Acta et Commentationes, Sciences of Education, nr. 4(22), 2020 ISSN 1857-0623
p. 7-17 E-ISSN 2587-3636

CZU: 378.147:004 DOI: 10.36120/2587-3636.v22i4.7-17

ABORDĂRI METODICE PRIVIND APLICAREA QUASIGRUPURILOR LA DEZVOLTAREA UNOR METODE DE CRIPTOGRAFIE

Liubomir CHIRIAC, doctor habilitat, profesor universitar
https://orcid.org/0000-0002-5786-5828
Aurel DANILOV, doctorand
https://orcid.org/0000-0003-0859-7043
Universitatea de Stat din Tiraspol

Rezumat. În lucrare autorii abordează problema pregătirii specialiștilor informaticieni, din perspectiva interdisciplinarității algebra abstractă și informatică. Este examinată aplicarea sistemelor algebrice non-asociative în criptografie. Sunt descrise etapele implementării quasigrupurilor la elaborarea algoritmilor criptografici. S-a demonstrat, din punct de vedere metodologic, necesitatea studierii conceptelor matematice de către informaticieni, pentru înțelegerea funcționării, utilizării și aplicării sistemului criptografic Markovski.

Cuvinte cheie: metode didactice, aspecte interdisciplinare, studierea conceptelor matematice, metode de criptare și decriptare a informației, Quasigrup, algoritmul Markovski.

METHODICAL APPROACHES REGARDING THE APPLICATION OF QUASI-GROUPS TO THE DEVELOPMENT OF CRYPTOGRAPHY METHODS

Abstract. In the paper, the authors address the issue of training computer science specialists, from the perspective of the interdisciplinarity of abstract algebra and computer science. The application of non-associative algebraic systems in cryptography is examined. The stages of implementation of quasi-groups in the elaboration of cryptographic algorithms are described. It was demonstrated, from a methodological point of view, the need to study mathematical concepts by computer scientists, in order to understand the operation, use and application of the Markovski cryptographic system.

Keywords: didactic methods, interdisciplinary aspects, study of mathematical concepts, methods of encryption and decryption of information, Quasigrup, Markovski algorithm.

1. Abordări interdisciplinare în dezvoltarea algoritmilor criptografici

Informatica este, prin esența ei, o „mare consumatoare” de noțiuni, concepte, afirmații din diverse ramuri ale matematicii moderne. Dezvoltarea unor direcții, precum teoria recursiei, limbajele formale, codurile, criptografia, tipurile abstracte de date. Semantica limbajelor de programare necesită o bună cunoaștere și înțelegere a conceptelor matematice și, în mod special, a algebrei abstracte. Datorită conținutului abstract rațional, algebra abstractă își găsește aplicarea în diverse ramuri ale informaticii contemporane, inclusiv în criptografie și securitatea informațională.

În zilele noastre tehnicile de criptare sunt omniprezente și sunt folosite în realizarea diverselor operațiuni zilnice: securizarea operațiunilor efectuate prin intermediul cardurilor bancare, securizarea implementării votului electronic, securizarea plăților on line, asigurarea confidențialității discuțiilor prin intermediul telefoanelor mobile, securizarea semnăturii electronice etc.

Cei mai eficienți algoritmii criptografici au la baza construcției lor concepte matematice moderne din algebra abstractă, teoria numerelor etc. Conform pronosticurilor existente, în viitorul apropiat, centrul de greutate al cercetărilor în domeniul informaticii se va transfera pe segmentul securizării informaționale și al algoritmilor criptografici. La moment, o mare parte din informaticienii începători nu manifestă un interes sporit pentru matematicile moderne. Pregătirea fundamentală a viitorilor specialiști în informatică, care vor alege să activeze în criptografie și securitatea informațională, domenii de mare perspectivă pentru dezvoltarea economiei reale, necesită abordări noi în studierea algebrei abstracte și a teoriei numerelor. Din aceste considerente, interpretarea și re-interpretarea algoritmilor criptografici moderni, bazată pe abordări didactice bine puse la punct, într-un limbaj simplu, clar și pe înțelesul studentului de „nivel mediu" vor conduce la creșterea interesului informaticienilor pentru studierea algoritmilor respectivi [4-9].

Cercetarea și aplicarea sistemelor algebrice non-asociative în criptografie și securitate informațională se efectuează pe larg de diverse școli de matematică și informatică, inclusiv de școala în domeniul quasigrupurilor și buclelor constituită de prof. Valentin Belousov din cadrul Institutului de Matematică și Informatică din Chișinău.

Utilizarea quasigrupurilor în criptografie este atribuită matematicianului german R. Schauffler, care, în lucrarea sa de doctorat din 1948, a redus problema spargerii cifrului lui Vigenere la determinarea unui anumit pătrat latin.

Elaborarea și implementarea algoritmilor criptografici, bazați pe conceptul de quasigrup, care deocamdată este un domeniu mai puțin studiat de studenții informaticieni, vor stimula, în opinia noastră, creșterea interesului din partea studenților și masteranzilor în raport cu studierea aspectelor interdisciplinare, care țin de teoria quasigrupurilor, criptografie și programare, domenii de mare actualitate pentru securitatea informațională.

În această lucrare, autorii vor demonstra și ilustra, din punct de vedere metodologic, necesitatea cunoașterii conceptelor matematice, inclusiv a noțiunii de quasigroup, pentru înțelegerea funcționării și utilizării unui cunoscut sistem criptografic, cunoscut în literatura de specialitate ca algoritmul criptografic Markovski [7-9].

2. Noțiuni și construcții matematice de bază

Mai jos vom puncta noțiunile matematice care vor fi utilizate la construcția algoritmilor criptografici.

Fie **Q** este o mulțime nevidă cu elemente din mulțimea numerelor naturale **N**.

Numărul elementelor dintr-o anumită mulțime este o proprietate cunoscută sub numele de cardinal; informal, aceasta este dimensiunea unei mulțimi. O mulțime infinită este o mulțime cu un număr infinit de elemente, în timp ce o mulțime finită este o mulțime cu un număr finit de elemente. Exemplele examinate în cazul nostru sunt cele de mulțimi finite. Astfel, cardinalul (dimensiunea) mulțimii **Q** = {1, 2, 3, …, **n**} este egal cu **n**, unde n-reprezintă numărul de elemente.

Definiția 1. Dacă **Q** este o mulțime nevidă și „•” o operație binară definită pe mulțimea dată, atunci (**Q**, •) se numește *grupoid*.

Fie **Q**={1, 2, 3}. Definim pe mulțimea **Q** operația binară „•” în felul următor:

•	1	2	3
1	1	2	1
2	1	3	2
3	2	3	3

Atunci (**Q**, •) este un *grupoid*. Grupoizii pot fi construiți prin intermediul *tabelelor Cayley*.

Definiția 2. Grupoidul (**Q**, •) se numește *quasigrup* dacă pentru operația binară „•” fiecare din ecuațiile **a•x**=**b** și **y•a**=**b** au soluții unice în **Q**, pentru ∀ **a**, **b** ∈ **Q**.

Exemplu 1. Fie **Q**={1, 2, 3}. Definim pe mulțimea **Q** operația binară „•” în felul următor:

•	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

În acest caz (**Q**, •) este quasigrup. Fiecare din ecuațiile **a•x**=**b** și **y•a**=**b** , ∀ **a**, **b** ∈ **Q** au o singură soluție în **Q**. De exemplu, pentru exemplul de mai sus, ecuația 3 • **x** = 1 are o singură soluție **x** = 2. Iar pentru ecuația **y** • 2 = 3 unica soluție este **y** = 2. Să observăm că quasigrupul (**Q**, •) este asociativ, deci este un grup.

Soluția ecuației **a•x**=**b** este **x**=**a\b** iar soluția ecuației **y•a**=**b** este **y**=**a/b**.

Operațiile „\” și „ /” sunt operații binare care se numesc respectiv *diviziune de stânga* și *diviziune de dreapta* și care fiind definite pe mulțimea Q se obțin respectiv quasigruprile (**Q**, \) și (**Q**, /) [1]. În continuare, vom arăta o metodă de construcție a qusigrupului *(Q*, *)* pornind de la quasigrupul (**Q**,•).

3. Construcția quasigrupului (Q,\)

Mai jos vom arăta cum se poate de obținut quasigrupul **(Q,\) transformând quasigrupul inițial** (**Q**, •).

Fie mulțimea **Q**={1,2,3}. Definim operație binară „•” în felul următor:

•	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

Cuplul (**Q**, •) este quasigrup. Fiecare din ecuațiile **a•x**=**b** și **y•a**=**b** *au soluții unice în* (**Q**, •). Altfel spus, pe linii și coloane grupoidului dat toate elementele sunt diferite.

Scriem ecuația **a•x**=**b** pentru orice **a**,**b**∈**Q** și determinăm soluțiile pentru ecuațiile respective utilizând relația **x**=**a****b** :

Pentru	**a** • **x** = **b**	avem	**x** = **a** \ **b**	deoarece **a** • (**a** \ **b**) =**b**
1)	1 • **x** = 1	=>	x = 1 \ 1 = 1,	1 • 1 = 1;
2)	1 • **x** = 2	=>	x = 1 \ 2 = 2,	1 • 2 = 2;
3)	1 • **x** = 3	=>	x = 1 \ 3 = 3,	1 • 3 = 3;
4)	2 • **x** = 3	=>	x = 2 \ 3 = 1,	2 • 1 = 3;
5)	2 • **x** = 1	=>	x = 2 \ 1 = 2, deoarece	2 • 2 = 1;
6)	2 • **x** = 2	=>	x = 2 \ 2 = 3,	2 • 3 = 2;
7)	3 • **x** = 2	=>	x = 3 \ 2 = 1,	3 • 1 = 2;
8)	3 • **x** = 3	=>	x = 3 \ 3 = 2,	3 • 2 = 3;
9)	3 • **x** = 1	=>	x = 3 \ 1 = 3,	3 • 3 = 1.

Astfel, pe mulțimea Q poate fi definită operația binară ”\” în felul următor:

\	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

În așa mod, am obținut quasigrupul (Q,\). Quasigrupul (**Q**, •) nu este isomorf cu (Q,\). Similar se poate construi și quasigrupul (**Q**, **/**).

4. Algoritmul criptografic Markovski

Mai jos vom descrie o metodă de construcție a algoritmului Markovski [2, 3]. Algoritmul Markovski presupune realizarea următorilor pași.

P_1. Se definește alfabetul **Al** (cu un număr arbitrar de caractere **n**).

Exemplu: $\mathbf{Al} = \underbrace{\{A, B, C, D, E, \ldots\}}_{\mathbf{n}\text{ elemente}}$.

P_2. Fie este dat mulțimea **Q** = {1, 2, 3,…, **n**}. Definim operația binară „•” astfel încât să obținem quasigrupul (**Q**, •) de dimensiunea **n**.

P_3. Se stabilește o corespondență biunivocă între elementele alfabetului **Al** și elementele mulțimii **Q**, prin intermediul funcției bijective **F** în felul următor:

F : **Al** → **Q**. Dacă **F** : **Al** → **Q** este o funcție bijectivă, atunci inversa funcției **F** va fi funcția $\mathbf{F}^{-1}$: **Q** →**Al** care asociază fiecărui element **y** din **Q** elementul **x** din **Al** astfel, încât **F**(**x**) = **y**. Mai jos vom utiliza și aplicația inversă F^{-1} .

Fie aplicația **F** este definită în felul următor **F**('**A**') = 1, **F**('**B**') = 2, **F**('**C**') = 3, **F**('**D**') = 4, **F**('**E**') = 5, …. Or, aplicația respectivă poate fi reprezentată în felul următor:

A	B	C	D	E	...
1	2	3	4	5	...

n elemente

P_4. Se alege cheia **k** , care este unul din elementele mulțimii **Q**.

Exemplu: Dacă mulțimea **Q** este alcătuită din 4 elemente, atunci **k**, de exemplu, poate fi oricare din aceste elemente.

P_5. Se construiește quasigrupul (**Q**, \) de dimensiunea **n**, în conformitate cu pașii descriși în secțiunea 3.

P_6. Se scrie mesajul secret $\mathbf{M} = \{\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_m\}$ cu simboluri din alfabetul $a_i \in \mathbf{Al}$, unde $1 \leq i \leq \boldsymbol{m}$, iar **m** este lungimea mesajului.

Exemplu: **M** = {A, B, A, C}, unde **m** = 4.

P_7. În baza aplicației **F**, pentru fiecare simbol al mesajului secret $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_m$, se identifică elementele corespunzătoare din mulțimea **Q**. Altfel spus, $\mathbf{F(a_i) = r_i}$. $1 \leq i \leq \boldsymbol{m}$. În așa fel, se obține mulțimea de elemente $\mathbf{R} = \{ \mathbf{r}_1, \mathbf{r}_2, ..., \mathbf{r}_m \}$. Astfel, avem identificată următoarea corespondență:

$\mathbf{a}_1$	$\mathbf{a}_2$	$\mathbf{a}_3$	...	$\mathbf{a}_m$
$\mathbf{r}_1$	$\mathbf{r}_2$	$\mathbf{r}_3$	...	$\mathbf{r}_m$

unde $\mathbf{r}_1, \mathbf{r}_2, ..., \mathbf{r}_m$ sunt imaginile simbolurilor $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_m$ din **M**, care este o submulțime din **Al**, la aplicația $\mathbf{F} : \mathbf{Al} \rightarrow \mathbf{Q}$. Exemplu:

M:	A	B	A	C
R:	1	2	1	3
	$\mathbf{r}_1$	$\mathbf{r}_2$	$\mathbf{r}_3$	$\mathbf{r}_4$

P_8. Se criptează mesajul secret prin intermediul operației binare „\” în conformitate cu realizarea următorilor pași:

$$\mathbf{b}_1 = \mathbf{k} \setminus \mathbf{r}_1;$$
$$\mathbf{b}_2 = \mathbf{b}_1 \setminus \mathbf{r}_2;$$
$$\mathbf{b}_3 = \mathbf{b}_2 \setminus \mathbf{r}_3;$$
$$... ... ...$$
$$\mathbf{b}_m = \mathbf{b}_{m-1} \setminus \mathbf{r}_m;$$

unde $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, ..., \mathbf{b}_m$ sunt valorile din **Q** ale mesajului criptat.

P_9. Se decriptează mesajul secret efectuând următorii pași:

$$\mathbf{u}_1 = \mathbf{k} \bullet \mathbf{b}_1;$$
$$\mathbf{u}_2 = \mathbf{b}_1 \bullet \mathbf{b}_2;$$
$$\mathbf{u}_3 = \mathbf{b}_2 \bullet \mathbf{b}_3;$$
$$... ... ...$$
$$\mathbf{u}_m = \mathbf{b}_{m-1} \bullet \mathbf{b}_m;$$

unde $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, ..., \mathbf{u}_m$ sunt valorile din **Q** ale mesajului decriptat.

P_{10}. Se restabilește mesajul scris folosind aplicația bijectivă $F^{-1} : Q \rightarrow Al$, unde $F^{-1}(\mathbf{u}_1) = a_1$, $F^{-1}(\mathbf{u}_2) = a_2$, …, $F^{-1}(\mathbf{u}_m) = a_m$. Ori aplicația $\mathbf{F}^{-1}$ poate fi reprezentată în felul următor:

$\mathbf{u}_1$	$\mathbf{u}_2$	$\mathbf{u}_3$	...	$\mathbf{u}_m$
$\mathbf{a}_1$	$\mathbf{a}_2$	$\mathbf{a}_3$	...	$\mathbf{a}_m$

P_{11}. Afișăm mesajul secret.

5. Aplicarea algoritmului criptografic Markovski

Să examinăm aplicarea algoritmului Markovski la soluționarea următoarei probleme.

PROBLEMĂ. Fie interlocutorul **A** trebuie să transmită un mesaj secret interlocutorului **B**. Interlocutorul **A** decide să stabilească numărul de simboluri ale alfabetului **Al** în funcție de mesajul secret **M** = {C, E, T, A, T, E}. Astfel, alfabetul definit de interlocutorul **A** pentru mesajul **M** este **Al** = {A, C, E, T}. Deoarece **Al** constă din 4 elemente, atunci interlocutorul **A** decide că și mulțimea **Q** la fel va avea 4 elemente. Deci, **Q** = {1, 2, 3, 4}. Pe mulțimea **Q**, interlocutorul **A** definește operația binară „•” astfel, încât obține quasigrupul (**Q**, •).

•	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	4	1	2	3
4	3	4	1	2

Interlocutorul **A** definește funcția bijectivă **F** : **Al** → **Q** și $\mathbf{F}^{-1}$: **Q** → **Al** în conformitate cu tabelul de mai jos:

A	C	E	T
1	2	3	4

Interlocutorul **A** decide ca cheia secretă va fi **k** = 3.

Să se descrie pașii care trebuie sa fie realizați de interlocutorul **A** pentru a cripta și a transmite mesajul secret, precum și pașii care trebuie întreprinși de interlocutorul **B** pentru a decripta mesajul, utilizând algoritmul Markovski.

Soluție. *Interlocutorul* **A** *efectuează următorii pași.*

P_1. Definește alfabetul **Al** din 4 caractere: **Al** = {A, C, E, T } și mulțimea **Q** = {1, 2, 3, 4}.

P_2. Pe mulțimea Q definește operația binară „•” obținând quasigrupul (**Q**, •) de ordinul 4:

•	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	4	1	2	3

4	3	4	1	2

P_3. Stabilește o corespondență biunivocă **F** între alfabetul **Al** și elementele mulțimii **Q**, adică **F** : **Al** → **Q**

A	C	E	T
1	2	3	4

P_4. Alege și utilizează cheia de criptare **k** = 3.

P_5. Se construiește quasigrupul (**Q**, \) de ordinul 4. În acest scop se scriu ecuațiile **a** • **x** = **b** pentru orice ∀ **a**, **b** ∈ (**Q**, •).

Pentru **a** • **x** = **b**		avem	**x** = **a** \ **b**	deoarece	**a** • (**a** \ **b**) = **b.**
1)	1 • **x** = 1		**x** = 1 \ 1 = 1,		1 • 1 = 1;
2)	1 • **x** = 2		**x** = 1 \ 2 = 2,		1 • 2 = 2;
3)	1 • **x** = 3		**x** = 1 \ 3 = 3,		1 • 3 = 3;
4)	1 • **x** = 4		**x** = 1 \ 4 = 4,		1 • 4 = 4;
5)	2 • **x** = 1		**x** = 2 \ 1 = 4,		2 • 4 = 1;
6)	2 • **x** = 2		**x** = 2 \ 2 = 1,		2 • 1 = 2;
7)	2 • **x** = 3		**x** = 2 \ 3 = 2,		2 • 2 = 3;
8)	2 • **x** = 4		**x** = 2 \ 4 = 3,		2 • 3 = 4;
9)	3 • **x** = 1	=>	**x** = 3 \ 1 = 2,	deoarece	3 • 2 = 1;
10)	3 • **x** = 2		**x** = 3 \ 2 = 3,		3 • 3 = 2;
11)	3 • **x** = 3		**x** = 3 \ 3 = 4,		3 • 4 = 3;
12)	3 • **x** = 4		**x** = 3 \ 4 = 1,		3 • 1 = 4;
13)	4 • **x** = 1		**x** = 4 \ 1 = 3,		4 • 3 = 1;
14)	4 • **x** = 2		**x** = 4 \ 2 = 4,		4 • 4 = 2;
15)	4 • **x** = 3		**x** = 4 \ 3 = 1,		4 • 1 = 3;
16)	4 • **x** = 4		**x** = 4 \ 4 = 2,		4 • 2 = 4;

Astfel, se obține quasigrupul (**Q**, \):

\	1	2	3	4
1	1	2	3	4
2	4	1	2	3
3	2	3	4	1
4	3	4	1	2

Interlocutorul **A** transmite, printr-un canal secret, interlocutorului **B**, cheia **k**, quasigrupul (**Q**, •) și funcția $\mathbf{F}^{-1}$: **Q** → **Al**.

Interlocutorul **A** *criptează mesajul secret.*

P_6. Interlocutorul **A** scrie mesajul secret **M** = {C, E, T, A, T, E}.

P_7. Aplicând funcția bijectivă F : Al → Q, fiecărui element al mesajului secret M, care este alcătuit din elemente ale alfabetului **Al**, i se pune în corespondență

elementul respectiv din mulțimea Q. În felul acesta, se formează mulțimea (mesajul) **R (**alcătuită din elemente ale mulțimii **Q)** care trebuie criptat.

M:	C	E	T	A	T	E
R:	2	3	4	1	4	3
	$\mathbf{r}_1$	$\mathbf{r}_2$	$\mathbf{r}_3$	$\mathbf{r}_4$	$\mathbf{r}_5$	$\mathbf{r}_6$

P_8. Interlocutorul **A** criptează mesajul **R**, utilizând operațiile din (**Q**, \) și efectuând următorii pași:

$$\mathbf{b}_1 = \mathbf{k} \setminus \mathbf{r}_1 = 3\backslash 2 = 3;$$
$$\mathbf{b}_2 = \mathbf{b}_1 \setminus \mathbf{r}_2 = 3\backslash 3 = 4;$$
$$\mathbf{b}_3 = \mathbf{b}_2 \setminus \mathbf{r}_3 = 4\backslash 4 = 2;$$
$$\mathbf{b}_4 = \mathbf{b}_3 \setminus \mathbf{r}_4 = 2\backslash 1 = 4;$$
$$\mathbf{b}_5 = \mathbf{b}_4 \setminus \mathbf{r}_5 = 4\backslash 4 = 2;$$
$$\mathbf{b}_6 = \mathbf{b}_5 \setminus \mathbf{r}_6 = 2\backslash 3 = 2;$$

Astfel, interlocutorul **A** obține mesajul criptat: **B** = { 3, 4, 2, 4, 2, 2}, unde

$\mathbf{b}_1$	$\mathbf{b}_2$	$\mathbf{b}_3$	$\mathbf{b}_4$	$\mathbf{b}_5$	$\mathbf{b}_6$
3	4	2	4	2	2

Interlocutorul **A** transmite mesajul criptat interlocutorului **B** prin intermediul unui canal deschis. *În continuare interlocutorul* **B** *efectuează paşii* $P_9 - P_{11}$.

P_9. Interlocutorul **B** recepționează mesajul criptat și dorește sa-l decripteze. În acest scop el va utiliza cheia secretă k, quasigrupul (**Q**, •) și funcția bijectivă $F^{-1} : Q \rightarrow Al$, recepționate prin canalul secret. Interlocutorul **B**, decriptează mesajul {$\mathbf{b}_1$, $\mathbf{b}_2$, $\mathbf{b}_3$, $\mathbf{b}_4$, $\mathbf{b}_5$, $\mathbf{b}_6$} sau {3, 4, 2, 4, 2, 2} folosind operația binară „•” și cheia k :

$$\mathbf{u}_1 = \mathbf{k} \bullet \mathbf{b}_1 = 3 \bullet 3 = 2$$
$$\mathbf{u}_2 = \mathbf{b}_1 \bullet \mathbf{b}_2 = 3 \bullet 4 = 3$$
$$\mathbf{u}_3 = \mathbf{b}_2 \bullet \mathbf{b}_3 = 4 \bullet 2 = 4$$
$$\mathbf{u}_4 = \mathbf{b}_3 \bullet \mathbf{b}_4 = 2 \bullet 4 = 1$$
$$\mathbf{u}_5 = \mathbf{b}_4 \bullet \mathbf{b}_5 = 4 \bullet 2 = 4$$
$$\mathbf{u}_6 = \mathbf{b}_5 \bullet \mathbf{b}_6 = 2 \bullet 2 = 3$$

Astfel, interlocutorul **B** obține mesajul decriptat **U** cu elemente din **Q**. În așa fel, obține **U** = {2, 3, 4, 1, 4, 3} și corespondența respectivă:

$\mathbf{u}_1$	$\mathbf{u}_2$	$\mathbf{u}_3$	$\mathbf{u}_4$	$\mathbf{u}_5$	$\mathbf{u}_6$
2	3	4	1	4	3

P_{10}. Interlocutorul **B** restabilește mesajul secret folosind elemente din alfabetul **Al** și funcția inversă $F^{-1} : Q \rightarrow Al$ definită la pasul P_4. Astfel, avem $\boldsymbol{F^{-1}(u_i)} = a_i$, unde $\boldsymbol{u_i \in U \subseteq Q}$ și $a_i \in Al$, $\boldsymbol{1 \leq i \leq 6}$. Așa dar, $F^{-1}(\mathbf{2}) = C$, $F^{-1}(\mathbf{3}) = E$, $F^{-1}(\mathbf{4}) = T$, $F^{-1}(\mathbf{1}) = A$, $F^{-1}(\mathbf{4}) = T$, $F^{-1}(\mathbf{3}) = E$. Ori:

u_1	u_2	u_3	u_4	u_5	u_6
2	3	4	1	4	3
C	E	T	A	T	E

P_{11}. Interlocutorul **B**, citește mesajul secret: CETATE.

O reprezentare grafică al aplicării algoritmului Markovski este redată în figura 1, unde interlocutorul **A** transmite mesaje criptate spre interlocutorul **B** care le decriptează: 1. Se determină alfabetul; 2. Interlocutorul **A** stabilește cheia secretă; 3. Printr-un canal închis, secret, interlocutorul **A** transmite lui B cheia secretă k, quasigrupul (**Q**, •) și funcția inversă F^{-1} : Q →Al 4. Interlocutorul **A** criptează mesajul; 5. Printr-un canal deschis, interlocutorul **A** transmite interlocutorului **B** mesajul criptat; 6. Interlocutorul **B** decriptează mesajul.

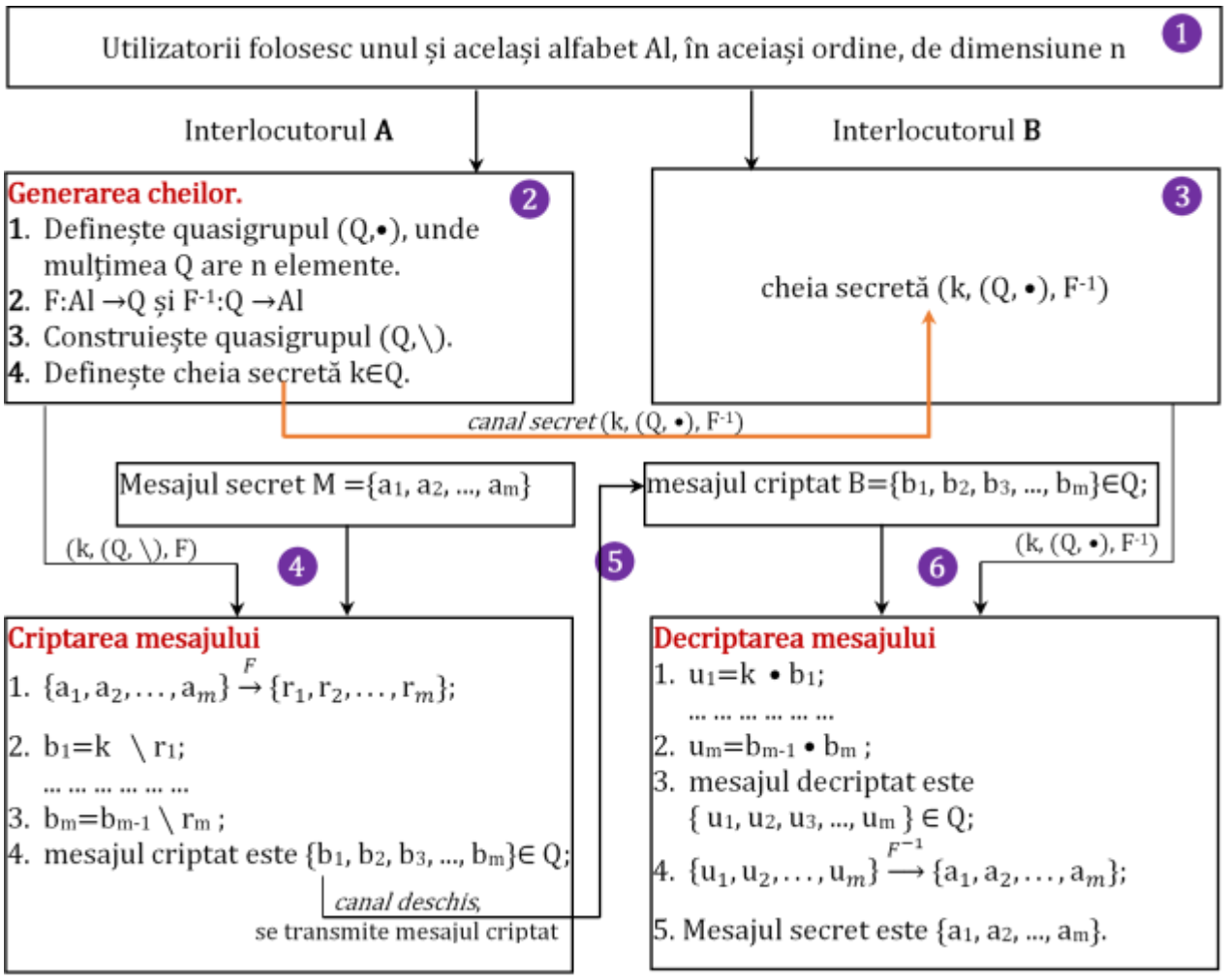

Figura 1. Etapele aplicării algoritmului de criptare Markovski

6. Programul C++ pentru algoritmul criptografic Markovski

Pentru a implementa algoritmul Markovski a fost elaborat un program C++ care efectuează toți pașii P1-P9 descriși mai sus.

Mai jos este prezentat fragmentul de program care realizează criptarea (P8) și decriptarea (P9) mesajului secret.

```
void mCriptare(int k, int Q[nn][nn], int R[nn], int m, int B[nn]){
     int i=1;
     B[i]=Q[k][R[i]];
     for (i=2; i<=m; i++){
     B[i]=Q[B[i-1]][R[i]];
     }}
void mDecriptare(int k,int Q[nn][nn],int B[nn],int m,int U[nn]){
     int i=1;
     U[i]=Q[k][B[i]];
     for (i=2; i<=m; i++){
     U[i]=Q[B[i-1]][B[i]];
     }}
```

Apel la aceste funcţii se realizează după cum urmează:

mCriptare(k,S,R,m, B), unde **S** este operaţia quasigrupului (Q,\).

mDecriptare(k,P,B,m, U), unde **P** este operaţia quasigrupului (Q,*).

Rezultatul realizării programului:

```
Introdu alfabetul cu litere MARI Al= ACET
Introdu cheia k= 3
Introdu operatia quasigrupului (Q, *) de dimensiunea 4
 *| 1 2 3 4
--+------------
 1| 1 2 3 4
 2| 2 3 4 1
 3| 4 1 2 3
 4| 3 4 1 2
Introdu mesajul (cu litere MARI) M= CETATE
R= {2, 3, 4, 1, 4, 3}
CRIPTARE
(Q,\)={1, 2, 3, 4};
Cu operatia binara:
 \| 1 2 3 4
--+------------
 1| 1 2 3 4
 2| 4 1 2 3
 3| 2 3 4 1
 4| 3 4 1 2
B= {3, 4, 2, 4, 2, 2}
Mesajul criptat: ETCTCC
DECRIPTARE
Se foloseste operatia quasigrupului (Q,*)
U= {2, 3, 4, 1, 4, 3}
Mesajul decriptat: CETATE
```

Concluzii. În utilizarea algoritmului Markovski în procesul de criptare a informaţiei sunt utilizate următoarele noţiuni şi concepte din algebra abstractă: operaţie binară, grupoid, grup, quasigroup, operaţia binară „diviziune stânga” în quasigroup, operaţia binară

„diviziune dreapta” în quaisgroup, corespondență biunivocă, funcție bijectivă, funcție inversă, construcția quasigrupului (Q, \) și construcția quasigrupului (Q, /). Fără cunoașterea acestor noțiuni și metode este imposibilă înțelegerea și aplicarea algoritmului Markovski. Din aceste considerente pregătirea specialiștilor în informatică necesită o pregătire fundamentală în algebra abstractă. Dezvoltarea și aplicarea unor algoritmi criptografici performanți necesită cunoștințe profunde în algebra abstractă aplicată, teoria numerelor, structuri algebrice, sisteme algebrice neasociative etc. Într-o perspectivă apropiată se prefigurează noi implementări ale criptografiei în domenii care țin de tehnologii SMART, robotică, Internet of Things, Cloud Computing, securitate casnică etc. Toate argumentele punctate mai conduc la necesitatea revizuirii programelor de studii care țin de pregătirea studenților informaticieni (atât de la licență, cât și de la masterat) și corelarea lor cu cerințele stringente ale pieței muncii din domeniul IT.

Bibliografie

1. Belousov V. D. Foundation of the theory of quasigroups and loops. Moscow, Nauka, 1967.
2. Markovski S., Gligoroski D., Bakeva V. Quasigroups and hash functions. In: Res. Math. Comput. Sci., volume 6, p. 43–50. Blagoevgrad: SouthWest Univ., 2002.
3. Markovski S., Gligoroski D., Stojcevska B. Secure two-way on-line communication by using quasigroup enciphering. Novi Sad J. Math., 2000. Vol. 30, no. 2, p. 43-49.
4. Simion E., Naccache D. Criptografie și securitatea informațiilor. Aplicații. Matrixrom, 2011. ISBN: 9789737556752. 107 p.
5. Мирзоев М.С. Математическая культура учителя информатики: теоретико-методический аспект: монография. Прометей М, 2015. 305 с.
6. Козлов В.Н. Математика и информатика: Учеб. пособие. Москва, 2004. 266 с.
7. Коджаспирова Г.М., Коджаспиров А.Ю. Педагогический словарь: для студ. высш. и сред. пед. Учеб. заведений. М.: «Академия», 2001. 176 с.
8. Sherbacov V. A. Quasigroups in cryptology. Computer Sci. J. Moldova 17(2) (2009), p. 193-228.
9. Chiriac L., Danilov A., Bogdanova V. Utilizarea conceptelor din teoria numerelor in elaborarea algoritmilor criptografici asimetrici. În: Învăţământ superior: tradiţii, valori, perspective. Vol. 1. Ch.: UST, 29-30 septembrie 2020. p. 239-247.

Articolul este elaborat în cadrul proiectului de cercetări științifice „Metodologia implementării TIC în procesul de studiere a științelor reale în sistemul de educație din Republica Moldova din perspectiva inter/transdisciplinarității (concept STEAM)”, inclus în „Program de stat” (2020-2023), Prioritatea IV: Provocări societale, cifrul 20.80009.0807.20