MOLDOVA STATE UNIVERSITY

DOCTORAL SCHOOL OF PHYSICAL, MATHEMATICAL, INFORMATION, AND ENGINEERING SCIENCES

Presented as manuscript
U.D.C.: 519.21:004.421(043.2)

MALYUTINA NADEZHDA

THE USE OF INFORMATION TECHNOLOGIES IN THE DEVELOPMENT OF CRYPTOGRAPHIC AND ALGEBRAIC ALGORITHMS

Summary of the Ph.D. thesis in Computer Science

122.03 – Models, Mathematical Methods, Software Products

Author: Malyutina Nadezhda

PhD Supervisors: Corlat Andrei, Ph.D. in physical and mathematical sciences, university professor
Shcherbacov Victor, Ph.D. hab.in physical and mathematical sciences, university professor

Guidance commission: Cojocaru Svetlana, Ph.D. hab.in computer science, corresponding member
Arnautov Vladimir, Ph.D. hab.in physical and mathematical sciences, academician
Titchiev Inga, Ph.D. in computer science, university professor

CHISINAU, 2023

The thesis was elaborated at the Doctoral School of Physical, Mathematical, Information, and Engineering Sciences, Moldova State University.

Ph.D. Commission:

The President of the Commission:	**GAINDRIC Constantin,** Ph.D. hab.in computer science, Corresponding Member, „Vladimir Andrunachievici" Institute of Mathematics and Computer Science, Moldova State University;
Ph.D. supervisors:	**CORLAT Andrei**, Ph.D. in physical and mathematical sciences, associate professor, Technical University of Moldova;
	SHCHERBACOV Victor, Ph.D. hab.in physical and mathematical sciences, university professor, „Vladimir Andrunachievici" Institute of Mathematics and Computer Science, Moldova State University;
Official reviewers:	**CHIRIAC Liubomir,** Ph.D. hab.in physical and mathematical sciences, university professor, "Ion Creangă" State Pedagogical University;
	TITCHIEV Inga, Ph.D. in computer science, associate professor, „Vladimir Andrunachievici" Institute of Mathematics and Computer Science, Moldova State University;
	OHRIMENCO Serghei, Ph.D. hab. in economics, university professor, Academy of Economic Studies;
	PETIC Mircea, Ph.D. in computer science, associate professor, "Alecu Russo" State University from Balti;
Scientific secretary:	**NOVAC Ludmila,** Ph.D. in physical and mathematical sciences, associate professor, Moldova State University.

The thesis defense will take place on the 21 of April 2023, at 14-00, bureau 340, „Vladimir Andrunachievici" Institute of Mathematics and Computer Science, Academiei str. 5, Chisinau, Moldova.

The doctoral thesis and the summary can be consulted at the Library of the Moldova State University and on the website of the National Agency for Quality Assurance in Education and Research (www.cnaa.md).

Summary sent on _____2023

Secretary of Doctoral Commission: _____ **NOVAC Ludmila**

Author: _____ **MALYUTINA Nadezhda**

CONTENTS

1. CONCEPTUAL GUIDELINES OF THE RESEARCH

The topicality and importance of the research

Most of the known constructions of error detection and correction codes, cryptographic algorithms, and encryption systems used associative algebraic structures such as groups and fields [1, 2]. The analysis of the studies showed that such non-associative structures as quasigroups can be used quite successfully in many branches of coding theory, especially in cryptology. Codes and ciphers based on non-associative systems show better capabilities than known codes and ciphers based on associative systems [3, 4].

The first professional cryptographers who were associated with the development of the theory of quasigroups are A.A. Albert, A. Drisko, M. M. Glukhov, J.B. Rosser, E. Schönhardt, C. I. Mendelson, and R. Schaufler. Some results obtained in the field of application of quasigroups in cryptology and coding theory are described in the works of J. Denes and A.D. Keedwell [3, 5-7]. Many of the results of non-associative public key cryptography are reflected in the work of A. Kalka [8].

Important results in the application of the theory of quasigroups in cryptography were obtained by M.E. Tuzhilin [9]; Y.M. Movsisyan [10]; A.V. Gribov, P.A. Zolotykh, and A.V. Mikhalev [11]; G. Maze, C. Monico, and J. Rosenthal [12]; V. Shpilrain and A. Ushakov [13]; R.E. Atani, Sh.E. Atani, and S. Mirzakuchaki [14]; A. Krapez [15, 16]; K. A. Meyer [17]; V.A. Artamonov, S. Chakrabarti, V. T. Markov, and S. K. Pal [18, 19].

C. Koscielny and G.L. Mullen presented a public key cryptosystem using generalized stream ciphers based on quasigroups in [20]. Quasigroups for secure coding are suggested to be used by E. Ochodkova and V. Snasel [21]; S. Markovski, D. Gligoroski, B. Stojcevska, and V. Bakeva [22, 23]; S. Markovski, V. Dimitrova, Z. Trajcheska, M. Petkovska, M. Kostadinoski, and D. Buhov [24].

Smile Markovski and his co-authors introduce a near-public key stream cipher based on quasigroups in [22]. Markovski algorithm and its generalizations are currently widely known and often used by stream ciphers based on quasigroups. Improvements and research of the Markovski algorithm were intensively carried out by V.A. Shcherbacov in [25].

Important results were obtained by A. Krapez, V. Bakeva, V. Dimitrova, and A. Popovska-Mitrovikj [26-28]. A. Krapez and D. Zivkovic propose to use parastrophic transformations of quasigroups and their modification, which are quite promising for application and research [29]. Cryptanalysis of these ciphers was studied in the dissertation work of Milan Vojvoda [30].

Some generalizations and modifications of the Markovski algorithm can be found in the works of V.A. Shcherbacov and A. Petrescu [31-35]. Further development of the Markovski algorithm is presented by S. Markovski, D. Gligoroski, L. Kocarev, S. J. Knapskog, and M. Hassinen [36-38]; C. Sucheta, K. Pal Saibal, and G. Sugata [39]. Important information about cryptanalysis of some stream ciphers can be found in the article of V.A. Shcherbacov and P. Csorgo [40].

Markovski algorithm has many different generalizations, and it can be used to construct analogues of the ElGamal scheme. An analogue of the ElGamal encryption system based on the Markovski algorithm is given in the works of V.A. Shcherbacov, A.V. Shcherbacov, and N.A. Moldovyan [41]; A.V. Gribov [42].

Cryptographic techniques have become widely used in electronic commerce, telecommunications, and many other environments. These methods are used not only to encrypt transactions and control the production of crypto-currencies, but they also ensure the safe operation of banking systems, plastic cards, ATMs, wireless devices, etc.

Modern cryptography deals with such information security problems as confidentiality, integrity, authentication, the impossibility of denial of authorship by the parties, and key management. The creation of reliable encryption algorithms is the key task of information protection. Therefore, any constructed algorithm must be subjected to careful analysis in order to identify its weaknesses and the possibility of hacking.

The following questions are raised in the thesis:

Problem 1. To investigate and construct algorithms based on the Markovski algorithm using quasigroups and groupoids.

Problem 2. To carry out cryptanalysis of ciphers constructed using generalized algorithms.

Task 1 is discussed in Chapter 2, and Task 2 is solved in Chapters 3 and 4.

The purpose and the objectives of the thesis

The purpose of the scientific research is to build new and improve the already developed cryptographic algorithms based on the Markovski algorithm, carry out their cryptanalysis, and write programs that perform the work of these algorithms.

To achieve this purpose, the following objectives were set:

- Development of an effective cryptographic algorithm based on the Markovski algorithm using left and right binary quasigroups and *n*-ary groupoids;
- Development of programs that implement the work of the constructed algorithms;
- Carrying out attacks on all studied and constructed ciphers;

- Comparative analysis of the attacks carried out;
- Finding texts of the minimum length for all studied types of attacks.

Research hypothesis

The classical Markovski algorithm can serve as a basis for constructing new generalizations based on quasigroups and groupoids that are invertible in one fixed place. The constructed generalized algorithms will have a higher degree of resistance to the known types of attacks. Cryptanalysis of ciphers built by using generalized algorithms is an interesting area of research for cryptanalysts.

Applied methods of research

In this thesis, the analysis of scientific literature and practical experience, systematization of previously obtained results on the research problem, comparison of existing approaches to solving the problems posed, comparison of modern methods of constructing cryptographic algorithms based on non-associative structures and their properties, and in particular, methods of non-associative algebra, including methods for constructing *n*-ary groupoids as well as classical methods of cryptanalysis. The study is based on the use of the classical Markovski algorithm and its generalizations.

The object of the research is generalized Markovski algorithms based on binary quasigroups and n-ary groupoids.

The scientific novelty and originality

All results of the work are new and original. They represent a continuation of previous research in this area. Algorithms were developed and generalized that allowed improving the work of the classical Markovski algorithm; attacks on ciphers were built using generalized algorithms that were studied, and the degree of resistance of these ciphers was shown. The results presented in the dissertation are of interest for study by cryptologists.

The important scientific problem being solved in the research consists in the development of new modifications of the classical algorithm, which contribute to an increase in the resistance of the constructed cipher to the known types of attacks.

The theoretical significance consists in obtaining new improved algorithms and ciphers concerning the application of non-associative structures such as n-ary groupoids in computer science. The developed algorithms made it possible to approach the problems associated with coding and cryptanalysis from a new point of view.

The applicative value of the thesis

New modifications of coding algorithms using left quasigroups, right quasigroups, and invertible in one place n-ary groupoids are proposed. The developed methods made it possible to solve the assigned tasks and indicated the range of further tasks that still have to be solved. The applied value of the work lies in the use of the obtained results in scientific research related to data coding, the study of the efficiency of information presentation, and the cryptanalysis of data. They can also be used in the design of specialized courses for students, masters, and doctoral students related to the study of cryptology on abstract algebraic structures.

The results of the presented dissertation were introduced into the work of the research laboratory "Algebra and its applications" of the Transnistrian State University named after T.G. Shevchenko (Tiraspol).

Thesis publications

The results of the research were published in 21 scientific papers, including 7 scientific articles (2 articles without co-authors), 8 papers in the materials of scientific conferences (6 papers without co-authors), and 6 abstracts at scientific conferences (2 abstracts without co-authors).

The author directly developed mathematical and algorithmic support for encryption and decryption texts built on the basis of generalized Markovski algorithms and also carried out cryptanalysis of all constructed ciphers.

The structure and volume of the thesis

The thesis consists of Introduction, four chapters, general conclusions and recommendations, bibliography of 201 sources, 3 annexes, 217 pages (including 145 pages of the main text), one figure, and 71 tables.

Keywords: Markovski algorithm, quasigroup, left and right quasigroup, translation, plaintext, ciphertext, attack, key, encryption, decryption.

2. CONTENT OF THE THESIS

The structure of the thesis is represented by four chapters, which contain the theoretical and practical results, obtained in the study, and construction of generalizations of the Markovski algorithm, as well as their cryptanalysis.

The introduction formulates the relevance and importance of the research topic, defines the object of the research, formulates the goal and objectives of the research, defines research methods, and reveals the scientific novelty and theoretical and practical significance of the dissertation. The studied scientific problem is presented with an emphasis on the importance of the applied value of the work. The main provisions for the defense are formulated, the information about the approbation and implementation of the results is given. A brief analysis of speeches and publications on the topic of the dissertation is presented. At the end of this section, a summary of the content of the work is provided.

The first chapter – Current situation in the field of use of information technologies in the development of cryptographic and algebraic algorithms – consisting of seven paragraphs, has an introductory character. It provides an overview of the current state of the most important areas of modern cryptography for our work. The basic concepts of cryptology are described, which are necessary for the further presentation of the work. An analysis of one of the most used classifications of cryptographic algorithms is given, and it is noted what conditions modern encryption algorithms must satisfy.

The main features and problems of symmetric and asymmetric encryption are analyzed. The advantages and disadvantages typical for modern symmetric and asymmetric systems are revealed. Special attention is paid to the cryptanalytic methods existing today. A review of the application of non-associative algebraic structures in cryptology is made, in which the main attention is paid to the Markovski algorithm and its generalizations constructed to date.

In the second Chapter – The Markovski algorithm and its new generalizations – we study the operation of the Markovski algorithm for binary quasigroups and the peculiarities of the operation of the algorithm for left and right quasigroups. Generalizations of the Markovski algorithm for invertible groupoids at any one fixed place are constructed. These algorithms were built together with V.A. Shcherbacov. The chapter consists of eight paragraphs, in which objective 1 is achieved.

The first three sections are devoted to the results obtained in the study of the Markovski algorithm in the case of binary quasigroups. It is shown that the algorithm for the left quasigroup does not differ from the traditional Markovski algorithm. A feature in the Markovski algorithm for the right quasigroup is indicated. Programs that implement the work of these algorithms have been written. The resulting programs work to encrypt and decrypt texts of a given length (the length of the text can be easily changed). The programs work for any leaders' values (leaders are chosen by the user). Using these programs, you can build an implementation of the Markovski algorithm for any binary quasigroup.

In addition to binary quasigroups, n-ary quasigroups and their parastrophes can also be used to construct the Markovski algorithm [43, 25].

Paragraph 2.4. of the thesis is dedicated to the construction of Generalized Algorithm 1.

We can define the n-ary operation f as a set Q of $(n+1)$-tuples of the following form $\big(x_1, x_2, \dots, x_n, f(x_1, x_2, \dots, x_n)\big)$, where $x_1, x_2, \dots, x_n, f(x_1, x_2, \dots, x_n) \in Q$.

Definition 2.4.1. *An n-ary groupoid* (Q, f) is a non-empty set Q together with an n-ary operation f which is defined on it.

Definition 2.4.2. n-ary groupoid (Q, f) is called *invertible in the i-th place*, $i = \overline{1,n}$, if the equation $f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n) = a_{n+1}$ has a unique solution for any elements: $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1} \in Q$ [43].

In this case, the operation ${}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n) = x_i$ is defined in a unique way and we have:

$$\left.\begin{array}{l} f\big(a_1, \dots, a_{i-1}, {}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n\big) = a_{n+1} \\ {}^{(i,n+1)}f(a_1, \dots, a_{i-1}, f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n) = x_i \end{array}\right\}. \quad (\mathbf{2.1})$$

Definition 2.4.3. An n-ary groupoid (Q, f) with n-ary operation f such that in the equality $f(x_1, x_2, \dots, x_n) = x_{n+1}$ the fact of knowing any n elements of the set $\{x_1, x_2, \dots, x_n, x_{n+1}\}$ uniquely specifies the remaining one element and that is called *an n -ary quasigroup* [43, 25].

Definition 2.4.4. An n-ary groupoid (Q, f) is called *an n -ary quasigroup* if on set Q, there exist operations ${}^{(1,n+1)}f, {}^{(2,n+1)}f, \dots, {}^{(n,n+1)}f$ such that in algebra $\big(Q, f, {}^{(1,n+1)}f, {}^{(2,n+1)}f, \dots, {}^{(n,n+1)}f\big)$, the following identities are fulfilled for all $i = \overline{1,n}$:

$$\left.\begin{array}{l} f\big(x_1, \dots, x_{i-1}, {}^{(i,n+1)}f(x_1, \dots, x_n), x_{i+1}, \dots, x_n\big) = x_i \\ {}^{(i,n+1)}f(x_1, \dots, x_{i-1}, f(x_1, \dots, x_n), x_{i+1}, \dots, x_n) = x_i \end{array}\right\}. \quad (\mathbf{2.2})$$

It is clear that the number of i-invertible n-groupoids (number n is fixed) is more, then the number of n-ary quasigroups (number n is fixed). This fact served as an impetus for the construction of a new generalizations of the Markovski algorithm.

Algorithm 2.4.5. (Generalized Algorithm 1). Let Q be a non-empty finite alphabet and k be a natural number, $u_j, v_j \in Q, j \in \{1, \dots k\}$. Let us define an n-ary groupoid (Q, f), which is invertible in the i-th place, $i = \overline{1,n}$. Then the groupoid $(Q, {}^{(i,n+1)}f)$ is defined in a unique way.

In this case, the following equality takes place:

${}^{(i,n+1)}f(v_1, \dots, v_{i-1}, v_n, v_i, \dots, v_{n-1}) =$

$= {}^{(i,n+1)}f(v_1, \dots, v_{i-1}, f(v_1, \dots, v_{i-1}, u_n, v_i, \dots, v_{n-1}), v_i, \dots, v_{n-1}) = u_n.$

We take the fixed elements $l_1^{(n-1)^2}\left(l_1, l_2, \dots l_{(n-1)^2} \in Q\right)$, which are called leader elements.

Let $u_1, u_2, \dots u_k$ be a k- tuple of letters from Q.

The following *encryption procedure* is proposed:

$v_1 = f(l_1, l_2, \dots, l_{i-1}, u_1, l_i, \dots, l_{n-1}),$

$v_2 = f(l_n, l_{n+1}, \dots, l_{n+i-2}, u_2, l_{n+i-1}, \dots, l_{2n-2}), \dots,$

$v_{n-1} = f\left(l_{n^2-3n+3}, \dots, l_{n^2-3n+1+i}, u_{n-1}, l_{n^2-3n+2+i}, \dots, l_{(n-1)^2}\right),$

$v_n = f(v_1, \dots, v_{i-1}, u_n, v_i, \dots, v_{n-1}),$

$v_{n+1} = f(v_2, \dots, v_i, u_{n+1}, v_{i+1}, \dots, v_n),$

$v_{n+2} = f(v_3, \dots, v_{i+1}, u_{n+2}, v_{i+2}, \dots, v_{n+1}), \dots .$

The *deciphering algorithm* is constructed similarly to the binary case and has the form:

$u_1 = {}^{(i,n+1)}f(l_1, l_2, \dots, l_{i-1}, v_1, l_i, \dots, l_{n-1}),$

$u_2 = {}^{(i,n+1)}f(l_n, l_{n+1}, \dots, l_{n+i-2}, v_2, l_{n+i-1}, \dots, l_{2n-2}), \dots,$

$u_{n-1} = {}^{(i,n+1)}f(l_{n^2-3n+3}, \dots, l_{n^2-3n+1+i}, v_{n-1}, l_{n^2-3n+2+i}, \dots, l_{(n-1)^2}),$

$u_n = {}^{(i,n+1)}f(v_1, \dots, v_{i-1}, v_n, v_i, \dots, v_{n-1}),$

$u_{n+1} = {}^{(i,n+1)}f(v_2, \dots, v_i, v_{n+1}, v_{i+1}, \dots, v_n),$

$u_{n+2} = {}^{(i,n+1)}f(v_3, \dots, v_{i+1}, v_{n+2}, v_{i+2}, \dots, v_{n+1}), \dots .$

For the groupoid that is invertible in the last place (a special case when $i = n$) , *the encryption algorithm* will take the form:

$v_1 = f(l_1, l_2, \dots, l_{n-1}, u_1),$

$v_2 = f(l_n, l_{n+1}, \dots, l_{2n-2}, u_2), \dots,$

$v_{n-1} = f\left(l_{n^2-3n+3}, \dots, l_{(n-1)^2}, u_{n-1}\right),$

$v_n = f(v_1, \dots, v_{n-1}, u_n),$

$v_{n+1} = f(v_2, \dots, v_n, u_{n+1})$,

$v_{n+2} = f(v_3, \dots, v_{n+1}, u_{n+2}), \dots$.

The deciphering algorithm, in this case, will look like this:

$u_1 = {}^{(n,n+1)}f(l_1, l_2, \dots, l_{n-1}, v_1)$,

$u_2 = {}^{(n,n+1)}f(l_n, l_{n+1}, \dots, l_{2n-2}, v_2), \dots$,

$u_{n-1} = {}^{(n,n+1)}f(l_{n^2-3n+3}, \dots, l_{(n-1)^2}, v_{n-1})$,

$u_n = {}^{(n,n+1)}f(v_1, \dots, v_{n-1}, v_n)$,

$u_{n+1} = {}^{(n,n+1)}f(v_2, \dots, v_n, v_{n+1})$,

$u_{n+2} = {}^{(n,n+1)}f(v_3, \dots, v_{n+1}, v_{n+2}), \dots$.

The software implementation of encryption and decryption using Generalized Algorithm 1 is given in the work. The length of the text is set at the beginning of the program, then the value of the leader elements is entered. An encryption or decryption table is entered for each case individually, after which the processing of plaintext or encrypted text takes place.

Remark 2.4.9. An important condition for the correct operation of the algorithm is the unambiguous specification of the substitution at the site of the invertible operation.

The complexity of the algorithm increases with the growth of the arity of the operation used.

The obtained Generalized Algorithm 1 can be modified, and for this we used translations.

Paragraph 2.5. of the thesis is dedicated to the construction of Generalized Algorithm 2 using translations of various degrees.

A translation of i-invertible n-ary groupoid (Q, f) $(n > 2)$ will be denoted as $T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$, where $a_i \in Q$ for all $i = \overline{1,n}$ and $T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)x = f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$ for all $x \in Q$.

From the definition of i-invertible n-ary groupoid (Q, f), it follows that any translation of n-ary groupoid (Q, f) is a permutation of set Q. The next lemma is true for any value of variable i.

Lemma 2.5.1. If ${}_fT(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$ is a translation of an i-invertible n-ary groupoid (Q, f), then ${}_fT^{-1}(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n) = {}_{(i,n+1)_f}T(a_1, \dots, a_{i-1}, -, a_{i+1}, \dots, a_n)$.

Algorithm 2.5.2. (Generalized Algorithm 2). Let Q be a non-empty finite alphabet and k be a natural number, $u_j, v_j \in Q, j \in \{1, \dots k\}$.

We define an n-ary groupoid (Q, f), which is invertible in i-th place. It is clear that groupoid $(Q, {}^{(i,n+1)}f)$ is defined in a unique way.

We take the fixed elements $l_1^{(n^2-n)/2}$ $\left(l_1, l_2, \dots l_{(n^2-n)/2} \in Q\right)$ as leader elements.

Let $u_1, u_2, \dots u_k$ be a k-tuple of letters from Q and a, b, c, d ... be natural numbers (degrees of translation).

Then we get *the encryption algorithm* of the following form:

$v_1 = T^a(l_1, l_2, \dots, l_{i-2}, l_{i-1}, u_1^a, l_i, \dots, l_{n-1})$,

$v_2 = T^b(l_n, l_{n+1}, \dots, l_{n+i-3}, v_1, u_2^b, l_{n+i-2}, \dots, l_{2n-3})$,

$v_3 = T^c(l_{2n-2}, l_{2n-1}, \dots, l_{2n-i+4}, v_1, v_2, u_3^c, l_{2n-i+3}, \dots, l_{3n-6})$, …,

$v_{n-1} = T^d(l_{(n^2-n)/2}, v_1, \dots, v_{i-2}, u_{n-1}^d, v_{i-1}, \dots, v_{n-2})$,

$v_n = T^e(v_1, v_2, \dots, v_{i-1}, u_n^e, v_i, \dots, v_{n-1})$,

$v_{n+1} = T^f(v_2, v_3, \dots, v_i, u_{n+1}^f, v_{i+1}, \dots, v_n)$, … .

The following notations were used in the algorithm:

$u_1^a = \underbrace{f(f \dots f(l_1, l_2, \dots, l_{i-2}, l_{i-1}, u_1, l_i, \dots, l_{n-1}) \dots)}_{a\ times}$,

$u_2^b = \underbrace{f(f \dots f(l_n, l_{n+1}, \dots, l_{n+i-3}, v_1, u_2, l_{n+i-2}, \dots, l_{2n-3}) \dots)}_{b\ times}$,

$u_3^c = \underbrace{f(f \dots f(l_{2n-2}, l_{2n-1}, \dots, l_{2n-i+4}, v_1, v_2, u_3, l_{2n-i+3}, \dots, l_{3n-6}) \dots)}_{c\ times}$, …,

$u_n^e = \underbrace{f(f \dots f(v_1, v_2, \dots, v_{i-1}, u_n, v_i, \dots, v_{n-1}) \dots)}_{e\ times}$, … .

Taking into consideration Lemma 2.5.1., we can say that the deciphering algorithm can be constructed similar to the deciphering algorithm given for Generalized Algorithm 1 [25].

For an n -ary groupoid invertible in n-th place, *the decryption algorithm* will look as follows:

$u_1 = (T^a)^{-1}(l_1, l_2, \dots, l_{n-1}, v_1)$,

$u_2 = (T^b)^{-1}(l_n, l_{n+1}, \dots, l_{2n-3}, v_1, v_2)$,…,

$u_{n-1} = (T^c)^{-1}(l_{(n^2-n)/2}, v_1, \dots, v_{n-2}, v_{n-1})$,

$u_n = (T^d)^{-1}(v_1, v_2, \dots, v_{n-1}, v_n)$,

$u_{n+1} = (T^e)^{-1}(v_2, v_3, \dots, v_n, v_{n+1})$,

$u_{n+2} = (T^f)^{-1}(v_3, v_4, \dots, v_{n+1}, v_{n+2})$, … .

The features of the generalized algorithms are illustrated by the examples given in the dissertation.

Remark 2.5.6. An important task in Generalized Algorithm 2 is the determination of the inverse translations in the decryption procedure.

The software implementation of encryption and decryption using Generalized Algorithm 2 is given in the work. Comparing the programs for two generalized algorithms leads to the conclusion that the programs for the second algorithm are much more complex and voluminous. The complexity of the programs primarily depends on the degrees of used translations.

If we compare the constructed two algorithms, we see that the total number of necessary leader elements for the first algorithm is $(n-1)^2$, and for the second algorithm, the required number of leader elements is equal to $\frac{(n-1)n}{2}$. The second number is less than the first one by the value $(n-1)\left(\frac{n}{2}-1\right)$.

Generalized Algorithm 2 is much more complicated if we, in addition to the first and the second degree of translation, use the other higher degrees of translation. Of particular interest is the definition of inverse translations for those used in Generalized Algorithm 2. Considering all these differences and features, we can conclude that the second algorithm is of greatest interest for cryptanalysis.

The last two paragraphs of this chapter provide research related to the generalization of the ElGamal scheme based on the Markovski algorithm.

Usually the classical Taher ElGamal encryption system is formulated in the language of number theory using a multiplication modulo prime number [44]. ElGamal's scheme is a public key cryptosystem based on the difficulty of computing discrete logarithms in a finite field.

For the convenience of further presentation, we recall the definition of isotopy, which we used in constructing the generalized ElGamal scheme.

Definition 2.1.6. *Operation B is an isotope of operation A* , if $\exists\ \alpha, \beta, \gamma -$ substitutions for set Q , such as $B(x,y) = \gamma^{-1}A(\alpha x, \beta y) \quad \forall x, y \in Q, T = (\alpha, \beta, \gamma)$ *−isotopy***,** and $\alpha, \beta, \gamma -$ *left, right, and main components of the isotopy*, respectively.

In paragraph 2.7., we considered an analogue of the ElGamal encryption system based on the Markovski algorithm.

Let (Q, f) be a binary quasigroup and $T = (\alpha, \beta, \gamma)$ be its isotopy.

Alice's keys are as follows:

Public key: $(Q, f), T, T^{(m,n,k)} = (\alpha^m, \beta^n, \gamma^k), m, n, k \in \mathbb{N}$, and the Markovski algorithm.

Private key: m, n, k.

Bob's keys are as follows:

Public key: $(Q, f), T, T^{(r,s,t)} = (\alpha^r, \beta^s, \gamma^t), r, s, t \in \mathbb{N}$, and the Markovski algorithm.

Private key: r, s, t.

Encryption.

To send a message $b \in (Q, f)$, Bob calculates $T^{(r,s,t)}$ for the random $r, s, t \in \mathbb{N}$.

Then, knowing $T^{(m,n,k)}$, he computes $T^{(mr,ns,kt)}$ and $(T^{(mr,ns,kt)}(Q, f))$.

To encrypt message b, Bob uses the Markovski algorithm which is known to Alice.

The ciphertext is $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q, f))b)$.

Decryption.

Alice knows m, n, k, so if she gets ciphertext $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q, f))b)$, she calculates $(T^{(mr,ns,kt)}(Q, f))^{-1}$ using $T^{(r,s,t)}$, and finally, she calculates b.

An example of the operation of this scheme is given in the work.

In this algorithm, isostrophy [45] can be used instead of isotopy, algorithm from [25] instead of the Markovski algorithm, and n-ary $(n > 2)$ quasigroups [35] instead of binary quasigroups.

The next step after constructing the algorithm is its cryptanalysis, with the help of which it will be possible to draw conclusions about its reliability and quality.

The **third chapter− Cryptanalysis of some stream ciphers (binary case)** − consisting of five paragraphs, accomplishes the goal that is related to the cryptanalysis of the ciphers constructed in the second chapter using binary quasigroups. This solves objective 2.

For binary quasigroups, M. Vojvoda carried out his attacks, and the author of the thesis shows how these results can be improved (to carry out truncated attacks), in addition, the author offers her modified attacks, which show better results than M. Vojvoda attacks. For each case, the minimum number of characters required for a successful attack is determined. The limiting ratios of the number of symbols used in various types of attacks are analyzed.

M.Vojvoda has given the cryptanalysis of the file encoding system based on binary quasigroups [46, 30] and showed how to break this cipher. The article of M. Vojvoda [46] shows how to break this cipher using an attack with only an encrypted text, and the security issues of the stream cipher under study were discussed. He describes the stream cipher under study, as well as summarizes the results of the cipher studied at that time in the field of cryptanalysis.

In Sections 3.1. and 3.2., it is shown how attacks on chosen plaintext and ciphertext work for binary quasigroups.

First, attacks using the chosen ciphertext were considered.

Assume the cryptanalyst has access to the decryption device loaded with the key. He can then construct the following ciphertext:

$$q_1q_1q_1q_2q_1q_3 \cdots q_1q_n$$
$$q_2q_1q_2q_2q_2q_3 \cdots q_2q_n \cdots$$
$$q_nq_1q_nq_2q_nq_3 \cdots q_nq_n.$$

Then he can enter it into the decryption device.

The decryption device outputs the following plaintext:

$$l\backslash q_1q_1\backslash q_1q_1\backslash q_1q_1\backslash q_1q_2\backslash q_1q_1\backslash q_3 \cdots q_1\backslash q_n$$
$$q_n\backslash q_2q_2\backslash q_1q_1\backslash q_2q_2\backslash q_2q_2\backslash q_2q_2\backslash q_3 \cdots q_2\backslash q_n \cdots$$
$$q_n\backslash q_nq_n\backslash q_1q_1\backslash q_nq_n\backslash q_2q_2\backslash q_nq_n\backslash q_3 \cdots q_n\backslash q_n.$$

As a result, the Cayley table of the operation "\ "defined on Q is completely found and the construction of Cayley table of the operation " $*$ " is straightforward. The ciphertext used in the attack consists of $2n^2$ characters. We have found out that for a complete reconstruction of the Cayley table for the quasigroup $(Q,\backslash)$ it is enough to input only $2n^2 - 4n + 1$ characters instead of $2n^2$. We called this attack the truncated Vojvoda's attack.

Remark 3.1.1. Comparing the number of characters used in the attack of Vojvoda and the truncated attack of Vojvoda, we have the following limiting relation:

$$\lim_{n\to\infty} \frac{2n^2}{2n^2 - 4n + 1} = 1.$$

We propose to consider a new type of attack, which we will call a modified attack. It uses the following text in the decryption procedure:

$$q_1q_1q_2q_2q_3q_3 \cdots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3 \cdots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3 \cdots q_nq_{n-2}q_1q_{n-1}q_2q_n \cdots .$$

The last character depends on the parity of the order of the quasigroup, namely, if n is an odd number, then the last operation is $q_k\backslash q_n$, where $k = \left[\frac{n}{2}\right] + 1$. If n is an even number, then the last operation is $q_{\frac{n}{2}}\backslash q_n$. The presented attack requires $n^2 - 2(n-1)$ operations "\". And, what is important, this number does not depend on the leader element.

Remark 3.1.2. Comparing the number of characters used in the attack of Vojvoda, the truncated attack of Vojvoda and the modified attack, we have the following limiting ratios:

$$\lim_{n\to\infty} \frac{2n^2}{n^2-2n+2} = 2 \text{ and } \lim_{n\to\infty} \frac{2n^2-4n+1}{n^2-2n+2} = 2.$$

If we compare this result with the result obtained in Remark 3.1.1, we see a clear advantage of the modified attack.

After the chosen ciphertext attacks, we moved on to consideration of chosen plaintext attacks, which have their own distinctive features.

Suppose a cryptanalyst has access to an encryption device with an unknown key. In M. Vojvoda's work [47], the following text is built for encryption:

$$q_1q_1; q_1q_2; q_1q_3; \dots q_1q_n;$$
$$q_2q_1; q_2q_2; q_2q_3; \dots q_2q_n; \dots$$
$$q_nq_1; q_nq_2; q_nq_3; \dots q_nq_n.$$

This text is entered into the encryption device discretely by 2 characters. Thanks to this input, we have the following ciphertext:

$$l * q_1 \quad (l * q_1) * q_1; l * q_1 \quad (l * q_1) * q_2; \dots l * q_1 \quad (l * q_1) * q_n;$$
$$l * q_2 \quad (l * q_2) * q_1; l * q_2 \quad (l * q_2) * q_2; \dots l * q_2 \quad (l * q_2) * q_n; \dots$$
$$l * q_n \quad (l * q_n) * q_1; l * q_n \quad (l * q_n) * q_2; \dots l * q_n \quad (l * q_n) * q_n.$$

The plaintext used in the attack consists of $2n^2$ characters divided into pairs. However, a shorter encrypted text consisting of $2(n-1)^2$ characters can be constructed (truncated attack of Vojvoda).

The output that is line by line at an odd position is the line number, and at an even position – is the element of the quasigroup $(Q, *)$. The advantage of these attacks is that they do not depend on the leader used.

Now consider the option when characters are launched into the encryption device by the stream, namely as in the case of an attack with the chosen ciphertext:

$$q_1\ q_1\ q_1\ q_2\ q_1\ q_3 \dots q_1\ q_n$$
$$q_2\ q_1\ q_2\ q_2\ q_2\ q_3 \dots q_2\ q_n \dots$$
$$q_nq_1\ q_nq_2\ q_nq_3 \dots q_nq_n \dots .$$

We called this attack a stream attack of Vojvoda. In this attack, the number of characters used is less than in the previous two attacks, but the result depends on the leader element. This is the disadvantage of a stream attack.

For each case, it is possible to choose a streaming attack with a minimum number of characters, but this task is quite difficult. For a quasigroup of order n, the necessary minimum number of characters is $n(n-2)+2$.

Now we consider a modified attack using the chosen plaintext with a discrete input of characters:

$$q_1q_1; q_2q_2; q_3q_3; \dots q_{n-2}q_{n-2}; q_{n-1}q_{n-1}; q_nq_n;$$
$$q_2q_1; q_3q_2; q_4q_3; \dots q_{n-1}q_{n-2}; q_nq_{n-1}\ ; q_1q_n;$$
$$q_3q_1; q_4q_2; q_5q_3; \dots q_nq_{n-2}; q_1q_{n-1}; q_2q_n \dots .$$

The plaintext used in this attack consists of $2(n-1)^2$ characters divided into pairs. The result of the modified attack coincided with the result of the truncated Vojvoda attack. Thus, even in the binary case, when carrying out attacks with a chosen ciphertext or chosen plaintext, the number of characters used can be reduced.

We considered the modifications of crypto attacks, built by M. Vojvoda for quasigroups, conducted the comparative analysis, and identified positive and negative points of these attacks.

In the paragraphs 3.3. and 3.4., it is shown how attacks on chosen plaintext and on chosen ciphertext work for left and right quasigroups.

First, attacks using the chosen ciphertext were considered. We present the results of these attacks.

For a complete reconstruction of the Cayley table for the left quasigroup $(Q,\ \backslash)$, it suffices to input only $2n^2-2n+1$ characters at the input instead of $2n^2$. This is a truncated attack.

We offered a modified attack. If we run the following text on the decoder,

$$q_1q_1q_2q_2q_3q_3 \cdots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3 \cdots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3 \cdots q_nq_{n-2}q_1q_{n-1}q_2q_n \cdots,$$

the last character depends on the parity of the order of the quasigroup, namely, if n is an odd number, then the last operation is $q_n\backslash q_k$,where $k=\left[\frac{n}{2}\right]+1$. If n is an even number, then the last operation is $q_n\backslash q_{\frac{n}{2}+1}$.

The presented attack requires: $n^2-2\left(n-1-\left[\frac{n}{2}\right]\right)$ operations " \". In comparison with the attack of Vojvoda, the number of used characters is significantly reduced.

Next, we considered attacks with a chosen plaintext for left quasigroups. The plaintext used in the M. Vojvoda attack consists of $2n^2$ characters divided into pairs. However, a shorter text consisting of $2n^2-2n$ characters can be constructed. In the case of discrete character input, the results of the truncated attack and the modified attack are the same. When considering a streaming attack with a chosen plaintext, the result depends on the leader element used.

The best result is obtained using a modified streaming attack. In this attack, the number of characters used is $(n-1)n+1$, where n is the order of the left quasigroup used for encryption.

The results obtained from chosen ciphertext and chosen plaintext attacks on a generalized Markovski cipher based on right quasigroups are similar to those with left quasigroups.

The work of all the given attacks is illustrated by a number of examples.

The **fourth chapter− Cryptanalysis of some stream ciphers (n-ary case),** consisting of three paragraphs, accomplishes the goal that is related to the cryptanalysis of ciphers constructed using the generalized Markovski algorithm which is based on i-invertible n-ary groupoids, namely the cryptanalysis of ciphers based on Generalized Algorithm 1. This solves objective 2.

In Section 4.1., we investigated attacks with a chosen ciphertext built on the basis of i-invertible n-ary groupoid using Generalized Algorithm 1. Modifications of these attacks are presented. The required number of characters was found to carry out a successful attack with the chosen ciphertext. For a number of cases, examples of minimal texts are provided. Conclusions are drawn from all the attacks and studies carried out. Let us take a look at the most important ones.

Assume the cryptanalyst has an access to the decryption device loaded with the key. He can then construct the following ciphertext, where n is arity and m is the order of an i-invertible groupoid:

$$\underbrace{q_1q_1\cdots q_1q_1}_{n\ times}\underbrace{q_1q_1\cdots q_1q_2}\cdots\underbrace{q_1q_m\cdots q_mq_m}$$

$$\underbrace{q_2q_1\cdots q_1q_1}\underbrace{q_2q_1\cdots q_1q_2}\cdots\underbrace{q_2q_m\cdots q_mq_m}$$

$$\underbrace{q_3q_1\cdots q_1q_1}\underbrace{q_3q_1\cdots q_1q_2}\cdots\underbrace{q_3q_m\cdots q_mq_m}\cdots .$$

Then he enters it into the decryption device.

This text is a generalized version of the text used by M. Vojvoda for binary quasigroups.

For a complete reconstruction of the table of values of the operation ${}^{(i,n+1)}f$, and hence the table of values of the operation f, it is sufficient to submit at the input $(n\cdot m^{n-1}+1)(m-1)$ characters to get all the values.

It was possible to determine the length of the minimum required text and for a number of cases to construct such texts. For example, for the case $n=m=3$, we needed 56 characters to completely restore the table of values of the function ${}^{(i,4)}f$.

We improved this result and proposed the following text to be entered into the decryption device:

$$q_1q_1q_1q_2q_2q_2q_3q_3q_3 \quad 000111222$$
$$q_2q_1q_1q_3q_2q_2\ q_1q_3q_3 \quad \text{or} \quad 100211022$$
$$q_1q_2q_1q_2q_3q_2q_3q_1q_3 \quad 010121202$$
$$q_1q_1 \quad 00.$$

The output received 29 characters, which is enough to completely restore all the values of the function ${}^{(i,4)}f$.

So, the minimum number of characters in a modified attack will be $m^n + (n-1)$.

As a result of these two attacks, we manage to restore all the values of the decryption function. The main problem of the modified attack is the selection of optimal texts for groupoids of different degrees and orders.

It should be noted that for the values of the function f and its inverse function ${}^{(i,n+1)}f$ on the set $(q_{j_1}, q_{j_2}, \dots q_{j_{i-1}}, q_i, q_{j_{i+1}}, \dots q_{j_n})$, where the elements $q_{j_1}, q_{j_2}, \dots q_{j_{i-1}}, q_{j_{i+1}}, \dots q_{j_n}$ are chosen from the set $\{q_1, q_2, \dots q_m\}$ and are the fixed elements, for different values of the element q_i, the corresponding functions cannot take the same values. So, for each such fixed set, it is enough to determine the $m-1$ value of the corresponding function, and then the last value will be found automatically. Taking into account this remark, the built text will have the length: $m^{n-1} \cdot (m-1)$.

However, there are two features of this text that should be noted:

1) Determining the values of the remaining functions (m^{n-1} values are left) is a more difficult task than in the case of working with binary quasigroups;

2) For the case when $n = m = 3$, we have selected such a text, but will it be possible to select a similar text in other cases? And will it be possible to find the general form of such a text, or will it be different for each case?

For example, for the case $n = m = 3$, to restore the table of values of the operation ${}^{(i,4)}f$, it is enough to input 20 characters (to restore 18 values out of 27):

$$q_1q_1q_1q_2q_2q_2q_3q_3q_3 \quad 000111222$$
$$q_2q_1q_2q_1q_3q_1q_3q_2q_3 \quad \text{or} \quad 101020212$$
$$q_1q_2 \quad 01.$$

This text has the smallest length for the case $n = m = 3$. A feature of this attack is that we do not get all the values of the function, but only a sufficient number of characters to restore the entire table.

Now suppose that the key is hacked and we need to hack the decrypted text. The situation will be as follows: the first $(n-1)$ characters containing leaders can take on any values, and all other characters will be determined by them. Therefore, the possible options of deciphered texts will be m^n.

In Paragraph 4.2., we considered the attacks with chosen plaintext constructed using an n-ary groupoid, which is invertible in the i-th place, obtained using Generalized Algorithm 1. A feature of such attacks is that it is impossible to choose the optimal version of the general text for all of them.

Assume the cryptanalyst has an access to the encryption device loaded with the key. He can then construct the following plaintext (n is arity and m is the order of an i-invertible groupoid):

$$\underbrace{q_1q_1\cdots q_1q_1}_{n\ times}\underbrace{q_1q_1\cdots q_1q_2}\cdots\underbrace{q_1q_1\cdots q_1q_m}$$

$$\underbrace{q_1q_1\cdots q_2q_1}\underbrace{q_1q_1\cdots q_2q_2}\cdots\underbrace{q_1q_1\cdots q_2q_m}$$

$$\underbrace{q_1q_1\cdots q_3q_1}\underbrace{q_1q_1\cdots q_3q_2}\cdots\underbrace{q_1q_1\cdots q_3q_m}\cdots$$

$$\underbrace{q_1q_1\cdots q_mq_1}\underbrace{q_1q_1\cdots q_mq_2}\cdots\underbrace{q_1q_1\cdots q_mq_m}\cdots.$$

Then he enters it into the encryption device.

The number of characters required to restore the encryption table depends on the values of the chosen leader elements. Therefore, the question of determining the length of the used plaintext in each case is decided individually. The work of this type of attack is illustrated by several examples.

In conclusion, I would like to say a few words about the cryptanalysis of ciphers built on the basis of Generalized Algorithm 2. This cryptanalysis is a very difficult task, due to the fact that we do not know the degree of translations used in the algorithm. This again indicates that Generalized Algorithm 2 is more resistant to cryptanalysis than Generalized Algorithm 1.

Considering the research done, we can conclude that both generalized algorithms are of great interest for use in cryptography.

3. GENERAL CONCLUSIONS AND RECOMMENDATIONS

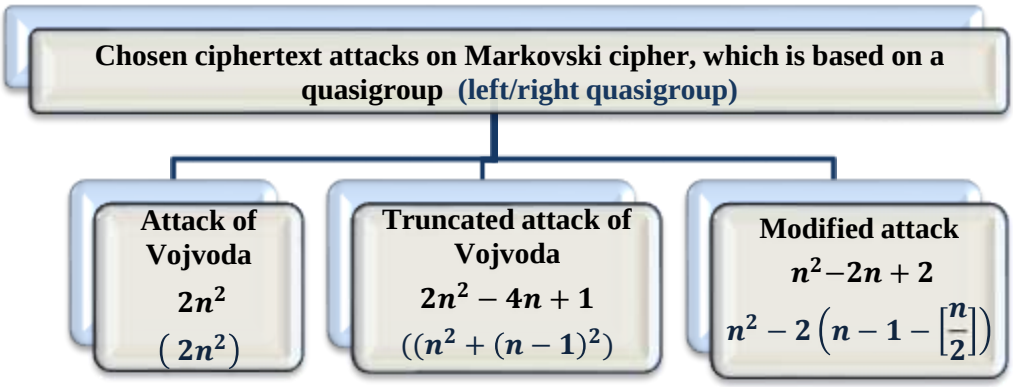
The research carried out within the Ph.D. thesis " **The use of information technologies in the development of cryptographic and algebraic algorithms**" fully corresponds to the goal and the objectives set out in the introduction chapter.

The main results of the work are new and original. We developed and generalized algorithms that allowed improving the work of the classical Markovski algorithm; the attacks on the constructed ciphers were studied, and the degree of resistance of these ciphers was shown.

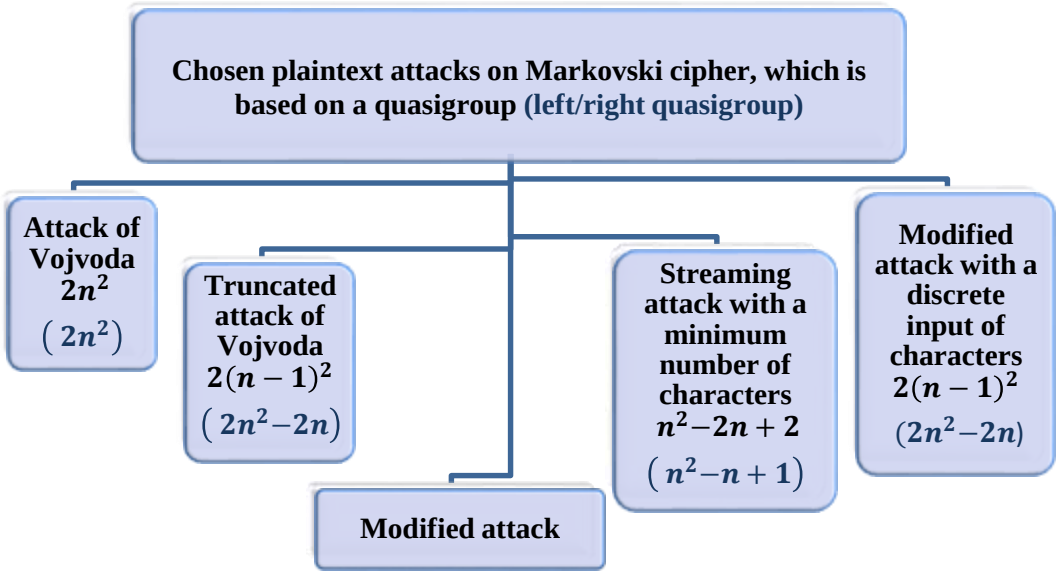
The theoretical significance of the thesis is determined by obtaining new algorithms and ciphers, built by using non-associative structures such as n-ary groupoids and quasigroups. The applied value of the dissertation lies in the use of the obtained results in coding theory and cryptanalysis.

The analysis of the obtained results allows us to highlight the following general results:

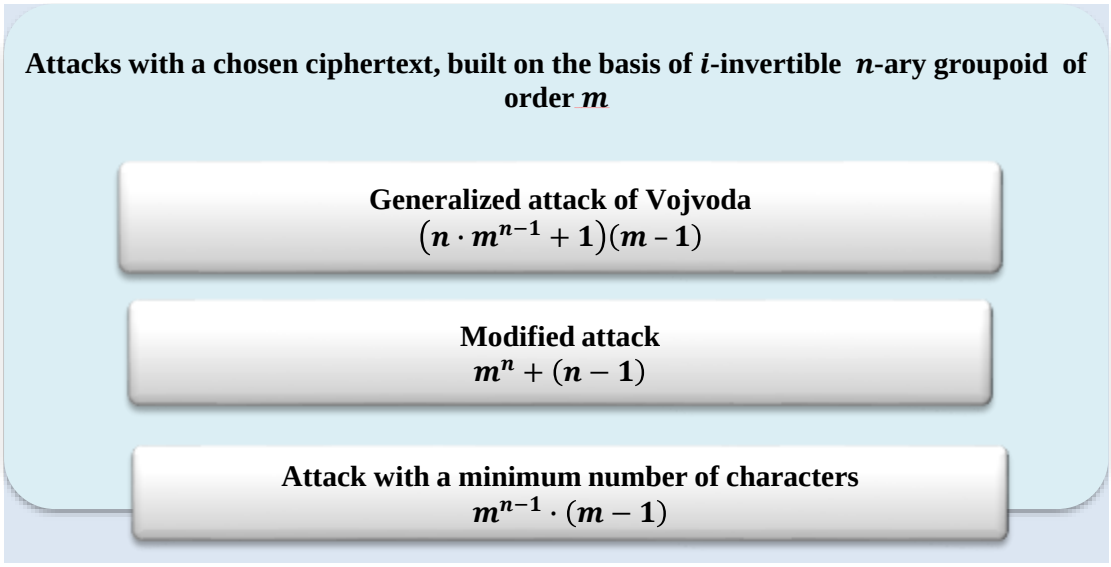
1. The key task of protecting information is to create strong encryption algorithms; so, any newly constructed algorithm must be subjected to careful analysis in order to identify its weaknesses and the possibility of breaking.
2. The use of quasigroups in cryptology shows better possibilities and results than the use of associative systems.
3. Generalized Markovski algorithms for left and right quasigroups and programs for their implementation have been developed (Annex 2), and these algorithms have their own characteristics and advantages.
4. Chosen ciphertext attacks were carried out on Markovski ciphers constructed by using quasigroups (left and right quasigroups); a comparative analysis was carried out; positive and negative aspects of these attacks were identified, and new modified attacks with improved results were proposed. The texts of the minimum length for each attack were selected.



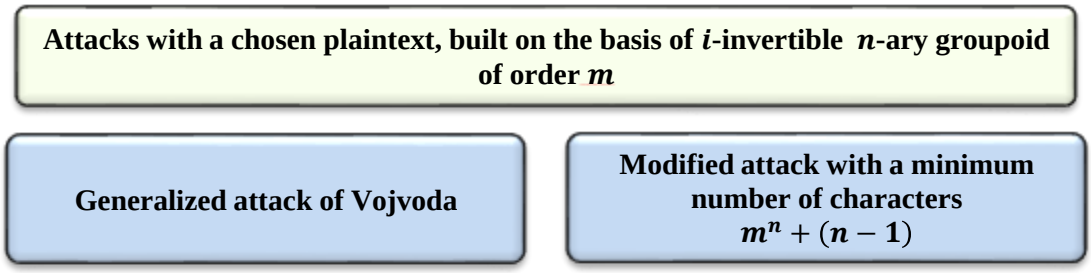
5. Chosen plaintext attacks were carried out on Markovski ciphers constructed by using quasigroups; positive and negative aspects of these attacks were identified, and new modified attacks with improved results were proposed. For streaming attacks of a chosen plaintext, the minimum required number of characters is determined to completely restore the encryption quasigroup table (the text depends on the used leader element).



6. A generalized Markovski algorithm for an n-ary groupoid invertible in one fixed place was constructed, Generalized Algorithm 1; and programs were written that implement the work of this algorithm.
7. The attacks were described using the chosen ciphertext on a cipher obtained by using the generalized Markovski algorithm (Generalized Algorithm 1).



8. An attack on the ciphertext can be carried out by exhaustive enumeration of all values of the functions in which the leader elements appear. The total number of these values is $\boldsymbol{m^{n-1}}$.
9. The attacks were described using the chosen plaintext on a cipher obtained by using the generalized Markovski algorithm (Generalized Algorithm 1).



10. For the third and fourth order groupoids, texts of the shortest length were built, but in each case, they are selected individually. The selection of such a text is a difficult task.
11. A generalized Markovski algorithm for an n-ary groupoid invertible in one fixed place was constructed using translations of any degrees, Generalized Algorithm 2; and programs were written that implement the work of this algorithm.
12. The total number of necessary leader elements for the first algorithm is $\boldsymbol{(n-1)^2}$, and for the second algorithm, the required number of leader elements is equal to $\frac{(n-1)n}{2}$. The second number is less than the first one by the value $\boldsymbol{(n-1)\left(\frac{n}{2}-1\right)}$. This suggests the advantage of the second algorithm against the first one (especially with the growth of the number n).
13. Generalized Algorithm 2 is much more complicated if we, in addition to the first and second degrees of translation, use the third, fourth, and the other higher degrees of translation. Of particular interest is the definition of inverse translations for those used in Generalized Algorithm 2.
14. An analysis of all developed programs was carried out, which includes an assessment of the most important parameters (among them: the length of the text, the algorithm used, the number of leader elements required, the average data processing speed, and the estimation of the algorithm complexity using the Big-O concept). As a result, it was concluded that the programs work successfully and have positive characteristics.

15. We considered an analogue of the ElGamal encryption system based on the Markovski algorithm; and its features were studied. New modifications are planned for it. Cryptanalysis of this generalized scheme is a complex problem that needs to be solved.

The proposed elaborations have a significant scientific value due to their high degree of novelty and originality. The results obtained in this thesis have a theoretical and applicative value in such domains as algebra, cryptology, and computer science.

Recommendations:

1. Of particular interest is the continuation of the application of the Markovski algorithm in coding theory, and especially in cryptography.
2. Research on the topic of the thesis can be continued both from algebraic and applicative points of view. Of particular interest is the study of the possibilities of using quasigroups and other non-associative systems in cryptology and coding theory.
3. The constructed algorithms can be used in banking information systems, as well as in the development of various banking products, as an additional protection that increases the reliability and durability of these systems and products (for example, in modern plastic cards).
4. The obtained results can be used to develop algebraic and cryptographic algorithms in various fields of informatics.
5. The contents of the thesis can serve as the basis for the development of special courses for doctoral and master's students.

REFERENCES

[1] MAGLIVERAS, STINSON and VAN TRUNG, T. New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trapdoors in Finite Groups. In: *J. Cryptology*. 2002, vol.15, no.4, pp. 285-297. ISSN 1432-1378.

[2] DEHORNOY, P. Braid-based cryptography. In: *Contemporary Mathematics, Group Theory, Statistics, and Cryptography*. 2004, vol. 360, pp. 5-33. ISBN 978-0-8218-3444-2.

[3] DENES, J. and KEEDWELL, A. D. Some applications of non-associative algebraic systems in cryptology. In: *Pure Mathematics and Applications*. 2001, vol. 12(2), pp.147-195. ISSN 1218-4586.

[4] KOSCIELNY, Cz. $NLPN$ Sequences over $GF(q)$. In: *Quasigroups and Related Systems*. 1997, vol.4, no.1, pp. 89-102. ISSN 1561-2848.

[5] DENES, J. and KEEDWELL, A. D. Latin Squares and their Applications. In: *Bulletin of the American mathematical society*. 1976, vol.82, no.3, pp. 468-471. ISSN 0273-0979.

[6] DENES, J. and KEEDWELL, A.D. Latin squares: New Developments in the Theory and Applications. In: *Annals of Discrete mathematics*. 1991, North-Holland, vol. 46, pp. 1-469. ISSN 0167-5060. ISBN 0 444 88899 3.

[7] DENES, J. On Latin squares and a digital encrypting communication system. In: *P.U.M.A., Pure Mathematics and Applications,* Department of Mathematics, Corvinus University of Budapest. 2000, vol. 11, iss.4, pp.559-563. ISSN 1218-4586.

[8] KALKA, A. *Non-associative public-key cryptography*. 2012. 32 p. [Online]. Available: https://arxiv.org/pdf/1210.8270.pdf

[9] ТУЖИЛИН, М. Э. Латинские квадраты и их применение в криптографии. В: *Прикладная дискретная математика, Математические методы криптографии*. 2012, №3(17), с. 47-52. ISSN 2311-2263 (Online).

[10] МОВСИСЯН, Ю. Сверхтождества в алгебрах и многообразиях. В: *Успехи математических наук*. 1998, том 53, выпуск 1(319), с. 61-114. ISSN 0042-1316.

[11] ГРИБОВ, А.В., ЗОЛОТЫХ, П.А., МИХАЛЕВ, А.В. Построение алгебраической криптосистемы над квазигрупповым кольцом. В: *Математические вопросы криптографии*. 2010, том 1, выпуск 4, с. 23-32. ISSN 2220-2617.

[12] MAZE, G., MONICO, C. and ROSENTHAL, J. Public key cryptography based on semigroup actions. In: *Advances in Mathematics of Communications*. 2007, vol.1, no.4, pp.489-507. ISSN 1930-5346.

[13] SHPILRAIN, V. and USHAKOV, A. Thompson's Group and Public Key Cryptography. In: *Applied Cryptography and Network Security*, ACNS, Lecture Notes in Computer Science, Springer. 2005, vol. 3531, pp.151-163. ISBN 978-3-540-26223-7. ISSN 0302-9743.

[14] ATANI, R.E., ATANI, SH.E. and MIRZAKUCHAKI, S. Public Key Cryptography Based on Semimodules over Quotient Semirings. In: *International Mathematical Forum*. 2007, vol.2, no.52, pp.2561-2570. ISSN 1312-7594.

[15] KRAPEZ, A. Cryptographically Suitable Quasigroups via Functional Equations. In: *ICT Innovations 2012*, Advances in Intelligent Systems and Computing. 2013, vol. 207, pp. 265-274. ISSN 1857-7288.

[16] KRAPEZ, A. ŠEŠELJA, B., TEPAVČEVIĆ, A. Solving linear equations by fuzzy quasigroups techniques. In: *Information Sciences*. 2019, vol. 491, pp.179-189. ISSN 0020-0255.

[17] MEYER, K. A. *A New Message Authentication Code Based on the Non-Associativity of Quasigroups*: PhD thesis of doctor of philosophy. Iowa State University, 2006. 91 p.

[18] ARTAMONOV, V. Applications of quasigroups to cryprography. In: *Sarajevo Journal of Mathematics.* 2018, vol.14 (27), no.2, pp. 191–205. ISSN 1840-0655.

[19] ARTAMONOV, V., CHAKRABARTI, S., MARKOV, V., PAL, S. Constructions of polynomially complete quasigroups of arbitrary order. In: *Journal of Algebra and Its Applications.* 2020, vol.20, no.12, 2150236. ISSN 0219-4988.

[20] KOSCIELNY, Cz. and MULLEN, G.L. A quasigroup-based public-key cryptosystem. In: *International Journal of Applied Mathematics and Computer Science*. 1999, vol.9, no.4, pp. 955-963. ISSN 1641-876X.

[21] OCHODKOVA, E. and SNASEL, V. Using quasigroups for secure encoding of file system. In: *Proceedings of the Conference Security and Protection of Information*, Abstract of Talks, Military Academy in Brno. 2001, pp. 175-181. ISBN 8085960281.

[22] MARKOVSKI, S., GLIGOROSKI, D. and STOJCEVSKA, B. Secure two-way on-line communication by using quasigroup enciphering with almost public key. In: *Novi Sad Journal of Mathematics*. 2000, vol. 30, iss.2, pp. 43-49. ISSN 0352-0900.

[23] MARKOVSKI, S., GLIGOROSKI, D. and BAKEVA, V. Quasigroup string processing: Part 1. In: *Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci*. XX (1-2). 1999, pp.13-28. ISSN 1857-9027.

[24] MARKOVSKI, S., DIMITROVA, V., TRAJCHESKA, Z., PETKOVSKA, M., KOSTADINOSKI, M., BUHOV, D. Block cipher defined by matrix presentation of quasigroups. In: *IACR Cryptology ePrint Archive*. 2021, vol. 2021/ 1512, 3 p.

[25] SHCHERBACOV, V.A. *Elements of Quasigroup Theory and Applications*. 1st ed: Chapman and Hall/CRC, 2017. 598 p. ISBN 9781315120058.

[26] BAKEVA, V. and DIMITROVA, V. Some probabilistic properties of quasigroup processed strings useful in cryptanalysis. In: *Communications in Computer and Information Science*. 2011, vol.83, pp. 61-70. ISSN 1865-0929.

[27] BAKEVA, V., DIMITROVA, V. and POPOVSKA-MITROVIKJ, A. Parastrophic quasigroup string processing. In: *Proceedings of the 8th Conference on Informatics and Information Technologies with International Participation*, 2011, Bitola, Macedonia, pp.19-21.

[28] DIMITROVA, V., BAKEVA, V., POPOVSKA-MITROVIKJ, A. and KRAPEZ, A. Classifications of quasigroups of order 4 by parastrophic quasigroups tranformation. In: *The International Mathematical Conference on Quasigroups and Loops, LOOPS'11*, Booklet of Abstracts, Trest, Czech Republic, 2011, p.6.

[29] KRAPEZ, A. and ZIVKOVIC, D. Parastrophically equivalent quasigroup equations. In: *Publications de l'Institut Mathématique*, Nouvelle Série, Beograd. 2010, vol.87(101), pp.39-58. ISSN 0350-1302.

[30] VOJVODA, M. *Stream Ciphers and Hash Functions: Analysis of Some New Design Approaches*: PhD thesis in technical sciences. Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Bratislava, Slovak Republic, 2004. 94 p

[31] SHCHERBACOV, V.A., *Elements of quasigroup theory and some its applications in code theory and cryptology*, 2003. 85 p. [online]. Available: https://www2.karlin.mff.cuni.cz/~drapal/speccurs.pdf

[32] SHCHERBACOV, V.A. *On some known possible applications of quasigroups in cryptology*, 2003. 15 p. [online]. Available: https://www2.karlin.mff.cuni.cz/~drapal/krypto.pdf

[33] PETRESCU, A. Applications of quasigroups in cryptography. In: *Interdisciplinarity in Engineering Scientific International Conference Tg. Mures*-Romania, 15-16 November, 2007, 5 p. ISSN 2285-0945.

[34] PETRESCU, A. n -Quasigroup cryptographic primitives: Stream ciphers. In: *Studia Universitatis Babeş-Bolyai Informatica*. 2010, vol. LV, iss.2, pp. 27-34. ISSN 1224-869X.

[35] SHCHERBACOV, V.A. Quasigroups in cryptology. In: *Computer Science Journal of Moldova*. 2009, vol.17, no.2(50), pp. 193-228. ISSN 1561-4042.

[36] GLIGOROSKI, D., MARKOVSKI, S. and KOCAREV, L. Edon-R, an infinite family of cryptographic hash functions. In: *International Journal of Network Security*. 2009, vol.8, no.3, pp.293-300. ISSN 1816-353X.

[37] GLIGOROSKI, D., MARKOVSKI, S. and KNAPSKOG, S. J. *A public key block cipher based on multivariate quadratic quasigroups*, 2008. 22 p. [Online]. https://arxiv.org/abs/0808.0247

[38] HASSINEN, M. and MARKOVSKI, S. Secure SMS messaging using Quasigroup encryption and Java SMS API. In: *Proceedings of the Eighth Symposium on Programming Languages and Software Tools SPLST'03*, June 17-18, 2003, Kuopio, Finland, pp.187-200.

[39] SUCHETA, C., SAIBAL, K. P. and SUGATA, G. An Improved 3-Quasigroup based Encryption Scheme. In: *ICT Innovations 2012, Secure and Intelligent Systems*, Web Proceedings, 2012, Ohrid, Macedonia, pp.173-184. ISSN 1857-7288.

[40] CSORGO, P., SHCHERBACOV, V. *On some quasigroup cryptographical primitives*, 2011. 11 p. [online]. https://arxiv.org/abs/1110.6591

[41] MOLDOVYAN, N.A., SHCHERBACOV, A.V and SHCHERBACOV, V.A. On some applications of quasigroups in cryptology. In: *Proceedings of the Workshop on Foundations of Informatics FOI-2015*, August 24-29, 2015, Chisinau, Republic of Moldova. pp.331-341. ISBN 978-9975-4237-3-1.

[42] ГРИБОВ, А.В. *Алгебраические неассоциативные структуры и их приложения в криптологии*: кандидатская диссертация, кандидата физико-математических наук, МГУ, Москва, 2015. 93 с.

[43] БЕЛОУСОВ, В.Д. *n-арные квазигруппы*. Кишинев: Штиинца, 1972. 225 с.

[44] ELGAMAL, T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: *IEEE Transactions on Information Theory*. 1985, vol.31, no.4, pp. 469-472. ISSN 0018-9448.

[45] SHCHERBACOV, V.A. On the structure of left and right F-, SM- and E-quasigroups. In: *Journal of Generalized Lie Theory and Applications*. 2009, vol. 3, no.3, pp.197-259. ISSN 1736-5279.

[46] VOJVODA, M. Cryptanalysis of a file encoding system based on quasigroup. In: *Journal of Electrical Engineering*. 2003, vol.54, no.12. ISSN 1335-3632.

[47] VOJVODA, M. *Attacks on a file encryption system based on quasigroup*. In: *Proceedings of Elitech 2003*, Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology,2003, Bratislava, Slovak Republic, pp. 54-56.

ANNOTATION

Malyutina Nadezhda: "The use of information technologies in the development of cryptographic and algebraic algorithms"

PhD Thesis in Computer Science, Chisinau, 2023

Thesis structure: the thesis consists of Introduction, four main chapters, general conclusions and recommendations, bibliography of 201 sources, and 3 annexes. The thesis contains 145 pages of the main text, one figure, and 71 tables. The obtained results were published in 21 scientific works.

Keywords: Markovski algorithm, quasigroup, left and right quasigroup, translation, plaintext, ciphertext, attack, key, encryption, decryption.

The purpose of the thesis: construction of new modifications and improvement of already developed cryptographic algorithms and their cryptanalysis.

The objectives of the work: 1. Development of an effective cryptographic algorithm based on the Markovski algorithm using n-ary groupoids; 2. Writing programs that perform the work of the constructed algorithms; 3. Carrying out attacks on all built ciphers; 4. Comparative analysis of the attacks carried out; 5. Finding texts of the minimum length for all investigated types of attacks.

The scientific novelty and originality: the main results of the work are new and original. They are a continuation of previous research in this area. Algorithms were developed and generalized that allowed us improving the work of the classical Markovski algorithm, the attacks on the constructed ciphers were studied, and the degree of resistance of these ciphers was shown.

The important scientific problem being solved in the research: it consists in the development of new generalizations of the classical algorithm, which contribute to an increase in the resistance of the constructed cipher to known types of attacks.

The theoretical significance of the thesis: is determined by obtaining new algorithms and ciphers built using non-associative structures such as n-ary groupoids. New generalizations of coding algorithms using left and right quasigroups, n-ary groupoids invertible in one fixed place are developed.

The applicative value of the thesis: it lies in the use of the obtained results in coding theory and cryptanalysis.

The implementation of the scientific results: the results obtained can be used in scientific research related to data coding, study of the efficiency of information presentation, and data cryptanalysis. They can also be used in the design of an elective course for university students related to the study of cryptology on abstract algebraic structures.

ADNOTARE

Maliutina Nadejda: "Utilizarea tehnologiilor informaționale la elaborarea algoritmilor criptografici și algebrici"

Teză de doctor în informatică, Chișinău, 2023

Structura tezei: teza constă din introducere, patru capitole, concluzii generale și recomandări, bibliografie din 201 titluri și 3 anexe. Teza conține 145 pagini de text de bază, o figură și 71 tabele. Rezultatele obținute sunt publicate în 21 lucrări ştiinţifice.

Cuvinte-cheie: algoritm Markovski, cvazigrup, cvazigrup de stânga și de dreapta, translație, text deschis, text cifrat, atac, cheie, criptare, decriptare.

Scopul lucrării: construirea noilor și îmbunătățirea algoritmilor criptografici deja construiți și a criptoanalizei acestora.

Obiectivele cercetării: 1. Dezvoltarea unui algoritm criptografic eficient bazat pe algoritmul Markovski folosind grupoizi n-ari; 2. Elaborarea programelor, care implementează lucrul algoritmi construiti; 3. Efectuarea atacurilor asupra tuturor cifrurilor construite; 4. Analiza comparativă a atacurilor comise; 5. Găsirea textelor de lungime minimă pentru toate tipurile de atacuri investigate.

Noutatea și originalitatea științifică: Rezultatele lucrării sunt noi și originale. Ele sunt o continuare a cercetărilor anterioare în acest domeniu. Au fost dezvoltați și generalizați algoritmi, care au permis îmbunătățirea activității algoritmului clasic Markovski, au fost studiate atacurile asupra cifrurilor construite și a fost arătat gradul de rezistență al acestor cifruri.

Rezultatul obținut care contribuie la soluționarea unei probleme ştiinţifice importante: constă în dezvoltarea noilor generalizări ale algoritmului clasic care cresc rezistența cifrului construit la tipuri cunoscute de atacuri.

Semnificația teoretică a lucrării: este determinată prin obținerea noilor algoritmi și cifrurilor construite, folosind structuri neasociative precum grupoizii n-ari. Sunt dezvoltate noi generalizări ale algoritmilor de codare folosind cvazigrupuri de stânga și de dreapta, grupoizi n-ari inversabili la un loc fixat.

Valoarea aplicativă: constă în utilizarea rezultatelor obținute în teoria codificării și criptoanaliză.

Implementarea rezultatelor ştiinţifice: rezultatele obținute pot fi utilizate în cercetările științifice legate de codificarea datelor, studierea eficienței prezentării informațiilor și criptoanaliza datelor. Ele pot fi utilizate și în proiectarea unui curs opțional pentru studenții universitari legat de studiul criptologiei pe structuri algebrice abstracte.

АННОТАЦИЯ

Малютина Надежда: "Использование информационных технологий в разработке криптографических и алгебраических алгоритмов"

Докторская диссертация по информатике, Кишинёв, 2023

Структура диссертации: диссертация состоит из введения, четырех глав, общих выводов и рекомендаций, списка литературы из 201 источника и 3 приложений. Диссертация содержит 145 страниц основного текста, 1 рисунок и 71 таблицу. Полученные результаты были опубликованы в 21 научных работах.

Ключевые слова: Алгоритм Марковского, квазигруппа, левая и правая квазигруппа, трансляция, открытый текст, зашифрованный текст, атака, ключ, шифрование, дешифрование.

Цель исследования: построение новых и усовершенствование уже построенных криптографических алгоритмов и их криптоанализ.

Задачи исследования: 1. Разработка эффективного криптографического алгоритма на основе алгоритма Марковского с использованием n-арных группоидов; 2. Написание программ, реализующих работу построенных алгоритмов; 3. Проведение атак на все построенные шифры; 4. Сравнительный анализ проведенных атак; 5. Нахождение текстов минимальной длины для всех исследованных типов атак.

Научная новизна и оригинальность работы: результаты работы новые и оригинальные. Они являются продолжением предыдущих исследований в этой области. Разработаны и обобщены алгоритмы, которые позволили улучшить работу классического алгоритма Марковского, изучены атаки на построенные шифры и показана степень стойкости этих шифров.

Полученный результат, который способствует решению важной научной проблемы: состоит в разработке новых обобщений классического алгоритма, которые способствуют увеличению стойкости построенного шифра к известным видам атак.

Теоретическая значимость работы: определяется получением новых алгоритмов и шифров, построенных с применением неассоциативных структур, таких как n-арные группоиды. Разработаны новые обобщения алгоритмов кодирования с использованием левых и правых квазигрупп, n-арных группоидов обратимых на одном фиксированном месте.

Прикладная ценность работы заключается в использовании полученных результатов в теории кодирования и криптоанализе.

Внедрение научных результатов: Полученные результаты могут быть использованы в научных исследованиях, связанных с кодированием данных, изучением эффективности представления информации, криптоанализе данных. Они также могут быть использованы при разработке факультативного курса для студентов университетов, связанного с изучением криптологии на абстрактных алгебраических структурах.

MALYUTINA, NADEZHDA

THE USE OF INFORMATION TECHNOLOGIES IN THE DEVELOPMENT OF CRYPTOGRAPHIC AND ALGEBRAIC ALGORITHMS

122. 03 – Models, Methods of Mathematics, Software Products

Summary of the Ph.D. Thesis in Computer Science

Approved for printing: 09.03.2023	Paper size 60x84 1/16
Offset paper. Offset printing.	Copies 30 ex.
Print sheets: 1,5	Order No. 15

Shop "PRINTER", Sverdlova street, 92, Tiraspol, MD-3300

Email: alex@impreso.md