Waldemar WOJCIK[1], Maksat KALIMOLDAEV[2,3], Rustem BIYASHEV[2,3], Nursulu KAPALOVA[2,3], Ardak AKHMETOVA[2,3], Salima NUGMANOVA[3,4], Yelzhassar MERGENBAYEV[4]

Lublin University of Technology, Poland (1), Institute of Information and Computational Technologies, Kazakhstan (2), AL-Farabi National University, Kazakhstan (3), Abai Kazakh National Pedagogical University, Kazakhstan (4)

doi:10.15199/48.2018.02.38

Creating an algorithm of encryption based on prime numbers in positional systems of calculating residual classes

***Abstract**. Building a secure local and remote data warehouse requires data transfer over network channels, identification and authentication of objects and subjects of information protection. Development of reliable and efficient cryptographic tools for information protection and security is needed. The goal is achieved through the development of encryption algorithms, formation and exchange of secret keys on the basis of the residual class system. In the article an unconventional algorithm of enciphering an electronic message of a given length consisting of two stages has been proposed.*

***Streszczenie.** Budowanie bezpiecznej lokalnej i zdalnej hurtowni danych rymaga przesyłu danych przez kanały sieciowe, identyfikacji i uwierzytelniania obiektów i podmiotów ochrony informacji. Potrzebne jest opracowanie niezawodnych i wydajnych narzędzi kryptograficznych do ochrony i bezpieczeństwa informacji. Cel ten jest osiągany poprzez rozwój algorytmów szyfrowania, tworzenie i wymianę tajnych kluczy na podstawie systemu klas* resztkowych*. W artykule zaproponowano niekonwencjonalny algorytm szyfrowania wiadomości elektronicznej o zadanej długości, składający się z dwóch etapów. (**Tworzenie algorytmu szyfrowania na bazie liczb pierwszych w pozycyjnych układach obliczania klas resztowych**).*

Keywords: please cryptography, non-positional number systems, cryptostability, deduction, residual class system.
Słowa kluczowe: kryptografia, niepozycyjne systemy liczb, kryptostabilność, dedukcja, system klas resztkowych.

Introduction

Known encryption algorithms and methods are built in positional number systems. Non-traditional algorithms created on the basis of positional number systems and cryptographic methods make it possible to increase the crypto-stability and efficiency of encryption algorithms. Creation of cryptographic algorithms models of information protection is considered on the basis of positional number systems using the features of the algebraic method. A feature is the implementation of positioning systems based on residual classes. At the same time, information protection is carried out by effective software as a module of combining cryptographic system.

This cryptographic information security, as well as processing information in a local and distributed information environment designed to prevent unauthorized access to objects in the environment can be used as an internal information security system.

Among the tasks of the information protection system are identification, authentication and authorization (or access isolation) of users when providing secure access to local or remote data. The information protection system includes the developed multicriterial system of access isolation (MSAI). MSAI will be adapted for this information security system. The adapted MSAI is also a subsystem along with CIPF. It provides the user with a secure access area in the form of information resources group available to it in accordance with its authority. The main objective of MSAI, as a subsystem of the information protection system, is to provide multicriterial access to multilevel or classified data. A software implementation of the information system will be implemented.

In our country (mainly) foreign software, hardware applications of information protection are used. These applications are naturally transparent to their developers. In this regard, the Security Council of the Republic of Kazakhstan has accepted the Concept of Information Security of the Republic of Kazakhstan. It points out the necessity of designing a national system of providing information for various levels of its secrecy (confidentiality) with subsequent hardware and software implementation. In connection with significant change in the technical base, capabilities and scale of modern communication systems, the issue of telecommunication systems and networks has also been thrown into sharp relief.

The scientific and practical significance of the project ensues from the fact that the results obtained will contribute to the development of the main components of scientific, technical and organizational information security, which are:

- development of theoretical researches and applied developments in the field of information security in infocommunication systems;
- increasing the level of protection of classified information by the gradual replacement of currently used foreign cryptographic systems with national encryption systems, digital signatures and access control;
- ensuring the required level of information security of limited use of accumulated, processed, transmitted through public telecommunications channels and provided to users with appropriate authority, accessible and effective means of protection.

In 1648 Claude Shannon's works on the mathematical theory of cryptography were declassified. He is one of the first researchers of the cipher mathematical model. The results of his secret works K. Shannon published in 1945. These works had a strong influence on the growth and development of scientific research on the theory of cryptography [1], [2].

Literature review

The wide use of modern information technologies in state and financial structures, as well as in the society in general puts forward the solution of the problem of information security in number of basic ones. Except direct damage from possible information leaks, informatization can turn into means of suppressing human freedom, become a source of serious threats to the state and spiritual life of an individual [3].

The first data encryption standard, Data Encryption Standard (DES), was published in 1977 in the USA. In 1980 it was accepted by National Institute of Standards and Technology Standards (NIST) in the USA [4]. The algorithm of the standard has been built according to Feistel's scheme and Kerckhoffs' principle.

Since 1976 cryptographic systems have been divided into two types - symmetric (with a private key) and asymmetric (with public key), that year W. Diffie's and M. Hellman's work was published, which describes the principles of cryptography with public keys [5-8].

There is sufficient experience in the use of traditional methods of encryption in the creation and practical use of the various effectiveness of methods and means of information protection in the countries of near and far abroad. It should also be noted that countries that have national standard for data encryption algorithms use software with lower cryptographic strength when exporting information and communication technology equipment to other countries, since national standards are not used in software products intended for export.

Therefore, attraction of other means to ensure information security is real necessity for Kazakhstan. All CIS countries including Russia face the same problem.

At present, there is an increased interest in the search for new effective cryptographic methods in FSU and beyond. Algorithms built in the 70-80's of the XX century, were to meet the requirements in cost-effectiveness of their implementation. Today, capabilities of the technical basis on ciphers implementation have increased a lot in comparison with the capabilities of their hardware implementation in the 70's and 80's of the last century. As a result, possibilities of their cryptanalysis have increased proportionally and requirements for cryptographic stability have substantially increased. It caused changes in modern approaches to building block ciphers with secret keys.

In May 2002 in the United States, according to the results of the competition, a new standard of AES encryption was accepted. Unlike previous algorithms, an algebraic approach is widely used when developing AES in its transformations. An algorithm with a structure based on Feistel's 'embedded' networks won in the competition in the European Union. These competitions had a strong influence on the development of cryptography and cryptanalysis [9], [10]. In Russia, GOST 28147-89 is standard for cryptographic data conversion in information processing systems. Its application is obligatory in state and certain commercial organizations of Russia [11]. In 2011 the Republic of Belarus accepted the state standard for symmetric encryption and integrity control BelT-STB 34.101.31-2007 'Information technology and security. Cryptographic algorithms for encryption and integrity control'.

Modern information technologies are actively being introduced and created in our republic – 'e-technologies'. In this regard, there is a growing need for persistent and effective means to ensure information security in electronic interaction. In the information security laboratory of the Institute an encryption algorithm and an algorithm of electronic digital signature formation were developed and studied using NPNS [12]-[17]. Algorithms and methods, based on NPNS, are non-conventional, or non-positional. Key length is one of cryptographic strength indicators. In developed non-conventional encryption systems and digital signatures, it was suggested to use the cryptographic strength of encryption algorithms and digital signature calculations, which is characterized by a full secret key, as a criterion for cryptographic stability. Besides the standard secret key, it consists of secret parameters of crypto-algorithms developed on the basis of modular arithmetic. Researches on the above-mentioned subjects are not done by other organizations in Kazakhstan. According to the open press there are no similar developments in other countries. One of the directions in the development of modular arithmetic is the research work of R.G. Biyashev on creation, analysis and use of non-positional polynomial number systems [22]. He says that the algebra of polynomials over a field modulo a polynomial irreducible over this field is a field, an analogue of the Chinese remainder theorem for polynomials, a system and the reconstruction of a polynomial from its remainders are proved. In [18, 19, 20] modeling of software implementation of asymmetric non-position encryption scheme, non-conventional encryption algorithm, cryptanalysis of encryption algorithm based on non-positional polynomial number systems.

Methods

In 1955 Czech engineer M. Valakh was the first to put forward an idea, that was actively supported by the Czech mathematician A. Svoboda, to use the system of residual classes for operations on computer numbers.

In computing practice, it was an outstanding idea, using the well-known Chinese remainder theorem. This idea attracted the attention of a large group of scientists. There was a new scientific area - modular arithmetic. The works of M. Valakh and A. Sloboda interested the Americans and a few years later they moved to the United States.

In 1955, research in this field began also in the USSR [21], [29]. In the system of residual classes, the most powerful computers for their time were developed and created, which are still "working" in the system of the Russian antimissile defense system.

One of the areas of the development of modular arithmetic is the research work of the scientific project supervisor R.G.Biyashev on the creation, analysis and use of non-position polynomial number notations [22].

He says that the algebra of polynomials over a field modulo a polynomial irreducible over this field is a field, an analogue of the Chinese remainder theorem for polynomials, a system, and the reconstruction of a polynomial from its remainders has been proved.

In [24, 25, 26], a model of an encryption algorithm developed on the basis of non-position polynomial number notations has been proposed. The possibility of modification of the developed model using Feistel network and encryption modes has been considered. The proposed model of the cryptographic algorithm will significantly increase the statistical characteristics of the obtained ciphertexts.

In the protection of information in the creation of a system for the formation and distribution of keys, the cryptographic stability of the encryption algorithm is used as the criterion for encryption and the cryptographic stability of digital systems, but not the key length. This system is based on the use of arithmetic of positioning systems, that is, the use of the system of calculation of residual classes.

In the classical system of residual classes, the basis of the number system is taken to be relatively prime numbers, then any number is represented as the remainder of the division into a system. In comparison of the classical system, the proposed cryptographic procedures are considered in the residual classes of the number system, where prime numbers are taken as a basis. In the encryption algorithm, the key sequence and prime numbers are taken as the full key, and as the basis of the system, all prime numbers not exceeding the length of the encrypted message from the selected bases in the order of distribution are selected [27, 28].

If a set of positive integers $p_1, p_2, ..., p_n$ is given, hereinafter referred to as the basis of the system, then the number system in the residual classes is understood to be a system in which a positive integer N is represented as a set

of residues on the selected grounds $N=(\alpha_1,\alpha_2,...,\alpha_n)$, and the formation of digits α_i is carried out by the following process:

(1) $$\alpha_i = N - \left[\frac{N}{p_i}\right] p_i$$

i.e. the digit of the i-th order α_i of the number N is the smallest positive remainder of dividing N by p_i and $\alpha_i < p_i$.

Here and in the following [Y] denotes the integer part of the number Y.

In contrast to the positional number notation, the formation of the digit of each digit is made in this case independently of each other.

In accordance with the Great Chinese Remainder Theorem, the representation of a number N in the form of a sequence of digits $\alpha_1,\alpha_2,...,\alpha_n$ will be unique if the numbers p_i are pairwise simple.

The volume range of the representable numbers in this case is

$$P = p_1 p_2 \cdots p_n .$$

Here, similar to the positional number notation, the range of representable numbers grows as the product of bases, and the digit capacity of numbers N increases as the sum of the digits of the same bases.

Thus, in a classical system of residual classes (SRC) pairwise prime numbers are chosen as a system of bases, and any number in it is uniquely represented by its residues (deductions) from dividing by this basis system.

Example 1. Let the bases of SRC be numbers

(2) $$p_1 = 3,\ p_2 = 5,\ p_3 = 7$$

The range of SRC is defined as $P = p_1 p_2 p_3 = 105$.

We represent the numbers A = 17 and B = 63 in the system of residual classes for the selected bases (2):

A=17=(2,2.3), B=63=(0,3,0).

We consider the rules of performing addition and multiplication operations in a system of residual classes, in case if both numbers and the result of the operation are in the range [0, P).

Suppose that the numbers A and B are represented by deductions α_i and β_i by bases p_i, respectively:

$$A=(\alpha_1,\alpha_2,...,\alpha_n),\ B=(\beta_1,\beta_2,...,\beta_{nn}).$$

Suppose also that the results of addition $A+B$ and multiplication AB are represented respectively by residues γ_i and δ_i for the same bases p_i:

$$A+B=(\gamma_1,\gamma_2,...,\gamma_{nn}),\quad AB=(\delta_1,\delta_2,...,\delta_{nn}).$$

Here the following relations hold;

$$A<P,\ B<P,\ A+B<P,\ AB<P.$$

It is proved that the digits of the result of addition and multiplication are taken respectively:

(3) $$\gamma_i = \alpha_i + \beta_i - \left[\frac{\alpha_i+\beta_i}{p_i}\right] p_i ,$$

(4) $$\delta_i = \alpha_i\beta_i - \left[\frac{\alpha_i\beta_i}{p_i}\right] p_i ,$$

i.e. γ_i is comparable with $\alpha_i+\beta_i$ the modulo p_i, but δ_i is comparable with $\alpha_i\beta_i$ the same module p_i:

$$\gamma_i \equiv \alpha_i+\beta_i (\mathrm{mod}\, p_i),\ \delta_i \equiv \alpha_i\beta_i (\mathrm{mod}\, p_i).$$

Note. In modular arithmetic or in the theory of congruences, the integers a and b are called comparable modulo n if their remainders on division n coincide. It is denoted as $a \equiv b (\mathrm{mod}\, n)$. The number n is called a module.

To indicate the remainder, a parentheses free notation $b = a \bmod n$ is used, which means that $a = kn + b$, where b is the remainder of dividing a by n.

Example 2. For the example 1, we get.

In accordance with the formula (3) A + B = (2,0,3). Verification: the sum of the numbers A = 17 and B = 63 is 80, if we write it in the non-position form (that is, in the residual class system) for the bases of Example 1, then it will have the form 80 = (2,0,3).

Example 3. Let us find the product of numbers A = 17 and B = 6. In the system of residual classes (for the example 1), they will be presented as:

A=17=(2,2.3), B=6=(0,1,6).

In accordance with the formula (4), AB = (0,2,4) and is equal to 102.

Results.

Unlike classical systems in residual classes, the proposed cryptographic procedures are considered in polynomial number systems in residual classes in which polynomials are considered instead of numbers and the bases are not simple numbers but irreducible polynomials with binary coefficients.

Irreducible polynomials in the NPNS are the analog of prime numbers in system of residual classes.

The non-position polynomial number notation is constructed in a manner similar to the classical SRC. We denote the chosen polynomial bases $p_1, p_2,..., p_n$, they are called working bases (since in the formation algorithm of the electronic digital signature the redundant or additional bases will be introduced).

The procedure of selecting the working bases will be described below when deriving Eq. (12).

Let $\alpha_1,\alpha_2,...,\alpha_n$ be the remainders of dividing the polynomial N into bases $p_i, i=1,2,...,n$. Then the polynomial N, by analogy with the number notation in residual classes with pairwise simple bases, is represented in the form of residues from the division $N(x)$ into the chosen system of bases:

(5) $$N=(\alpha_1,\alpha_2,...,\alpha_n),$$

where

(6) $$\alpha_i = N - \left[\frac{N}{p_i}\right] p_i,\ i=\overline{1,n}$$

there is a remainder of dividing N by p_i, here $i=\overline{1,n}$ means $i=1,2,...,n$.

Algorithm of encryption based on the positional number notation

The nontraditional algorithm of encrypting an electronic message of a given length N includes two steps:

- the choice of a system of polynomial bases (the formation of NPNS) and the order of their location;
- generation of a key (pseudo-random) sequence.

These two stages describe the choice of one (or one variant) of the base system. Their essence consists in the following.

Stage 1. Let $p_1, p_2,..., p_S$ be irreducible polynomials with binary coefficients, used as working bases.

The polynomial $P = p_1 p_2 \cdots p_S$ is the main operating range. In this system, any single representation in the form

of its deductions by working bases (or remainders from division by) $p_1, p_2,..., p_S$ respectively.

Then a message of length N bits can be interpreted as a sequence of residues $\alpha_1, \alpha_2,..., \alpha_S$ from dividing a polynomial $F(x)$ into working bases $p_1, p_2,..., p_S$, respectively:

(7) $F = (\alpha_1, \alpha_2,..., \alpha_S)$,

where $F \equiv \alpha_i (\mathrm{mod}\, p_i)$, $i = \overline{1, S}$. In the expression (7), the residues $\alpha_1, \alpha_2,..., \alpha_S$ are selected in such a way that the first l_1 bits of the message are mapped to the binary residual coefficients α_1, the next bits l_2 are the residual binary coefficients α_2, and so on, the binary coefficients α_S of the residue are mapped to the last binary bits l_S.

The representation (or reconstruction) in the positional form of the polynomial F is made by its non-position form (7). In the case of storage, transmission and processing of information, it is carried out according to the following formula:

(8) $$F = \sum_{i=1}^{S} \alpha_i B_i,\ B_i = \frac{\prod_{i=1}^{S} p_i}{p_i} M_i \equiv 1 (\mathrm{mod}\, p_i);$$

where $i = \overline{1, S}$ and the values of the polynomials M_i are also selected for the comparison indicated in the formula. For the stored and transmitted information, the recovery occurs according to the expression:

(9) $F = \sum_{i=1}^{S} \alpha_i P_i$, where $P_i = \frac{P}{p_i}$, $i = \overline{1, S}$.

Stage 2. For encryption, a key sequence of length N bits is used, which is also interpreted as a sequence of residuals, but from dividing some other $G(x)$ along the same working bases of the system:

(10) $G = (\beta_1, \beta_2,..., \beta_S)$

where $G \equiv \beta_i (\mathrm{mod}\, p_i)$, $i = \overline{1, S}$.

In accordance with the operations of the number notation, operations in the functions F, G, H are performed in parallel with respect to those chosen as working bases. Computer implementation of the developed encryption algorithm uses an nontraditional cryptographic method. The use of different encryption methods gives different cryptographic models.

In this encryption model, the cryptogram of the electronic message $H(x) = (\omega_1(x), \omega_2(x),..., \omega_S(x))$ is obtained as a result of multiplying the polynomials (7) and (10) in accordance with the properties of the comparisons.

Then the elements of the residue sequence $\omega_1(x), \omega_2(x),..., \omega_S(x)$ are the smallest residues from the division of products $\alpha_i(x)\beta_i(x)$ into the corresponding bases $p_i(x)$:

(11) $\alpha_i(x)\beta_i(x) \equiv \omega_i(x) (\mathrm{mod}\ p_i(x))$, i=1,2,…S.

In the form of the cryptogram $H(x)$ will look like this: $\omega_1(x)$ the remainder coefficients are associated with the first bit l_1 of the cryptogram $H(x)$. The following bits l_2 of the cryptogram are put in correspondence to the coefficients of the remainder $\omega_2(x)$, and so on. The coefficients of the last residue ω_S are put in correspondence with the last cryptograms l_S.

When decrypting the cryptogram H from the known key G for each value β_i, the inverse polynomial is calculated, as follows from (11), from the condition that the following comparison is performed:

(12) $\beta_i \beta_i^{-1} \equiv 1 (\mathrm{mod}\ p_i)$, i=1,2,…S.

As a result, a polynomial inverse $G^{-1} = (\beta_1^{-1}, \beta_2^{-1},..., \beta_S^{-1})$, to the polynomial $G(x)$ is obtained. Then the original message in accordance with (11) and (12) is restored through deductions by the following comparisons:

(13) $\alpha_i \equiv \beta_i^{-1} \omega_i (\mathrm{mod}\, p_i)$, i=1,2,…S.

Thus, in the model of the algorithm of encrypting an electronic message of a given length N bits in the NPNS, the complete key is the chosen polynomial base system $p_1, p_2,..., p_S$, obtained by generating a pseudorandom sequence key $G = (\beta_1, \beta_2,..., \beta_S)$ and an inverse key $G^{-1} = (\beta_1^{-1}, \beta_2^{-1},..., \beta_S^{-1})$ to it, which is computed in accordance with expression (12).

Let's consider examples of translation from a positional system to a system of residual classes and back

1. We set working bases $\rho_1 . \rho_2 . \rho_3 ....., \rho_n$

2. We calculate $p = \rho_1 . \rho_2 . \rho_3 ..., \rho_n$

3. We select $\mathrm{A} \in [0; \rho)$; and $\mathrm{B} \in [0 \rho)$

4. We move to the residual classes A and B

$$\mathrm{A} = \mathrm{A} (\mathrm{mod}\, \rho_i) = (\alpha_i, \alpha_2, \alpha_3, .., \alpha_n)$$

$$\mathrm{B} = \mathrm{B} (\mathrm{mod}\, \rho_i) = (\beta_1, \beta_2, \beta_3, ..., \beta_n)$$

$$\mathrm{A} + \mathrm{B} = \mathrm{A} + \mathrm{B} (\mathrm{mod}\, \rho_i) = (j_1, j_2, j_3, .., j_n)$$

5. Using the $\delta = \frac{\rho}{\rho_i} (\mathrm{mod} \rho_i), i = 1,2,..,n$ determine δ_i.

6. We choose m_i so that the comparison

$\frac{m_i \rho}{\rho_i} \equiv 1 (\mathrm{mod}\, \rho_i)$ is performed.

7. $\mathrm{B}_i = \frac{m_i \rho}{\rho_i}$, $i = 1,2,...., n$

8. We apply p_i encryption to $\mathrm{A} + \mathrm{B} = \sum_{i=1}^{n} \mathrm{B}_i \cdot j_i (\mathrm{mod}\, \rho)$.

Set working bases $\rho_1 . \rho_2 . \rho_3 ....., \rho_n$, $\rho_1 = 17$, $\rho_2 = 29$, $\rho_3 = 23$, $\rho_4 = 3$.

Define the range $p = \rho_1 . \rho_2 . \rho_3 ..., \rho_n$ $\rho = 17 \cdot 29 \cdot 23 \cdot 3 = 34017$

$\mathrm{A} = \mathrm{A} (\mathrm{mod}\, \rho_i)$ $\mathrm{A} = 184$.

$\mathrm{A}_1 = 184 \mathrm{mod} 17 = 14 \mathrm{mod} 17$. $\mathrm{A}_3 = 184 \mathrm{mod} 23 = 0 \mathrm{mod} 23$.

$\mathrm{A}_2 = 184 \mathrm{mod} 29 = 10 \mathrm{mod} 29$. $\mathrm{A}_4 = 184 \mathrm{mod} 3 = 1 \mathrm{mod} 3$.

$\mathrm{A} = (14; 10; 0; 1)$

$\mathrm{B} = \mathrm{B} (\mathrm{mod}\, \rho_{i(\ )})$ $\mathrm{B} = 48$. $\mathrm{B}_3 = 48 \mathrm{mod} 23 = 2 \mathrm{mod} 23$.

$B_1 = 48 \bmod 17 = 14 \bmod 17.\quad B_4 = 48 \bmod 3 = 0 \bmod 3.$

$B_2 = 48 \bmod 29 = 19 \bmod 29.$

$B = (14;19;2;0)$

$A + B = A + B(\bmod \rho_i).\quad A + B = (11;0;2;1)$

This rule is repeated for the product $A \cdot B = A \cdot B(\bmod \rho_i)$

$A \cdot B = (9;16;0;0)$

$$\rho = \frac{\rho}{\rho_i}$$

$$\rho_1 = \frac{34017}{17} = 2001.$$

$$\rho_2 = \frac{3417}{29} = 1173.$$

$$\rho_3 = \frac{34017}{23} = 1479.$$

$$\rho_4 = \frac{34017}{3} = 11339.$$

$$\delta_i = \frac{\rho}{\rho_i}$$

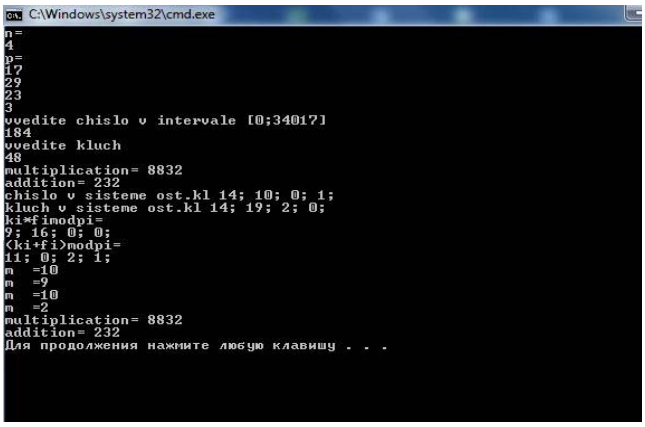
$$\delta_1 = \frac{2001}{17} = 12.$$

$$\delta_2 = \frac{1173}{29} = 13.$$

$$\delta_3 = \frac{1479}{23} = 7.$$

$$\delta_4 = \frac{11339}{3} = 2.$$

$m_1 = 10;\quad m_2 = 9;\quad m_3 = 10;\quad m_4 = 2.$



We find the basis $B_{baz} = m \cdot \rho.$

$B_{baz1} = 10 \cdot 2001 = 20010.$

$B_{baz2} = 9 \cdot 1173 = 10577.$

$B_{baz3} = 10 \cdot 1479 = 14790.$

$B_{baz4} = 2 \cdot 11339 = 22678.$

$$A + B = \sum_{i=1}^{n} B_i \cdot j_i (\bmod \rho)$$

$A = 14 \cdot 20010 + 10 \cdot 10557 + 0 \cdot 14790 + 1 \cdot 22678 =$

$= 280140 + 10570 + 0 + 22678 = 408388 - 12 \cdot 34017 = 184.$

$B = 14 \cdot 20010 + 19 \cdot 10557 + 2 \cdot 147990 + 0 \cdot 22678 =$

$= 280140 + 200583 + 29580 + 0 = 510303 - 15 \cdot 34017 = 48$

$A + B = (11;0;2;1)$

$A + B = 11 \cdot 20010 + 0 \cdot 10557 + 2 \cdot 14790 + 1 \cdot 22678 =$

$= 220110 + 0 + 29580 + 226678 = 272368 - 8 \cdot 34017 = 238.$

$A \cdot B = (9;16;0;0)$

$A \cdot B = 9 \cdot 20010 + 16 \cdot 10557 + 0 \cdot 14790 + 0 \cdot 22678 =$

$= 180090 + 168912 + 0 + 0 = 349002 - 10 \cdot 34017 = 8832$

Discussion

For the protection of information, mainly foreign hardware and software are used, then the creation of domestic means of cryptographic protection and the access control to information for different levels of confidentiality are certainly important. Application of the obtained research results will reduce the probability of unauthorized access to information, its theft and modification. Authentication and integrity of information, accessibility and confidentiality determine the economic effect of information security.

The obtained results can be used to protect electronic information during its storage and transmission in info-telecommunication systems and networks for various purposes, as well as in cloud structures.

The target consumers of the results obtained are state institutions, commercial enterprises, research institutes, universities and other organizations that have distributed corporate systems and networks.

Conclusions

The nontraditional algorithm of encrypting an electronic message of a given length N consisting of two stages has been proposed:

- choice of the system of bases (formation) and the order of their location;
- generation of key (base system for encryption and their placement, generation of key)

These two stages describe the choice of one (or one variant) of the base system.

***Authors**: Waldemar Wójcik, Politechnika Lubelska, Instytut Elektroniki i Technik Informacyjnych, Nadbystrzycka 38A, 20-618 Lublin, E-mail: waldemar.wojcik@pollub.pl; Maksat Kalimoldayev, Institute of Information and Computational Technologies of SC MES RK, Pushkin 125, 050010 Almaty, Kazakhstan, and al-Farabi Kazakh National University, 71 al-Farabi Ave., Almaty, Kazakhstan, E-mail: mnk@ipic.kz; Rustem Biyashev, Institute of Information and Computational Technologies of SC MES RK, Pushkin 125, 050010 Almaty, Kazakhstan, and al-Farabi Kazakh National University, 71 al-Farabi Ave., Almaty, Kazakhstan, E-mail: info@ipic.kz; Nursulu Kapalova, Institute of Information and Computational Technologies of SC MES RK, Pushkin 125, 050010 Almaty, Kazakhstan, and al-Farabi Kazakh National University, 71 al-Farabi Ave., Almaty, Kazakhstan, E-mail: info@ipic.kz; Ardak Akhmetova, Institute of Information and Computational Technologies of SC MES RK, Pushkin 125, 050010 Almaty, Kazakhstan, and al-Farabi Kazakh National University, 71 al-Farabi Ave., Almaty, Kazakhstan, E-mail: info@ipic.kz; Salima A. Nugmanova, al-Farabi Kazakh National University, 71 al-Farabi Ave., Almaty, Kazakhstan, and Abai Kazakh National Pedagogical University, Dostyk ave. 13, 050010 Almaty, Kazakhstan, E-mail: nugm_s@mail.ru; Yelzhassar B. Mergenbayev, al-Farabi Kazakh National University, 71 al-Farabi Ave., Almaty, Kazakhstan, and Abai Kazakh National Pedagogical University, Dostyk ave. 13, 050010 Almaty, Kazakhstan, elzhasar_kz@mail.ru*

REFERENCES

[1] Shannon K., Mathematical theory of communication, Works on computer science and cybernetics, Moscow: IIL,(1963), 245-332.

[2] Shannon K., Theory of communication in secret systems, *Proceedings on computer science and cybernetics*, Moscow: IIL, (1963), 333-402.

[3] Harbarchuk V., Wójcik W., Zadiraka V., Computer Technologies for Information Security, *Lublin: Lublin University of Technology*, (2011)

[4] DES Modes of Operation, *FIPS 81*, *http//:csrc.nist.gov*, (1980).

[5] Diffie U., Hellman M.E., Security and Spoofing Resistance: Introduction to Cryptography, *TIIER - Proceedings of the Institute of Electrical and Electronics Engineering*, 67(1979), No.3. 71-109.

[6] Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Fundamentals of Cryptography: study guide for higher education institutions. 2nd edition. *Helios ARV*, (2002).

[7] Schneier B.A., Applied cryptography. Protocols, algorithms, initial tests in C language, *Moscow, TRIUMPH*, (2003).

[8] Forouzan B.A., Cryptography and network security: Textbook, *Moscow: Internet-University of Information Techn. BINOM. Knowledge lab,* (2010).

[9] Zenzin O.S., Ivanov M.A. The cryptographic protection standard -AES. Finite fields, *KUDITS-OBRAZ*, (2002).

[10] Panasenko S.P. Algorithms of coding. Special reference book, *SPb.: BHV-Petersburg*, (2009).

[11] GOST 28147-89, Information processing system. Cryptographic protection. Algorithm of cryptographic transformation, *Moscow, Gosstandart SSR*, (1989).

[12] Omiotek Z., Burda A., Wójcik W., The use of decision tree induction and artificial neural networks for automatic diagnosis of Hashimoto`s disease, *Expert Systems With Applications*, 40(2013), No. 16, 6684-6689.

[13] Biyashev R., Nyssanbayeva S., Kapalova N., Asymmetric Encryption on the Basis of Non-positional Polynomial Notations, Proceedings of the 6th International Conference on Applied Informatics and Computing Theory (AICT '15), (2015), 225-231.

[14] Biyashev R. G., Nyssanbayeva S.E., Kapalova N.A., Duysenbayev D.S., Modeling of software implementation of asymmetric non-position encryption scheme, *Proceedings of "XI International Asian School and Seminar "Problems of complex systems optimization"*, (2015), 162-166.

[15] Biyashev R., Kalimoldayev M., Nyssanbayeva S., Kapalova N., Khakimov R., Software Implementation of the Cryptographic System Models with the Given Cryptostrength, *Bulletin of the KazNU. Al-Farabi, series of mathematics, mechanics, computer science*, 86(2015), No. 3,117-121.

[16] Biyashev, R. Nyssanbayeva S., Kapalova N., Haumen A., Modified symmetric block encryption-decryption algorithm based on modular arithmetic, *Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016)*, (2016), 263-265.

[17] Biyashev R., Nyssanbayeva S., Kapalova N., Asymmetric Encryption on the Basis of Non-positional Polynomial Notations, *Proceedings of the 6th International Conference on Applied Informatics and Computing Theory (AICT '15)*, (2015), 225-231.

[18] Biyashev R., Nyssanbayeva S., Kapalova N., Khakimov R., Modular models of the cryptographic protection of information, Proc. International Conference on Computer Networks and Information Security (CNIS2015), (2015), 393-398.

[19] Biyashev R., Nyssanbayeva S., Kapalova N., Khakimov R.A., Development of a cryptographic protection system based on modular arithmetic, *Proc. XIII International Scientific and Practical Conference "IB-2013". Part I.-Taganrog: SFU publ.house*, (2013), 215-220.

[20] Nyssanbayeva S.E., Magzom M.M. Simulation of non-traditional encryption algorithm, *Bulletin of KazNTU*, (2015), No.4, 596-599.

[21] 19. Akushskyi I.Y., Yudickiy D.I. Machine arithmetic in the residual classes.-M .:Soviet radio,1968.-p.439.

[22] 20. Biyashev R.G. Development and research of methods of end-to-end reliability increase in data exchange systems of distributed Automatic Control Systems: Thesis for a degree of Dr of Tech.Sc. - M.,1985.-p.328.

[23] ST RK 1073-2007. Tools of cryptographic protection of information/ General technical requirements, *Ent. 2009.01.01.-Astana,* (2009), 15.

[24] Devyanin P.N., Models of security of computer systems. Control of access and information flows, Training manual for high schools, *Moscow, Hot line-Telecom*, (2011).

[25] Gaidamakin N.A., Theoretical foundations of Computer Security: training manual, *Ekaterinburg: Publishing House of the Ural University*, (2008).

[26] Ivanov M.A. Cryptographic methods of information protection in computer systems and networks. Educational-reference publication, *Moscow: KUDITS-OBRAZ*, (2001).

[27] Kapalova N., Dyusenbayev D., Security analysis of an encryption scheme based on nonpositional polynomial notations, *Open Engineering*, (2016), No.6, 250-258.

[28] Kapalova N.A., Dyusenbayev D.S., Cryptanalysis of the encryption algorithm on the basis of non-position polynomial number notations, Bulletin of KazNU. Mathematics, Mechanics, Informatics Series. Almaty, 90(2016), No.3/1, 41-51.

[29] Akushskyi I.Y., Khatskevich V.K., Inverse representations of numbers in the system of residual classes, *Digital computer engineering and programming, edition 2.*, (1967).