Acta et Commentationes, Exact and Natural Sciences ISSN: 2537-6284
Volume 2(14), 2022, Pages 117–131 E-ISSN: 2587-3644
CZU 512.548 (043.3) DOI: 10.36120/2587-3644.v14i2.117-131

Dedicated to the memory of Professor Alexandru Basarab

Encryption and decryption algorithm based on the Latin groupoid isotopes

Liubomir Chiriac, Aurel Danilov, and Violeta Bogdanova

Abstract. This paper studies encryption and decryption algorithm, using isotopes of Latin groupoid. Cryptographic algorithms are computationally intensive processes which consume large amount of CPU time and space during the process of encryption and decryption. The goal of this paper is to study the encryption and decryption algorithm with the help of the concept of Latin groupoid and notion of isotopes. The proposed algorithm is safe in the implementation process and can be verified without much difficulty. An example of encryption and decryption based on the Latin groupoid and the concept of isotopy is examined.

2010 Mathematics Subject Classification: 34C14, 34C40.

Keywords: Latin groupoid, isotopes, encryption and decryption algorithm.

Algoritmul de criptare și decriptare bazat pe izotopii grupoidului latin

Rezumat. În lucrarea de faţă este dezvoltat un algoritm de criptare şi decriptare care se bazează pe utilizarea grupoidului latin, concept care a fost introdus de autori, şi a izotopilor grupoidului examinat. Implementarea algoritmilor criptografici reprezintă procese intensive din punct de vedere computaţional şi presupune consumul unei cantităti mari de timp pentru funţionarea procesorului, cât şi un volum important de spaţiu pentru memoria calculatorului pe durata procesului de criptare şi decriptare. Scopul lucrării este de a studia algoritmul de criptare şi decriptare conceput cu ajutorul conceptului de grupoid latin şi noţiunii de izotop. Algoritmul propus de autori este sigur în procesul de implementare şi poate fi verificat fără prea multe dificultăţi. Este soluţionat un exemplu practic privind utilizarea algoritmului de criptare şi decriptare dezvoltat în baza grupoidului latin şi a izotopiilor de grupoid.

Cuvinte-cheie: grupoid latin, izotopi, algoritm de criptare si decriptare.

1. Introduction

In cryptography the encryption and decryption procedures consist of a set of algorithms and mathematical concepts and formulas that indicate the rules of conversion of plain text to cipher text and vice versa combined with the secured key. In some encryption and decryption algorithms sender and receiver use the same key. While in other encryption and decryption procedures sender and receiver use different keys. The major goal is to develop any algorithmic encryption and decryption procedure to improve the level of security. Therefore, this paper aims to propose a new encryption and decryption algorithm to improve the secure level using, the concept of the Latin groupoid and notion of isotopes.

Our main results can be summarized as follows. In Section 2 we give the basic algebraic notions. In Section 3 we propose an Algorithm to Encrypt and Decrypt message, using isotopes of Latin groupoids. Finally, in Section 4 we give one example of Encryption and Decryption algorithm based on the concept of Latin groupoid and isotopes.

We dedicate this paper to the memory of Professor Alexandru Basarab, who worked for more than 50 years at the Faculty of Physics and Mathematics of Tiraspol State University, Republic of Moldova and made many important contributions to theory of loops and quasigroups.

2. Basic notions

In this section we recall some fundamental definitions and notations.

A non-empty set G is said to be a *groupoid* with respect to a binary operation denoted by $\{\cdot\}$, if for every ordered pair (a, b) of elements of G there is a unique element $ab \in G$.

A quasigroup is a binary algebraic structure in which one-sided multiplication is a bijection in that all equations of the form $ax = b$ and $ya = b$ have unique solutions.

An element $e \in G$ is called an *identity* if $ex = xe = x$ every $x \in G$.

A quasigroup with an identity is called a *loop*. The notion of quasigroup is hence a generalization of the notion of group, in that it does not require the associativity law, nor the existence of an identity element.

A groupoid G is called *medial* if it satisfies the law $xy \cdot zt = xz \cdot yt$ for all $x, y, z, t \in G$.

If a guasigroup G contains an element e such that $e \cdot x = x$ $(x \cdot e = x)$ for all x in G, then e is called a *left (right) identity* element of G and G is called a *left (right) loop.*

In mathematical terms, a permutation of a set is defined as a bijective function $p : X \rightarrow X$. For example, there are six permutations of the set $\{1, 2, 3\}$, namely $(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2)$ and $(3, 2, 1)$.

It is called permutation of degree n bijective function $p : N^* \rightarrow N^*$ and is written in the following form:

$$p = \begin{pmatrix} 1 & 2 & ... & n \\ p(1) & p(2) & ... & p(n) \end{pmatrix}.$$

Denote by S_n the set of permutations of degree n and $\text{card}(S_n) = n!$ Permutations can be defined as bijections from a set S onto itself. All permutations of a set with n elements form a symmetric group, denoted S_n, where the group operation is function composition. Thus, for two permutations, α and β in the group S_n, the four group axioms hold: closure, associativity, identity and invertibility. For every permutation α, there exists an inverse permutation α^{-1}, so that $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha= e$, where e is identity permutation. In general, composition of two permutations is not commutative.

Let E be a non-empty set. Then the set $S(E) = \{f : E \longrightarrow E : f-bijective\}$, together with the function composition operation, is a group, called the permutation group of the set E (or the symmetric group associated with the set E). If F is a set with the property that there is a bijection between F and E, then the groups $S(F)$ and $S(E)$ are isomorphic.

Permutations are used in almost every branch of mathematics and many other areas of science. In computer science, they are used to analyze sorting algorithms; in quantum physics, for describing the states of particles; and in biology, for example, for describing RNA sequences.

Let $(G, \star)$, $(H, \circ)$ be groupoids. An isotopy from $(G, \star)$ to $(H, \circ)$ is an ordered triple: $\phi = (f, g, h)$, of bijections from $(G, \star)$ to $(H, \circ)$, such that $f(a) \circ g(b) = h(a \star b)$ or $h^{-1}(f(a) \circ g(b)) = a \star b$ for all $a, b \in G$.

An $(H, \circ)$ is called an isotope of $(G, \star)$, or $(H, \circ)$ is isotopic to $(G, \star)$ if there is an isotopy $\phi = (f, g, h)$:$(G, \star) \to (H, \circ)$.

Hereafter, we share some examples of isotopies. If $f : G \to H$ is an isomorphism, then $(f, f, f) : G \to H$ is an isotopy. We can write $f = (f, f, f) : G \to H$. If all 3 permutations coincide: $f = g = h$, then isotopy turns into isomorphism. In this case we will write $f(x) \circ f(y) = f(x * y)$. In particular $(1_G, 1_G, 1_G) : G \to G$ is an isotopy where 1_G is the identity function on G.

If $\phi = (f, g, h)$:$(G, \star) \to (H, \circ)$ is an isotopy, then so is

$$\phi^{-1} = (f^{-1}, g^{-1}, h^{-1}) : (H, \circ) \to (G, \star),$$

for if $f^{-1}(a) = c$ and $g^{-1}(b) = d$, then $ab = f(c)g(d) = h(cd)$, so that

$$f^{-1}(a)g^{-1}(b) = cd = h^{-1}(ab).$$

Let $\mathbb{N} = \{1, 2, ...\}$ and $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$. We shall use the notations and terminology from [1, 2, 3, 4, 5, 7]. The results established here are related to the work in [8, 6, 9, 10, 11, 12].

Example 1. Let $(Q, \star)$ be a quasigroup, determined by the following Cayley table:

★	1	2	3	4
1	1	3	2	4
2	2	1	4	3
3	3	4	1	2
4	4	2	3	1

Let α, β, and γ be three arbitrary permutations of the set Q. Then, applying the permutation α of the elements on the border line, the permutation β of the elements on the border column and the permutation γ of the elements inside the table, one obtains a new law of composition $(\circ)$ on Q and it is clear that $(Q, \circ)$ is isotopic to the quasigroup $(Q, \star)$.

Thus, we consider:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Applying the permutations α, β, and γ, it is obtained the following:

★	1	2	3	4
1	1	3	2	4
2	2	1	4	3
3	3	4	1	2
4	4	2	3	1

$\overrightarrow{\alpha}$

·	1	2	3	4
1	2	1	4	3
2	3	4	1	2
3	4	2	3	1
4	1	3	2	4

$\overrightarrow{\beta}$

∗	1	2	3	4
1	3	4	1	2
2	2	1	4	3
3	1	3	2	4
4	4	2	3	1

$\overrightarrow{\gamma}$

∘	1	2	3	4
1	4	3	2	1
2	1	2	3	4
3	2	4	1	3
4	3	1	4	2

We note that the quasigroup $(Q, \star)$ is medial, non-associative, since $(3 \star 4) \star 2 \neq 3 \star (4 \star 2)$ and $e = 1$ is the right identity because $x * 1 = x$ for every $x \in (Q, \star)$. Isotop quasigroup $(Q, \circ)$ is medial, non associative, but $e = 2$ is the left identity because $2 * x = x$ for every $x \in (Q, \circ)$. We conclude from this that, unlike isomorphism which preserves all properties of an algebraic operation, an isotopism does not preserve all properties.

A *Latin groupoid* of order n is a $n \times n$ array filled with s, distinct symbols (by convention $\{al_1, ..., al_s\}$),where $s \leq n^2$, such that there are symbols which are repeated twice or more times, in rows or columns.

It should be mentioned that a Latin groupoid is a Latin square of order n, is a $n \times n$ array filled with $n = s$ distinct symbols, such that no symbol is repeated twice in any row or column.

Two Latin groupoids are isotopic if each can be turned into the other by permuting the rows and columns. This isotopy relation is an equivalence relation; the equivalence classes are the isotopy classes.

During the exposition of the material we will use also and another definition.

A non-empty couple of sets (G, Al), where $|G| = n$ and $|Al| = s$, is said to be a *Latin groupoid* with respect to a composition or operation $(\bullet)$ that sends any two elements $a, b \in G$ to another element, $a \bullet b = al_i \in Al$, where $i = \{1, ..., s\}$ and the number of all elements of the type $al_i \in Al$, which some of them can be repeated several times in rows or columns, is equal to n^2.

Denote a *Latin groupoid* by $(G, Al, \bullet)$.

Example 2. Let be $Q = \{1, 2, 3, 4, 5, 6\}$ and $Al = \{$space, S, !, B, V, R, H, G, O, D, H, E, L, T, I, A, W,$\}$. Let $(\bullet)$ be defined by the following Cayley table:

$\bullet$	1	2	3	4	5	6
1	M	G	O	D	H	E
2	L	T	I	S	B	V
3	W	A	R		O	D
4	H	E	R	L	T	I
5	S	B	!	W	A	M
6	O	E	A	H		T

Then $(Q, Al, \bullet)$ is a Latin groupoid.

3. Encryption and Decryption Algorithm based on the Latin Groupoid and Isotopes

Below we describe the respective algorithm.

3.1. Steps to Encrypt the message

1. Define the alphabet $Al = \{al_1, al_2, ..., al_t\}$, where t is dimension of the set Al and $t \in N$.

2. Define a set of n ordered elements $Q = \{1, 2, ..., n\}$, where $n \in N$ and $n^2 > t$.

3. Construct a Latin groupoid $(Q, Al, \bullet)$.

The construction of the Latin groupoid begins with the definition of the composition or operation on the set Q. Define the operation $(\bullet)$ on the couple of sets (Q, Al), taking into account the following conditions:

3.1. The result of the operation $a \bullet b$ with respect to a operation $(\bullet)$ is an element $a \bullet b = al_i \in Al$, for all $a, b \in Q$ and $i = \overline{1, t}$.

3.2. All results of the operations $a \bullet b = al_i \in Al$, for all $a, b \in Q$ and $i = \overline{1, t}$, made up of the elements of the alphabet Al, are placed in a Cayley table, which has the dimension $n \times n$.

3.3. The elements inside in the Cayley table $al_1, al_2, ..., al_t$ are placed randomly. The important thing is that each element of the alphabet $al_i \in Al$, $i = \overline{1, t}$ is found at least once as a result of the operation $a \bullet b$ for all $a, b \in G$. The number of all elements of the type $al_i \in Al$, where some of them can be repeated several times, is equal to n^2.

3.4. In this way we obtain a Latin groupoid $(G, Al, \bullet)$ in which the results of the operation $a \bullet b$ for all $a, b \in G$ are all the elements of the alphabet Al and some elements can be repeated several times. There is no maximum limit for how many times an element of the Al alphabet could be repeated as a result.

4. In the Cayley table, it is determined how many times each of the elements of the Latin groupoid $(Q, Al, \bullet)$ is repeated.

Denote by K the set of the number of repetition of all elements in the alphabet Al.

4.1. Let element al_1 be repeated by k_1 times, element al_2 be repeated by k_2 times,...,element al_t be repeated by k_t times. In this way we get the set $K = \{k_1, k_2, ..., k_t\}$, where k_s indicates the number of repetitions of the element al_s in the alphabet Al, and $s = \overline{1, t}$. By $r = max\{k_1, k_2, ..., k_t\}$ it is denoted the maximum number of repetitions of the elements $k_s \in K$, $s = \overline{1, t}$.

4.2. Then there are determined all the pairs $i \bullet j$, where $i, j = \overline{1, n}$, of the elements which give us the same result for each of the elements $al_s \in Al$, $s = \overline{1, t}$.

Denote by O_p, where $p = 1, 2, ..., r$, the p-set of the results of the operations $i \bullet j = al_s \in Al$ for all $i, j \in Q$ and $s = \overline{1, t}$.

First, the set O_1 is constructed by including only one result at a time of the operations $i \bullet j = al_s$ for all $i, j \in Q$ and for all elements $al_s \in Al$ and $s = \overline{1, t}$. For example, if $al_{s_\star} = i_1 \bullet j_1 = i_2 \bullet j_2 = ... = i_r \bullet j_r$ then will be include in the set O_1 only result of the operation $i_1 \bullet j_1$. It is obviously $|O_1| = m$, where m is the dimension of the secret message.

Afterwards, the set O_2 is constructed by counting and including only one result at a time of the operations $i \bullet j = al_s$ for all $i, j \in Q$ and for each element $al_s \in Al$,$s = \overline{1, t}$, with the exception of the results that were already included in the set O_1. For example, if $al_{s_\star} = i_1 \bullet j_1 = i_2 \bullet j_2 = ... = i_r \bullet j_r$ then will be include in the set O_2 only result of the operation $i_2 \bullet j_2$.

At the last stage the set O_r is constructed through identification and including all results of the operations (with the exception of the results that were already included in the sets $O_1, ..., O_{r-1}$) $i \bullet j = al_s \in Al$ for all $i, j \in Q$ and $s = \overline{1, t}$.

For example, if $al_{s_\star} = i_1 \bullet j_1 = i_2 \bullet j_2 = ... = i_r \bullet j_r$ then will be include in the set O_r only result of the operation $i_r \bullet j_r$.

It is important to note that $\bigcap_{p=1}^{r} O_p = \emptyset$.

5. Define a set of n_1 ordered elements $Q_1 = \{1, 2, ..., n_1\}$, where $n_1 \leq n$.

6. Define the permutations α and β on the set Q_1.

7. Get the message for Encryption.

Let the secret text be $M1 = \{al_1, al_2, ..., al_m\}$, where m is the dimension of the message and $al_s \in Al$, $s = \overline{1, t}$.

8. In the next table we will construct:

8.1. The set $M1$ which represents the message to be encrypted. The elements of the set $M1$ are the elements of the secret text and $|M1| = n_1^2 = m$.

8.2. The set K_1 which indicates the number of repetitions of the elements of the secret message $M1$. The number of elements in the set K_1 coincides to the dimension m of the secret message $M1$. All the elements of the set K_1 are one of the the numbers $\{1, ..., r\}$ which can be repeated several times.

8.3. The set P where the elements of the set P are formed by the numbers $p = 1, ..., r$. Each element of the set P indicates from which set O_p the corresponding element $i \bullet j = al_s \in Al$ for all $i, j \in Q$ and $s = \overline{1, t}$ is taken. The number of elements of the set P coincides with the dimension m of the secret message $M1$.

8.4. The set R that includes all the element $i \bullet j = al_s \in M1$ for all $i, j \in Q$ and $s = \overline{1, n_1^2}$ is taken.

The set $R = \{r_1, r_2, ..., r_m\}$ represents the secret message, where $r_i \in O_p$, $p = 1, ..., r$ is determined by all pairs $i \bullet j = al_s \in M1$ for all $i, j \in Q$ and $s = \overline{1, n_1^2}$.

9. Construct the Latin groupoid $(Q_1, R, \circ)$.

In order to increase the degree of protection of the message R we will construct the Latin groupoid $(Q_1, R, \circ)$. All results of the operations $i \bullet j = r_s \in R$ for all $i, j \in Q_1$ and $s = \overline{1, n_1^2}$, made up of the elements R, are placed in a Cayley table of a Latin groupoid $(Q_1, R, \circ)$ which has the dimension $n_1 \times n_1$, respects the order of the elements in the set R and places them one by one in the table, starting with the first row, the second one and so on until the last $n_1 - th$ row. In each row there will be exactly n_1-elements.

10. The permutation α is applied to the Latin groupoid $(Q_1, R, \circ)$. Get the Latin groupoid $(Q_1, R, \circ_\alpha)$.

11. The permutation β is applied to the Latin groupoid $(Q_1, R, \circ_\alpha)$. Get the Latin groupoid $(Q_1, R, \circ_\beta)$. The Latin groupoid $(Q_1, R, \circ_\beta)$ is an isotope of the Latin groupoid $(Q_1, R, \circ)$.

The secret key for encryption is Latin groupoid $(Q, Al, \bullet)$ and the permutations α and β on the set Q_1. The Latin groupoid $(Q_1, R, \circ_\beta)$ represents the secret message and will be send to receiver.

3.2. Steps to Decrypt the message

1. The secret key for decryption is the Latin groupoid $(Q, Al, \bullet)$ and the permutations α^{-1} and β^{-1} on the set Q_1.

2. Applying the permutation β^{-1} on the Latin groupoid $(Q_1, R, \circ_\beta)$, get the Latin groupoid $(Q_1, R, \circ_\beta^{-1})$.

3. Applying the permutation α^{-1} on the Latin groupoid $(Q_1, R, \circ_\beta^{-1})$, get the Latin groupoid $(Q_1, R, \circ_\alpha^{-1})$ which coincides to the Latin groupoid $(Q_1, R, \circ)$.

4. Using the Latin groupoid $(Q, Al, \bullet)$ that was constructed at step 3 in the Encryption Algorithm, we obtain the decrypted message.

4. Example of the use of the Encryption and Decryption Algorithm

Example. Interlocutor A needs to sent a secret message to interlocutor B. For this purpose, the following steps are undertaken:

Step 1. Interlocutor A decides to determine the number of symbols of the alphabet Al according to the secret message
$M1$ = {GOOD HEALTH IS ABOVE WEALTH! REMEMBER!}, where $m = 38$ is the number of all elements, inclusive empty space.

Thus, the alphabet, defined by interlocutor A for message $M1$, is
Al = {space, G, O, D, H, E, L, T, I, A, W, S, !, B, V, R, H}.

Since Al consists of $t = 17$ elements, then the set Q will have $n = 6$ elements. Hence, $Q = \{1, 2, 3, 4, 5, 6\}$ and $n^2 = 36 \geq 17 = t$.

Step 2. Interlocutor A, taking into the consideration the conditions 3.1 – 3.4., defines the operation $(\bullet)$ on the set Q and gets the Latin groupoid $(Q, Al, \bullet)$.

Interlocutor A defines the set Q_1= $\{1, 2, 3, 4, 5, 6\}$ and the permutations α and β on the set Q_1. Let:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 3 & 2 & 6 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 6 & 3 & 2 \end{pmatrix}.$$

The secret key for encryption is the Latin groupoid $(Q, Al, \bullet)$ and the permutations α and β.

Step 3. Interlocutor A defines the operation $(\circ)$ on the set Q_1 and gets the Latin groupoid $(Q_1, R, \circ)$, where R is set which represents secret message with the elements $i \bullet j = al_s \in M1$ for all $i, j \in Q$ and $s = \overline{1, 38}$.

Step 4. Interlocutor A applies the permutations α, β for encrypting the secret message and sends it to interlocutor B.

Step 5. Interlocutor B receives the secret message $(Q_1, R, \circ)$ and secret keys: Latin groupoid $(Q, Al, \bullet)$ and permutations α and β.

Step 6. Interlocutor B computes and applies the permutations α^{-1} and β^{-1} for decrypting the secret message $(Q_1, R, \circ)$ and read it.

It is required to describe more detailed Steps 1 – 5 in accordance with the algorithm presented above.

Solve.

Steps to Encrypt the message.

1. Define the alphabet $Al = \{$space,G, O, D, H, E, L, T, I, A, W, S, !, B, V, R, H$\}$, where numbers of characters $t = 17$.

2. Define a set of n = 6 ordered elements $Q = \{1, 2, 3, 4, 5, 6\}$, where $36 = n^2 > t = 17$.

3. Construct a Latin groupoid $(Q, Al, \bullet)$.

Define the operation $(\bullet)$ on the couple of sets (Q, Al), taking into account the following conditions:

3.1. The result of the operation $i \bullet j$ with respect to an operation $(\bullet)$ is an element $i \bullet j = al_s \in Al$, for all $i, j \in Q$ and $s = \overline{1, 17}$, where $Al = \{$space, G, O, D, H, E, L, T, I, A, W, S, !, B, V, R, H$\}$.

3.2. All results of the operations $i \bullet j = al_s \in Al = \{$space, G, O, D, H, E, L, T, I, A, W, S, !, B, V, R, H$\}$ for all $i, j \in Q$ and $s = \overline{1, 17}$, made up of the elements Al, are placed in a Cayley table of a Latin groupoid $(Q, Al, \bullet)$, which has the dimension 6×6.

3.3. All elements $al_s \in Al$ inside the Cayley table are placed randomly. An important rule is that each element of the alphabet Al is found at least once as a result of the operation $i \bullet j$ for all $i, j \in Q$. Number of all elements of the type $al_i \in Al$, which some of them can be repeated several times, is equal to 6^2.

Below, can see the operation table of the Latin groupoid $(Q, Al, \bullet)$.

•	1	2	3	4	5	6
1		G	O	D	H	E
2	L	T	I	S	B	V
3	W	A	R		O	D
4	H	E	R	L	T	I
5	S	B	!	W	A	M
6	O	E	A	H	T	M

4. In the Cayley table, it is determined how many times each of the elements of the Latin groupoid $(Q, Al, \bullet)$ is repeated.

In the tables below we will construct: the set K which indicates the number of repetition of all elements in the alphabet Al and the sets O_p, where $p = 1, 2, ..., r$, which indicate the results of the operations $i \bullet j = al_s \in Al$ for all $i, j \in Q$ and $s = \overline{1, 17}$.

As the maximum number of repetitions of the elements in Al is $r = 3$, then the set K is formed from the elements $1, 2, 3$. We will have the sets O_1, O_2 and O_3.

It should be mentioned that $\bigcap_{p=1}^{3} O_p = \emptyset$.

In this way we obtain the tables below.

Al	space	G	O	D	H	E	L	T	I	A
K	2	1	3	2	3	3	2	3	2	3
O_1	$1 \bullet 1$	$1 \bullet 2$	$1 \bullet 3$	$1 \bullet 4$	$1 \bullet 5$	$1 \bullet 6$	$2 \bullet 1$	$2 \bullet 2$	$2 \bullet 3$	$3 \bullet 2$
O_2	$3 \bullet 4$		$3 \bullet 5$	$3 \bullet 6$	$4 \bullet 1$	$4 \bullet 2$	$4 \bullet 4$	$4 \bullet 5$	$4 \bullet 6$	$5 \bullet 5$
O_3			$6 \bullet 1$		$6 \bullet 4$	$6 \bullet 2$		$6 \bullet 5$		$6 \bullet 3$

Al	W	S	!	B	V	R	M
K	2	2	1	2	2	2	2
O_1	$3 \bullet 1$	$2 \bullet 4$	$5 \bullet 3$	$2 \bullet 5$	$2 \bullet 6$	$3 \bullet 3$	$5 \bullet 6$
O_2	$5 \bullet 4$	$5 \bullet 1$		$5 \bullet 2$	$5 \bullet 3$	$4 \bullet 3$	$6 \bullet 6$

Each element $k_i \in K = \{2, 1, 3, 2, 3, 3, 2, 3, 2, 3, 2, 2, 1, 2, 2, 2, 2\}$ indicates the number of repetitions of the corresponding element $al_i \in Al = \{$space, G, O, D, H, E, L, T, I, A, W, S, !, B, V, R, H$\}$, where $i = \overline{1, 17}$.

5. Define a set of n_1=6 ordered elements $Q_1 = \{1, 2, 3, 4, 5, 6\}$.

6. Define the permutations α and β on the set Q_1 in the following way:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 3 & 2 & 6 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 6 & 3 & 2 \end{pmatrix}.$$

7. Get the message for Encryption. Let the secret text be $M1 = \{$GOOD HEALTH IS ABOVE WEALTH! REMEMBER!$\}$, where $m = 38$ is the dimension of the message. In this message we have 5 empty spaces. To reduce the dimension of the message to 36 we will omit 2 empty spaces. Therefore, the secret message will be $M1 = \{$GOODHEALTH IS ABOVE WEALTH!REMEMBER!$\}$, where $m = 36$.

8. In the tables below we will construct the sets: $M1$, K_1, P and R.

$M1$	G	O	O	D	H	E	A	L	T	H
K_1	1	3	3	2	3	3	2	3	2	3
P	1	1	2	1	1	1	1	1	1	2
R	$1 \bullet 2$	$1 \bullet 3$	$3 \bullet 5$	$1 \bullet 4$	$1 \bullet 5$	$1 \bullet 6$	$3 \bullet 2$	$2 \bullet 1$	$2 \bullet 2$	$4 \bullet 1$

$M1$	space	I	S	space	A	B	O	V	E	space
K_1	2	2	2	2	3	2	3	2	3	2
P	1	1	1	1	2	1	3	1	1	1
R	$1 \bullet 1$	$2 \bullet 3$	$2 \bullet 4$	$1 \bullet 1$	$5 \bullet 5$	$2 \bullet 5$	$6 \bullet 1$	$2 \bullet 6$	$4 \bullet 2$	$3 \bullet 4$

$M1$	W	E	A	L	T	H	!	R	E	M
K_1	2	3	3	2	3	3	1	2	3	2
P	1	3	3	2	2	3	1	1	1	1
R	$3 \bullet 1$	$6 \bullet 2$	$6 \bullet 3$	$4 \bullet 4$	$4 \bullet 5$	$6 \bullet 4$	$5 \bullet 3$	$3 \bullet 3$	$1 \bullet 6$	$5 \bullet 6$

$M1$	E	M	B	E	R	!
K_1	3	2	3	3	2	1
P	2	2	3	3	2	1
R	$4 \bullet 2$	$6 \bullet 6$	$5 \bullet 2$	$6 \bullet 2$	$4 \bullet 3$	$5 \bullet 3$

In the above tables it is show that the result of the operation $i \bullet j \in R$, which determines the corresponding element $al_i \in M1$, is taken from the set O_r, where $r = 1, 2, 3$.

For example, the result of the binary operation $1 \bullet 3 \in R$, give us the element $O \in M1$ which is repeated 3 times in the text, because corresponding element in the set K_1 is $3 \in K_1$. The result $1 \bullet 3 = O$ is taken from the set O_1, because the corresponding element in the set P is $1 \in P$. The set

$R = \{1 \bullet 2, 1 \bullet 3, 3 \bullet 5, 1 \bullet 4, 1 \bullet 5, 1 \bullet 6, 3 \bullet 2, 2 \bullet 1, 2 \bullet 2, 4 \bullet 1, 1 \bullet 1, 2 \bullet 3, 2 \bullet 4, 1 \bullet 1, 5 \bullet 5, 2 \bullet 5, 6 \bullet 1, 2 \bullet 6, 4 \bullet 2, 3 \bullet 4, 3 \bullet 1, 6 \bullet 2, 6 \bullet 3, 4 \bullet 4, 4 \bullet 5, 6 \bullet 4, 5 \bullet 3, 3 \bullet 3, 1 \bullet 6, 5 \bullet 6, 4 \bullet 2, 6 \bullet 6, 5 \bullet 2, 6 \bullet 2, 4 \bullet 3, 5 \bullet 3\}$ determine the secret message. The dimension of the set R is $m = 36$.

9. Construct the Latin groupoid $(Q_1, R, \circ)$.

In order to increase the degree of protection of the message R we will construct the Latin groupoid $(Q_1, R, \circ)$. All results of the operations $i \bullet j = r_s \in R$ for all $i, j \in Q_1$ and $s = \overline{1, 36}$, made up of the elements R, are placed in a Cayley table of a Latin groupoid $(Q_1, R, \circ)$, which has the dimension 6 × 6.

$\circ$	1	2	3	4	5	6
1	$1 \bullet 2$	$1 \bullet 3$	$3 \bullet 5$	$1 \bullet 4$	$1 \bullet 5$	$1 \bullet 6$
2	$3 \bullet 2$	$2 \bullet 1$	$2 \bullet 2$	$4 \bullet 1$	$1 \bullet 1$	$2 \bullet 3$
3	$2 \bullet 4$	$1 \bullet 1$	$5 \bullet 5$	$2 \bullet 5$	$6 \bullet 1$	$2 \bullet 6$
4	$4 \bullet 2$	$3 \bullet 4$	$3 \bullet 1$	$6 \bullet 2$	$6 \bullet 3$	$4 \bullet 4$
5	$4 \bullet 5$	$6 \bullet 4$	$5 \bullet 3$	$3 \bullet 3$	$1 \bullet 6$	$5 \bullet 6$
6	$4 \bullet 2$	$6 \bullet 6$	$5 \bullet 2$	$6 \bullet 2$	$4 \bullet 3$	$5 \bullet 3$

10. The permutation:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 3 & 2 & 6 \end{pmatrix}$$

is applied to the Latin groupoid $(Q_1, R, \circ)$. It is obtained the Latin groupoid $(Q_1, R, \circ_\alpha)$.

$\circ_\alpha$	1	2	3	4	5	6
1	$1 \bullet 2$	$1 \bullet 3$	$3 \bullet 5$	$1 \bullet 4$	$1 \bullet 5$	$1 \bullet 6$
2	$4 \bullet 2$	$3 \bullet 4$	$3 \bullet 1$	$6 \bullet 2$	$6 \bullet 3$	$4 \bullet 4$
3	$4 \bullet 5$	$6 \bullet 4$	$5 \bullet 3$	$3 \bullet 3$	$1 \bullet 6$	$5 \bullet 6$
4	$2 \bullet 4$	$1 \bullet 1$	$5 \bullet 5$	$2 \bullet 5$	$6 \bullet 1$	$2 \bullet 6$
5	$3 \bullet 2$	$2 \bullet 1$	$2 \bullet 2$	$4 \bullet 1$	$1 \bullet 1$	$2 \bullet 3$
6	$4 \bullet 2$	$6 \bullet 6$	$5 \bullet 2$	$6 \bullet 2$	$4 \bullet 3$	$5 \bullet 3$

11. The permutation

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 6 & 3 & 2 \end{pmatrix}$$

is applied to the Latin groupoid $(Q_1, R, \circ_\alpha)$. It is obtained the Latin groupoid $(Q_1, R, \circ_\beta)$.

$\circ_\beta$	1	2	3	4	5	6
1	$1 \bullet 2$	$1 \bullet 4$	$1 \bullet 5$	$1 \bullet 6$	$3 \bullet 5$	$1 \bullet 3$
2	$4 \bullet 2$	$6 \bullet 2$	$6 \bullet 3$	$4 \bullet 4$	$3 \bullet 1$	$3 \bullet 4$
3	$4 \bullet 5$	$3 \bullet 3$	$1 \bullet 6$	$5 \bullet 6$	$5 \bullet 3$	$6 \bullet 4$
4	$2 \bullet 4$	$2 \bullet 5$	$6 \bullet 1$	$2 \bullet 6$	$5 \bullet 5$	$1 \bullet 1$
5	$3 \bullet 2$	$4 \bullet 1$	$1 \bullet 1$	$2 \bullet 3$	$2 \bullet 2$	$2 \bullet 1$
6	$4 \bullet 2$	$6 \bullet 2$	$4 \bullet 3$	$5 \bullet 3$	$5 \bullet 2$	$6 \bullet 6$

The Latin groupoid $(Q_1, R, \circ_\beta)$ is the isotope of the Latin groupoid $(Q_1, R, \circ)$. The Latin groupoid $(Q_1, R, \circ_\beta)$ represents the encryption of the message $M1$ and will be sent to receiver B.

The secret key for the encryption message $M1$ is the Latin groupoid $(Q, Al, \bullet)$ and the permutations α and β on the set Q_1.

Steps to Decrypt the message

1. The secret key for decryption is Latin groupoid $(Q, Al, \bullet)$ and the permutations α^{-1}, β^{-1} on the set Q_1.

2. We compute the permutation β^{-1} and we get:

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 2 & 3 & 4 \end{pmatrix}.$$

Applying the permutation β^{-1} on the Latin groupoid $(Q_1, R, \circ_\beta)$, which represent encryption of the message $M1$, it is got the Latin groupoid $(Q_1, R, \circ_\beta^{-1})$.

$\circ_{\beta^{-1}}$	1	2	3	4	5	6
1	$1 \bullet 2$	$1 \bullet 3$	$3 \bullet 5$	$1 \bullet 4$	$1 \bullet 5$	$1 \bullet 6$
2	$3 \bullet 2$	$3 \bullet 4$	$3 \bullet 1$	$6 \bullet 2$	$6 \bullet 3$	$4 \bullet 4$
3	$4 \bullet 5$	$6 \bullet 4$	$5 \bullet 3$	$3 \bullet 3$	$1 \bullet 6$	$5 \bullet 6$
4	$2 \bullet 4$	$1 \bullet 1$	$5 \bullet 5$	$2 \bullet 5$	$6 \bullet 1$	$2 \bullet 6$
5	$3 \bullet 2$	$2 \bullet 1$	$2 \bullet 2$	$4 \bullet 1$	$1 \bullet 1$	$2 \bullet 3$
6	$4 \bullet 2$	$6 \bullet 6$	$5 \bullet 2$	$6 \bullet 2$	$4 \bullet 3$	$5 \bullet 3$

3. We compute the permutation α^{-1} and we get:

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 2 & 3 & 6 \end{pmatrix}.$$

Applying the permutation α^{-1} on the Latin groupoid $(Q_1, R, \circ_\beta^{-1})$, it is obtained the Latin groupoid $(Q_1, R, \circ_\alpha^{-1})$ which coincides to the groupoid $(Q_1, R, \circ)$.

$\circ$	1	2	3	4	5	6
1	$1 \bullet 2$	$1 \bullet 3$	$3 \bullet 5$	$1 \bullet 4$	$1 \bullet 5$	$1 \bullet 6$
2	$3 \bullet 2$	$2 \bullet 1$	$2 \bullet 2$	$4 \bullet 1$	$1 \bullet 1$	$2 \bullet 3$
3	$2 \bullet 4$	$1 \bullet 1$	$5 \bullet 5$	$2 \bullet 5$	$6 \bullet 1$	$2 \bullet 6$
4	$4 \bullet 2$	$3 \bullet 4$	$3 \bullet 1$	$6 \bullet 2$	$6 \bullet 3$	$4 \bullet 4$
5	$4 \bullet 5$	$6 \bullet 4$	$5 \bullet 3$	$3 \bullet 3$	$1 \bullet 6$	$5 \bullet 6$
6	$4 \bullet 2$	$6 \bullet 6$	$5 \bullet 2$	$6 \bullet 2$	$4 \bullet 3$	$5 \bullet 3$

4. Using the Latin groupoid $(Q, Al, \bullet)$ that was constructed at step 3 in the Encryption Algorithm, we obtain the decrypted message.

$\circ$	1	2	3	4	5	6
1	G	O	O	D	H	E
2	A	L	T	H		I
3	S		A	B	O	V
4	E		W	E	A	L
5	T	H	!	R	E	M
6	E	M	B	E	R	!

In this way we obtained the secret message $M1$ = {GOODHEALTH IS ABOVE WEALTH!REMEMBER!}.

4. Conclusion

We have proposed a simply and efficient Encryption and Decryption Algorithm based on the Latin groupoid isotopes. Cryptographic developed algorithm does not consume large amount of CPU time and space during in the process of encryption and decryption. This cryptographic algorithm is safe in the process of the implementation and it is not complicated to develop a program for the developed algorithm. In this sense, the authors, based on the proposed algorithms, developed a program in the C++ programming language that works quickly and efficiently.

Acknowledgements. Research supported by “Methodology of ICT implementation in the process of study of the real sciences in the education system of the Republic of Moldova from the perspective of inter/transdisciplinarity (STEAM concept)”, Project 20.80009.0807.20, included in the “State Program” (2020-2023) of the National Agency for Development and Research.

References

[1] Bruck, R.H. *A Survey of Binary Systems*, Springer-Verlag. New York, 1966.

[2] Belousov, V.D. *Foundation of the theory of quasigroups and loops*. Moscow, Nauka, 1967.

[3] Pflugfelder, Hala O. *Quasigroups and Loops. Introduction*. Helderman Verlag Berlin, Sigma Series in Pure Mathematics, Volume 7, 1990. ISBN 3-88538-007-2.

[4] Atanasiu, A. *Securitatea informatiei, (Protocoale de securitate)*, vol. 2. Ed. InfoData, Cluj, 2009.

[5] Barthelemy, P; Rolland, R. and Veron, P. *Cryptographie, Principes et mises en euvre*, Hermes Science, 2012.

[6] Shcherbacov, V. *Quasigroup based crypto-algorithms*, January 2012, https://arxiv.org/abs/1201.3016.

[7] Chiriac, L.; Danilov, A.; Bogdanov, V. Utilizarea conceptelor din teoria numerelor in elaborarea algoritmilor criptografici asimetrici, *Conferinta stiintifica nationala cu participare internationala*, Universitatea de Stat din Tiraspol, Chişinău, 29 - 30 septembrie 2020, 239–247.

[8] Chiriac, L.; Danilov, A. Abordari metodice privind aplicarea quasigrupurilor la dezvoltarea unor metode de criptografie, *Acta et Commentationes, Sciences of Education*, 2020, vol. 22, no. 4, 7–17.

[9] DANILOV, A.; CHIRIAC, L. Studierea sistemului criptografic asimetric ElGamal, *SIPAMI. International Symposium "Actual Problems of Mathematics and Informatics", dedicated to the 90th birthday anniversary of professor Ion Valuta*, November 27-28, 2020, TUM, Chişinău, p. 113.

[10] CHIRIAC, L.; DANILOV, A. Abordari metodice in studierea sistemului criptografic asimetric Merkle-Hellman, *Acta et Commentationes, Sciences of Education*, 2021, vol. 25, no. 3, 7–23.

[11] CHIRIAC, L.; DANILOV, A. Aspecte didactice privind studierea algoritmului de criptare RSA, functiilor hash si semnaturii digitale. *Proceedings of the 29-th Conference on Applied and Industrial Mathematics (CAIM2022)*, dedicated to the memory of Academician Mitrofan M. Choban, August 25-27, 2022, Chişinău. Communications in Education, p. 125–134.

[12] CHIRIAC, L.; DANILOV, A. Metodologia implementarii izotopiilor de grupoizi la criptarea/decriptarea textelor, *A doua Conferinta stiintifica Internationala "Abordari inter/transdisplinare in predarea stiintelor reale, (Concept STEAM)"*, 28 - 29 octombrie, 2022, Chişinău, p. 20.

Received: November 04, 2022 *Accepted: December 23, 2022*

(Liubomir Chiriac, Aurel Danilov, Violeta Bogdanova) TIRASPOL STATE UNIVERSITY / ION CREANGĂ STATE PEDAGOGICAL UNIVERSITY, 1 ION CREANGĂ ST., CHIŞINĂU, REPUBLIC OF MOLDOVA

E-mail address: `llchiriac@gmail.com`, `aureliu.danilov@gmail.com`, `bogdanovaleta@gmail.com`