасть в сеть. На сегодняшний день существуют специально разработанные программные средства, способны перекрыть эти каналы и снизить риск утечки, похищения или несанкционированного доступа к информации. Проблемой становится то, что с ростом числа нарушений снижается их раскрываемость. Актуальность угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты. 20 лет назад задача обеспечения безопасности информации решалась при помощи средств криптографической защиты, установления межсетевых экранов, разграничения доступа. Сейчас этих технологий недостаточно. Любая информация, имеющая финансовую, конкурентную, военную или политическую ценность, подвергается угрозе. Дополнительным риском становится возможность перехвата управления критическими объектами информационной инфраструктуры. Поэтому особенно актуальным является задание повышение стойкости блочных алгоритмов, в частности, RC5, который входит в состав различных открытых криптографических библиотек – OpenSSL, OpenVPN и т.д. Повышать криптографическую стойкость блочных схем и криптоалгоритмов можно разными методами. В статье рассматривается выбор функции сдвигов для модификации классического алгоритма RC5 с целью повышения его криптографической стойкости. В статье проведено моделирование криптографической системы, реализованной на базе модификации криптоалгоритма RC5 и получены временные и качественные характеристики модифицированного алгоритма.*

Ключевые слова: *шифрование, криптографический алгоритм RC5, блочные шифры, функция побитового смещения, библиотека OpenSSL, OpenVPN.*

Отримано *29 листопада 2019 року*, затверджено редколегією *24 грудня 2019 року*