Acta et Commentationes, Sciences of Education, nr. 2(36), 2024 ISSN 1857-0623
p. 10-25 E-ISSN 2587-3636

CZU: 004.6+51 DOI: 10.36120/2587-3636.v36i2.10-25

ALGORITMI DE DISTRIBUIRE A CHEILOR CRIPTOGRAFICE

Liubomir CHIRIAC, dr. hab. prof. univ.
https://orcid.org/0000-0002-5786-5828
Natalia JOSU, dr., conf. univ.
https://orcid.org/0000-0002-3687-5437
Violeta BOGDANOVA, dr., asistent
https://orcid.org/0000-0003-4140-6317
Catedra Informatică și Tehnologii Informaționale
Universitatea Pedagogică de Stat „Ion Creangă" din Chișinău

Rezumat. În articolul respectiv sunt examinați algoritmii privind schimbul de chei publice aplicând algoritmul Diffie-Helmann-Merkel pentru grupuri comutative și Stickel - Shpilrain pentru grupuri necomutative. Schimbul de chei după protocolul Diffie–Hellman-Merkel și Stickel - Shpilrain reprezintă metode matematice privind schimbul securizat de chei criptografice prin intermediul unui canal public. Algoritmul Diffie-Helmann-Merkel este unul dintre primele protocoale de chei publice în domeniul criptografiei. Autorii examinează implementarea algoritmilor respectivi prin intermediul structurilor algebrice abeliene și neabeline bazându-se pe problema logaritmului discret. La fel este examinat atacul „man-in-the-middle" și sunt construite exemple care ilustrează funcționarea algoritmilor menționați.
Cuvinte cheie: sistem criptografic, problema logaritmului discret, schimbul de chei Diffie-Helmann-Merkel, protocolul Stickel – Shpilrain, atac man-in-the-middle, grupuri abeliene și neabeliene.

CRYPTOGRAPHIC KEY DISTRIBUTION ALGORITHMS

Abstract. This article examines public key exchange algorithms applying the Diffie-Helmann-Merkel algorithm for commutative groups and the Stickel-Shpilrain algorithm for non-commutative groups. The protocols Diffie–Hellman–Merkel and Stickel–Spilrain key exchange are mathematical methods for the secure exchange of cryptographic keys over a public channel. The Diffie-Helmann-Merkel algorithm is one of the first public key protocols in cryptography. The authors examine the implementation of the respective algorithms through abelian and non-abelian algebraic structures based on the discrete logarithm problem. The man-in-the-middle attack is also examined. Examples are constructed that illustrate the operation of the mentioned algorithms.
Keywords: cryptographic system, discrete logarithm problem, Diffie-Helmann-Merkel key exchange, Stickel – Shpilrain protocol, man-in-the-middle attack, abelian and non-abelian groups.

1. Criptologia – noțiuni generale. Scurt istoric

Criptografia este o ramură a matematicii și informaticii aplicate, folosită pentru descrierea procesului de securizare a informației, autentificării și restricționării accesului într-un sistem informatic.

Astfel, termenul de criptografie derivă din cuvintele de origine greacă κρυπτός (kryptós – *ascuns*) și γράφειν (gráfein – *a scrie*).

Procesul de conversie sau de codificare a unui text clar într-unul *criptic* (numit text cifrat) se numeşte *criptare*.

Procesul invers, de conversie (de decodificare) a textului cifrat într-un text clar se numeşte *decriptare*.

Procedurile de criptare și decriptare constituie împreună ceea ce este cunoscut sub numele de *algoritm de criptare*.

Majoritatea algoritmilor de criptare țin de domeniul public, adică sunt cunoscuți. Caracterul secret (privat) al comunicării este determinat de utilizarea unei chei de criptare/decriptare, care este cunoscută doar de interlocutorii cu acest drept.

Se consideră că primele principii care se referă la construcția unui algoritm criptografic modern au fost propuse de Auguste Kerckhoffs (19 ianuarie 1835 – 9 august 1903) lingvist și criptograf olandez, la sfârșitul secolului al XIX-lea.

În anul 1883 în revista *Le Journal des Sciences Militaires* (Revista de științe militare), întitulată *La Cryptographie Militaire* (Criptografie militară) publică un articol în două părți. În premieră în articolul respectiv enunță principiile, actuale și astăzi, și care se află la baza construcției unui algoritm criptografic:

- *Sistemul construit ar trebui să fie, dacă nu teoretic greu de spart, atunci în practică ar trebui să fie indestructibil.*
- *Proiectarea unui sistem criptografic nu ar trebui să genereze probleme în cazul compromiterii unor detalii și să îngreuneze „discuția" interlocutorilor.*
- *Cheia sistemului construit ar trebui să fie memorabilă și ar trebui să fie ușor de schimbat.*
- *Criptogramele ar trebui să fie ușor transmisibile prin intermediului telegrafului.*
- *Echipamentul (aparatul) de criptare sau documentele trebuie să fie portabile și operabile de o singură persoană.*
- *Sistemul ar trebui să fie ușor, să nu necesite cunoașterea unei liste lungi de reguli și nici să nu implice efort mental.*

Principiile lui Auguste Kerckhoffs punctate mai sus au marcat o nouă etapă în dezvoltarea criptologiei. Codul lui Gilbert Sandford Vernam (3 aprilie 1890 – 7 februarie 1960), cunoscut până la moment sub numele de codul Vernam și în varianta ușor modificată, cunoscut ca *one-time-pad*, rămâne a fi singurul cod cu securitate necondiționată.

În opinia unor experți în domeniul criptologiei, criptografia modernă începe cu Claude Elwood Shannon (30 aprilie 1916 – 24 februarie 2001), matematician, inginer electrician, informatician și criptograf american cunoscut drept „părintele teoriei informației". El a fost primul care a descris porțile booleene (circuite electronice), care sunt esențiale pentru toate circuitele electronice digitale și a construit primul dispozitiv de învățare automată, întemeind astfel domeniul inteligenței artificiale, și totodată, direcționează dezvoltarea criptografiei sub egida criptografiei bazată pe matematică.

Alte contribuții majore la dezvoltarea criptografiei moderne au fost: codul lui Horst Feistel și criptosistemul cu cheie publică Diffie-Hellman-Merkle [1, 2, 3].

Criptograful american de origine germană Horst Feistel (30 ianuarie 1915 – 14 noiembrie 1990) a lucrat la proiectarea cifrurilor la *IBM*, inițiind cercetări care au culminat cu dezvoltarea standardului de criptare a datelor (*DES*) în anii 1970. Structura folosită în *DES*, numită rețea Feistel, este folosită în mod obișnuit în multe cifruri bloc.

Inventarea criptosistemului cu cheie publică Diffie-Hellman-Merkle, denotă startul dezvoltării criptografiei moderne și trecerea criptografiei tradiționale care ținea de domeniu militar în domeniu public de cercetare academic.

2. Criptografia cu cheie publică ori criptarea asimetrică

Deoarece în cadrul criptării simetrice (criptarea cu cheie secretă) nu puteau fi soluționate următoarele două probleme fundamentale în securitate:

a) transmisia de informații prin intermediul unui canal slab securizat (nesigur și care necesită pentru interlocutori o cheie secretă utilizată pentru criptare și decriptare);
b) posibilitatea de a semna digital informația care urmează să fie transmisă;

s-a dat startul dezvoltării criptografiei cu cheie publică, care nu necesită neapărat un canal sigur de comunicare.

În cadrul sistemului de criptare cu cheie publică problemele menționate mai sus pot fi soluționate pozitiv, deoarece cheia publică chiar dacă este interceptată nu conduce la decriptarea mesajului criptat. Unele idei în acest sens au fost examinate în [6-15].

Decriptarea, citirea din criptotext a mesajului original, o poate face doar interlocutorul care posedă cheia privată (cheia de decriptare ori cheia asimetrică).

Astfel, Bailey Whitfield Diffie (născut la 5 iunie 1944) criptograf și matematician american, interesat de topologie și ecuații diferențiale, alături de Martin Hellman (născut la 2 octombrie 1945) și Ralph Merkle (născut la 2 februarie 1952) sunt considerați pionierii criptografiei cu cheie publică. Lucrarea lui Diffie și Hellman „New Directions in Cryptography” [1] publicată în anul 1976, a introdus o metodă nouă de distribuire a cheilor criptografice, care a contribuit radical la dezvoltarea metodelor care țin de distribuția cheilor – o problemă fundamentală în criptografie. Articolul a stimulat dezvoltarea unei noi clase de algoritmi de criptare, algoritmii cu cheie asimetrică.

Se cunoaște, însă, că în 1974 Ralph Merkle a elaborat o construcție pentru un criptosistem, numită astăzi, Merkle's Puzzles, care funcționa având la bază conceptul de cheie publică, iar lucrarea, în care a fost argumentat și prezentat acest concept, a fost publicată în anul 1978 [2, 3].

După cum susține chiar Martin Hellman, descoperirea conceptului de criptare cu cheie publică îi aparține lui Ralph Merkle (în prefața de la cartea lui Yan [5]).

În acest sens, Whitfield Diffie, Martin Hellman și Ralph Merkle sunt considerați cercetătorii care au dezvoltat și au publicat conceptul criptării cu cheia publică, o metodă inovatoare pentru securizarea comunicațiilor electronice. Menirea conceptului respectiv este *distribuirea cheilor*, adică scopul este ca utilizatori să poată schimba o cheie secretă în siguranță, deci algoritmul este limitat, în mare parte, la schimbul cheilor secrete.

3. Noțiuni matematice de bază

Un grup este o structură algebrică formată dintr-o mulțime și o operație binară care este asociativă, are element neutru și elementele mulțimii sunt simetrizabile.

În termeni matematici un grup abstract reprezintă un cuplu (G, ▫) unde G este o mulțime nevidă iar (▫) este o operație binară, asociativă, care admite un element neutru e ∈ G, astfel încât pentru $\forall\, x \in G$, $e \,▫\, x = x \,▫\, e = x$ și pentru fiecare $x \in G$ există un element simetric $x^{-1} \in G$, încât $x \,▫\, x^{-1} = x^{-1} \,▫\, x = e$.

Dacă în grupul G este definită operația de înmulțire (·), atunci grupul $(G,\cdot)$ se numește *grup multiplicativ*. Ordinul unui grup G, notat $ord(G)$ sau $|G|$, reprezintă numărul elementelor grupului.

Fie grupul $(G, ▫)$ și e este elementul neutru. Vom spune că elementul g este de *ordinul m*, dacă $min\{m \in N^*: g^m = e\} = ord(g)$.

Fie Z_n^* este un grup. Elementul $g \in Z_n^*$ se numește generator ori rădăcină primitivă a grupului Z_n^* dacă pentru orice element $a \in Z_n^*$ se găsește așa un număr întreg k, astfel încât $g^k = a$.

Notăm $< g >= \{ g^k : k = 0, \dots, n-1 \} = \{ g^0, g^1, \dots, g^{n-1} \}$. Mulțimea $< g >$ reprezintă grupul format din elementele generate de g. Nu întotdeauna mulțimea generată de $< g >$ coincide cu întreg grupul examinat, adică $< g > \neq Z_n^*$. Dacă $< g > = Z_n^*$ vom spune că elementul g este generator al grupului Z_n^*.

Un *grup ciclic multiplicativ* este un grup ale cărui elemente sunt puteri ale unui element g din grup. Pentru comoditate și exactitate vom considera G – un grup multiplicativ Z_p^* de ordin $p - 1$, cu p – număr prim, unde operația este înmulțirea $modulo\ p$.

Un *grup finit generat* este un grup G care are o mulțime finită R de generatori, astfel încât orice element al lui G să poată fi scris ca o combinație (prin operația grupului) de un număr finit de elemente ale R.

Evidențiem următoarele proprietăți:

- Prin definiție, *orice grup finit* este și finit generat.
- Grupul care este generat de un singur element se numește *ciclic*.
- Orice grup ciclic este comutativ.
- *Orice grup ciclic infinit* este izomorf cu grupul aditiv al numerelor întregi *Z*.
- *Un subgrup al unui grup finit generat* nu este neapărat finit generat.

Exemplu A. Fie $p = 11$. Atunci $Z_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$ are ordinul $p - 1 = 10$. În tabelul de mai jos calculăm elementele $2^i \ mod\ 11$, $3^i \ mod\ 11$, $5^i \ mod\ 11$, $6^i \ mod\ 11$ pentru $i = 0,\ldots,9$.

i	0	1	2	3	4	5	6	7	8	9
$2^i \ mod\ 11$	1	2	4	8	5	10	9	7	3	6
$3^i \ mod\ 11$	1	3	9	5	4	1	3	9	5	4
$5^i \ mod\ 11$	1	5	3	4	9	1	5	3	4	9
$6^i \ mod\ 11$	1	6	3	7	9	10	5	8	4	2

Evident, $< 2 > = \{1,2,4,8,5,10,9,7,3,6\} = Z_{11}^*$ și $< 6 >= \{1,6,3,7,9,10,5,8,4,2\} = Z_{11}^*$ sunt generatori. Iar $< 3 > = < 5 > = \{1, 3, 4, 5, 9\}$ este un subgrup al grupului Z_{11}^*. Ușor se poate demonstra că generatorii grupului Z_{11}^* sunt $\{2, 6, 7, 8\}$. Iar grupul Z_7^*, de exemplu, are doi generatori *3* și *5*: $< 3 > = < 5 > \{1, 2, 3, 4, 5, 6\}$.

Fie G - un grup ciclic de ordinul n şi g – elementul generator al său. Fie d – un element din G. Atunci, *logaritmul discret* d în baza g (notăm: $\log_g(d)$), este unicul număr întreg $a, 0 \leq a \leq |G| - 1$, astfel încât $d = g^a$.

Problema Logaritmului Discret (DLP – *Discrete Logarithms Problem*)

Problema DLP constă în următoarele: Fie grupul ciclic finit $G = Z_p^*$, un generator g al lui G şi un element y din G. Se cere să se găsească un număr întreg a, pentru care $0 \leq a \leq p - 2$, astfel încât $y = g^a (mod\ p)$.

Noțiunea de *logaritm discret* este similară cu noțiunea de logaritm. Să examinăm unele proprietăți în acest sens. Se știe că *ordinul elementului u după modulo p* este cel mai mic număr întreg pozitiv astfel încât $u^k = 1 \ mod\ p$. Dacă $u^k = 1 \ mod\ p$ și $u^n = 1 \ mod\ p$, atunci k divide n. În acest caz, putem scrie că $\log_g y = a \ mod\ t$ este echivalent cu $y = g^a (mod\ p)$, unde t este ordinul elementului g după *modulo p*.

Exemplu B. Să calculăm valoarea logaritmului discret în grupul ciclic Z_{11}^* pentru *generatorii* $\{2, 6, 7, 8\}$. Obținem următorul tabel:

a	1	2	3	4	5	6	7	8	9	10
$\log_2(a)$	0	1	8	2	4	9	7	3	6	5
$\log_6(a)$	0	9	2	8	6	1	3	7	4	5
$\log_7(a)$	0	3	4	6	2	7	1	9	8	5
$\log_8(a)$	0	7	6	4	8	3	9	1	2	5

Se observă, de exemplu, că

$\log_2(3) = 8$, deoarece $2^8 \ mod\ 11 = 3$. La fel, $\log_6(3) = 2$, deoarece $6^2 \ mod\ 11 = 3$. Similar, obținem, $\log_7(3) = 4$, deoarece $7^4 \ mod\ 11 = 3$ și $\log_8(3) = 6$, deoarece $8^6 \ mod\ 11 = 3$.

Dacă t este ordinul lui $g \ modulo\ p$, atunci

logb (ac) = logb (a) + logb (c) (mod t) și *logb (a^s) = s logb (a) (mod t)*.

Fie *t = 10* și *7 modulo 11*, atunci

4·9 = 3 mod 11 și *log7 4+ log7 9 = log7 3(mod 10)* ori *6 +8 = 4 (mod 10)*,

deoarece *10* este ordinul elementului *g=7* după *modulo 11.*

Similar $4^3 = 9 \bmod 11$ și $3 \cdot \log_7 4 = \log_7 9 \pmod{10}$ ori $3 \cdot 6 = 8 \pmod{10}$.

În felul acesta, având tabelul logaritmului discret în raport cu generatorul g *modulo p* este simplu de efectuat calculele necesare.

4. Schema de criptare cu cheia publică

În criptografia tradițională (simetrică), aceeași cheie secretă era utilizată atât pentru a cripta, cât și pentru a decripta un mesaj. Pentru a păstra secretul, cheile trebuie schimbate prin curieri sau alte mijloace sigure de comunicare. În cazul criptării cu cheia publică fiecare individ are propria sa pereche de chei care constă dintr-o *cheie publică și o cheie privată*.

În contextul dat trebuie schimbată doar cheia publică, eliminând nevoia de curieri ori transmiterea prin canale de comunicare. Dacă cheia publică a unei persoane este folosită pentru a cripta un mesaj, atunci numai cheia privată (cheia secretă) corespunzătoare o poate decripta, oferind confidențialitate. La fel, dacă cheia sa privată este folosită pentru a semna (cripta) un mesaj, cheia publică corespunzătoare poate autentifica (decripta) mesajul.

În așa mod *o schemă de criptare cu cheie publică conține trei părți*:

Prima parte. *Se elaborează generatorul de chei, care returnează o pereche de chei: cheia publică (CP) și cheia secretă (CS), notăm (CP, CS);*

Partea a doua. *Se dezvoltă algoritmul de criptare, în care la intrare se introduce mesajul M (textul clar) și cheia publică CP, adică (M,CP) și în urmă execuției se returnează textul cifrat S.*

Partea a treia. *Se dezvoltă algoritmul de decriptare, care la intrare primește textul cifrat S și cheia secretă CS, adică (S,CS) și returnează mesajul decodificat M.*

În acest sens, în prezent, unii dintre cei mai utilizați algoritmi de criptare cu cheie publică sunt: *Algoritmul Merkle-Hellman*, *Algoritmul RSA*, *Algoritmul ElGamal*, *Algoritm pe Curbe Eliptice*, *Algoritmul McEliece*.

În criptografia asimetrică efectuarea „schimbului de chei”, prin intermediul cărora se efectuează criptarea și decriptarea mesajului, reprezintă una din procedurile importante în asigurarea securității.

Mai jos vom descrie diverse proceduri privind efectuarea schimbului de chei. Așa cum am menționat anterior idea centrală a fost concepută de Ralph Merkle și publicată inițial de Whitfiled and Ralph Hellman în anul 1976.

În contextul dat vom examina algoritmul **Diffie-Hellman-Merkel** care se aplică prin intermediul grupurilor abeliene și algoritmul **Stickel** care se utilizează prin

intermediul grupurilor neabeliene și care se fundamentează având la bază problema determinării logaritmului discret și alte noțiuni matematice importante.

5. Algoritmul Diffie-Hellman-Merkel

Problema 1. Fie G – grup ciclic abelian și $|G| = p$, unde p – este un număr prim și g – unul din generatorii grupului G. Se cere să se elaboreze un algoritm de generare a unor chei publice care ar permite interlocutorilor *A* și *B* să genereze chei secrete și să facă schimb de chei.

Problema 1 poate fi soluționată aplicând protocolul **Diffie-Hellman-Merkel.** Mai jos descriem algoritmul **Diffie-Hellman-Merkel** [1]**.**

Pasul 1. Interlocutorii *A* și *B* se înțeleg (cad de comun acord) asupra perechii de numere (p, g) și $ord\ (g) = p$.

Pasul 2. Interlocutorul *A* alege aleator (generează) un număr secret $a, 0 \leq a \leq |G| - 1$ și transmite public interlocutorului *B*, $g^a \ mod\ p$.

Pasul 3. Interlocutorul *B* alege aleator (generează) un număr secret $b, 0 \leq b \leq |G| - 1$ și transmite public interlocutorului *A*, $g^b \ mod\ p$.

Pasul 4. Interlocutorul *A* calculează $K_A = (g^b)^a \ mod$ p $= g^{ba} \ mod$ p.

Pasul 5. Interlocutorul *B* calculează $K_B = (g^a)^b \ mod$ p $= g^{ab} \ mod$ p.

Deoarece *G* este grup comutativ $ab = ba$, interlocutorii *A* și *B* posedă unul și același element al grupului *G*, cheia secretă $CS = K_A = K_B$.

Notă. Sesizăm că oricine, care cunoaște grupul *G* (deci și numărul prim *p*) și are acces la numerele: $g^a \ mod\ p$ și $g^b \ mod\ p$, ar putea să calculeze și generatorul *g,* deoarece sunt cunoscute metodele algebrice pentru determinarea generatorului grupului ciclic. În schimb, fiind date numere prime mari, pentru a calcula logaritmul discret (altfel spus pentru a afla numerele *a* și *b*) este necesar să posede capacități puternice de calcul pentru procesarea numerelor mari.

De exemplu, grupul Z_{71}^* are următorii generatori:

{7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69}.

Admitem că „cineva” utilizând o metodă algebrică determină generatorii grupului respectiv și identifică generatorul utilizat de interlocutorii *A* și *B*, $g = 67$. Pentru $d = 20$ problema algoritmului discret se formulează în felul următor: De găsit exponentul *a* astfel, încât $67^a = 20 \ mod\ 71$. Utilizând o metodă „brute-force” de încercări repetate ale valorilor lui *a*, ar putea determina că $a = 50$. Într-adevăr, se poate „ghici” că:

$67^{50} mod\ 71 = ((67^5)^5)^2 mod\ 71 = ((41)^5)^2 mod\ 71 = (34)^2 mod\ 71 = 20\ mod\ 71 = 20.$

Însă acest proces poate dura extrem de mult timp în cazul când numerele sunt foarte mari.

Exemplu 1. Fie *G* - grup ciclic abelian multiplicativ a numerelor întregi după modulo *p* = *11* și *g* = 7 – unul din generatorii grupului ciclic *G*.

Soluție.

Pasul 1. Interlocutorii *A* și *B* se înțeleg (cad de comun acord) asupra perechii de numere *(11, 7)*.

Pasul 2. Interlocutorul *A* alege aleator (generează) un număr secret *a=5* și transmite public interlocutorului *B*, $7^5 mod\ 11 = 10$.

Pasul 3. Interlocutorul *B* alege aleator (generează) un număr secret *b=3,* și transmite public interlocutorului *A*, $7^3 mod\ 11 = 2$.

Pasul 4. Interlocutorul *A* calculează $K_A = (7^3)^5\ mod\ 11 = (2)^5\ mod\ 11 = 32\ mod\ 11=10$.

Pasul 5. Interlocutorul *B* calculează $K_B = (7^5)^3\ mod\ 11 = (10)^3\ mod\ 11 = 1000\ mod\ 11=10$.

Interlocutorii *A* și *B* posedă unul și același element al grupului *G*, cheia secretă $CS = K_A = K_B=10$.

6. Algoritmul Diffie-Hellman-Merkel extins

Algoritmul Diffie-Hellman-Merkel poate fi extins pentru orice număr de interlocutori.

În continuare vom descrie algoritmul respectiv pentru interlocutorii *A*, *B* și *C*.

Problema 2. Fie *G* - grup abelian după *modulo p*, unde *p* - este un număr prim și *g* – unul din generatorii grupului *G*. Se cere să se elaboreze un algoritm de generare a unor chei publice care ar permite interlocutorilor *A*, *B* și *C* să genereze chei secrete și să facă schimb de chei.

Soluție.

Pasul 1. Interlocutorii *A*, *B* și *C* se înțeleg (cad de comun acord) asupra perechii de numere *(p, g)*.

Pasul 2.

2.1. Interlocutorul *A* alege aleator (generează) un număr secret $a, 0 \leq a \leq |G| - 1$ și publică $g^a\ mod\ p$.

2.2. Interlocutorul *B* alege aleator (generează) un număr secret $b, 0 \leq b \leq |G| - 1$ și publică $g^b\ mod\ p$.

2.3. Interlocutorul *C* alege aleator (generează) un număr secret $c, 0 \leq c \leq |G| - 1$ și publică $g^c\ mod\ p$.

Pasul 3.

3.1**.** Interlocutorul *A* utilizează $g^b\ mod\ p$ și $g^c\ mod\ p$, calculează $(g^b)^a\ mod\ p$ și $(g^c)^a\ mod\ p$ și publică rezultatele obținute.

3.2**.** Interlocutorul *B* utilizează $g^c\ mod\ p$, calculează $(g^c)^b\ mod\ p$ și publică rezultatul obținut.

Pasul 4.

4.1**.** Interlocutorul *A* utilizează $g^{cb}\ mod\ p$ și calculează $K_A = (g^{cb})^a\ mod\ p$.

4.2**.** Interlocutorul *B* utilizează $g^{ca}\ mod\ p$ și calculează $K_B = (g^{ca})^b\ mod\ p$.

4.3**.** Interlocutorul C utilizează g^{ba} *mod p* și calculează $K_C = (g^{ba})^c$ *mod p*.

Deoarece *G* este grup comutativ *ab = ba*, interlocutorii *A*, *B* și *C* posedă unul și același element al grupului *G*, cheia secretă $CS = K_A = K_B = K_C = g^{abc}$ *mod p*.

Exemplu 2. Fie *G* - grup abelian după modulo *p = 11,* un număr prim și *g = 6* – unul din generatorii grupului *G*. Se cere să se elaboreze un algoritm de generare a unor chei publice care ar permite interlocutorilor *A*, *B* și *C* să genereze chei secrete și să facă schimb de chei.

Soluție. Pe parcursul soluționării problemei respective vom utiliza relația:

$$(a^b)^c \bmod p = (a^b \bmod p)^c \bmod p.$$

Pasul 1. Interlocutorii *A*, *B* și *C* se înțeleg (cad de comun acord) asupra perechii de numere *(p=11, g=6)*.

Pasul 2.

2.1. Interlocutorul *A* alege aleator un număr secret *a = 4* și publică $g^a \bmod p = 6^4 \bmod 11 = (6^2)^2 \bmod 11 = 3^2 \bmod 11 = 9$.

2.2. Interlocutorul *B* alege aleator un număr secret *b =7* și publică $g^b \bmod p = 6^7 \bmod 11 = 8$.

2.3. Interlocutorul *C* alege aleator (generează) un număr secret *c=8* și publică $g^c \bmod p = 6^8 \bmod 11 = (6^4)^2 \bmod 11 = 9^2 \bmod 11 = 4$.

Pasul 3.

3.1**.** Interlocutorul *A* utilizează $g^b \bmod p$ și $g^c \bmod p$, calculează și publică rezultatele:
$(g^b)^a \bmod p = (6^7)^4 \bmod 11 = (8)^4 \bmod 11 = (8 \bmod 11)^4 \bmod 11 = 3^4 \bmod 11 = 4$ și $(g^c)^a \bmod p = (6^8)^4 \bmod 11 = 4^4 \bmod 11 = (4^2)^2 \bmod 11 = 3$.

3.2**.** Interlocutorul *B* utilizează $g^c \bmod p$, calculează $(g^c)^b \bmod p$ și publică rezultatul obținut. $(g^c)^b \bmod p = (6^8)^7 \bmod 11 = (6^8 \bmod 11)^7 \bmod 11 = 4^7 \bmod 11 = 5$.

Pasul 4.

4.1**.** Interlocutorul *A* utilizează $g^{cb} \bmod p$ și calculează $K_A = (g^{cb})^a \bmod p = (6^{8 \cdot 7})^4 \bmod p = 5^4 \bmod 11 = (5^2)^2 \bmod 11 = (3)^2 \bmod 11 = 9$.

4.2. Interlocutorul *B* utilizează $g^{ca} \bmod p$ și calculează $K_B = (g^{ca})^7 \bmod p = 3^7 \bmod 11 = 9$.

4.3. Interlocutorul *C* utilizează $g^{ba} \bmod p$ și calculează $K_C = (g^{ba})^c \bmod p = 4^8 \bmod 11 = (4^4)^2 \bmod 11 = 3^2 \bmod 11 = 9$.

Deoarece *G* este grup comutativ *ab = ba*, interlocutorii *A*, *B* și *C* posedă unul și același element al grupului *G*, cheia secretă $CS = K_A = K_B = K_C = g^{abc} \bmod p = 6^{4 \cdot 6 \cdot 8} \bmod 11 = 9$.

7. Algoritmul Stickel pentru generarea cheielor

Problema 3. Fie *G* – grup finit necomuativ și $|G| = k$. Se cere să se elaboreze un algoritm privind generarea unor chei publice care ar permite interlocutorilor *A* și *B* să genereze chei secrete și să facă schimb de chei.

Prezentarea Algoritmului Stikel [7]

Fie G – grup neabelian finit, public. Admitem că $a, b \in G$ și $ab \neq ba$, la fel sunt publice. Fie N și M sunt ordinele elementelor a și respectiv b.

Pasul 1. Interlocutorul A alege aleator (generează) două numere naturale secrete n, m astfel, încât $n < N$ și $m < M$ și transmite public interlocutorului B, $r(A) = a^n b^m$.

Pasul 2. Interlocutorul B alege aleator (generează) două numere naturale secrete r, s astfel, încât $r < N$ și $s < M$ și transmite public interlocutorului A, $r(B) = a^r b^s$.

Pasul 3. Interlocutorul A calculează $K_A = a^n\, r(B)\, b^m = a^{n+r}\, b^{m+s}$.

Pasul 4. Interlocutorul B calculează $K_B = a^r\, r(A)\, b^s = a^{n+r}\, b^{m+s}$.

Interlocutorii A și B posedă unul și același element al grupului G, cheia secretă $CS = K_A = K_B$.

Exemplu 3. Fie *D8* - grup diedral de ordinul 8. Grupul *D8* este generat de *a=3* și *b=2*. Astfel:

1) $a^2 = a \circ a = 3 \circ 3 = 4$; $b^2 = b \circ b = 2 \circ 2 = 1 = e$, unde $e = 1$ este elementul unitate;
2) $a^3 = a^2 \circ a = 4 \circ 3 = 5$; $a^3 = a \circ a^2 = 3 \circ 4 = 5$;
3) $ab = a \circ b = 3 \circ 2 = 6$; $ba = b \circ a = 2 \circ 3 = 8 = a^3 \circ b = a^3 b = 5 \circ 2$;
4) $a^2b = 4 \circ 2 = 7$; $ba^2 = 2 \circ 4 = 7$;

Compoziția celorlalte elemente din *D8* este dată de tabelul Cayley de mai jos.

▫	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	2	3	4	5	6	7	8
2	2	1	8	7	6	5	4	3
3	3	6	4	5	1	7	8	2
4	4	7	5	1	3	8	2	6
5	5	8	1	3	4	2	6	7
6	6	3	2	8	7	1	5	4
7	7	4	6	2	8	3	1	5
8	8	5	7	6	2	4	3	1

Grupul *D8* nu este comutativ. De exemplu $8 \circ 7 \neq 7 \circ 8$. Avem subgrupurile abeliene:

$$(\{2, 1\},\circ)\ ,\ (\{4, 1\},\circ),\ (\{6, 1\},\circ),\ (\{7, 1\},\circ),\ (\{8, 1\},\circ),\ (\{1, 3, 4, 5\},\circ),$$
$$(\{1, 2, 4, 7\},\circ),\ (\{1, 4, 6, 8\},\circ).$$

Grupul *D8* posedă centru netrivial. În algebra abstractă, centrul unui grup G este mulțimea de elemente care comută cu fiecare element al lui G. Se notează $Z(G)$. Astfel,

$$Z(G) = \{z \in G \mid \forall g \in G,\ zg = gz\}.$$

După cum putem observa elementul $a^2 = 4$ comută cu elementele b și a. Într-adevăr:

- Pentru elementul b, avem, $a^2 \circ b = b \circ a^2 = a^2 b$. Deci, $4 \circ 2 = 2 \circ 4 = 7$.
- Iar elementul a^2 comută, evident, cu elementul a. Deci, $a^2 \circ a = a \circ a^2 = 4 \circ 3 = 3 \circ 4 = 5$.

Deci, dacă elementul *4* comută cu generatorii, comută și cu toate elementele din G. În acest caz, $4 \circ z = z \circ 4$, pentru orice $z \in D8$. Și astfel, centrul $Z(D8)$ este exact $\{a^2, e\} = \{4, 1\}$

– centru non-trivial într-un grup non-abelian. Menționăm faptul că ordinul elementului $b = 2$ este doi, $ord\ (2) = 2$, deoarece $b^2 = b▫b=1$, iar ordinul elementului $a = 3$ este patru, deoarece:

$a=3$;
$a^2=a▫a=3▫3=4$;
$a^3=a^2 ▫a=4▫3=a▫a^2 =3▫4=5$;
$a^4 =a^2 ▫a^2 =4▫4=a^3▫a=5▫3=a▫a^3 =3▫5=1$.

La fel, ordinul elementului $a^3=5$ este patru, $ord(5)=4$. Celelalte elemente din grupul examinat au ordinul *2*. În scopul exemplificării **algoritmului Stickel** examinăm următorul exemplu.

Exemplu 4. Fie *D8* – grup finit necomutativ, din exemplul 3, care este public și elementele $a=5$, $b=2$ și $ab\neq ba$ din *G.* Se cere să se aplice Algoritmul Stickel privind generarea unor chei publice care ar permite interlocutorilor *A* și *B* să genereze chei secrete și să facă schimb de chei.

Soluție.

Pasul 1. Interlocutorii *A* și *B* cad de comun acord asupra grupului finit necomutativ $G = D8$ și a numerelor $a=5$ și $b=2$ și evident, $ab=8\neq6=ba$. Totodată, avem că $ord\ (5)=N=4$ iar $ord(2)=M=2$.

Pasul 2. Interlocutorul *A* alege aleator două numere naturale secrete $n=3<N$, $m=1<M$ și transmite public interlocutorului *B*, $r(A)=a^n\ b^m=5^3▫\ 2^1=3▫2=6$.

Pasul 3. Interlocutorul *B* alege aleator două numere naturale secrete $r=2<N$, $s=1<M$ și transmite public interlocutorului *A*, $r(B)=a^r\ b^s=5^2▫\ 2^1=4▫2=7$.

Pasul 4. Interlocutorul *A* calculează:

$$K_A=a^n\ r(B)\ b^m=5^3 ▫7▫2^1 =(3▫7)▫2=8▫2=5=a^{n+r}\ b^{m+s}=5^5 ▫2^2 =5▫1.$$

Pasul 5. Interlocutorul *B* calculează:

$$K_B=a^r r(A)\ b^s=5^2 ▫6▫2^1 =(4▫6)▫2 =8▫2=5= a^{n+r}\ b^{m+s}=5^5 ▫2^2 =5▫1.$$

Interlocutorii *A* și *B* posedă unul și același element al grupului *G*, cheia secretă $CS=K_A =K_B =5$.

8. Algoritmul Stickel - Shpilrain pentru generarea cheilor

O versiune mai generală a Algoritmului Stickel este Algoritmul Stickel – Shpilrain [7, 8].

Problema 4. Fie *G* – grup finit necomutativ care este public. La fel sunt cunoscute și elementele arbitrare $a,b\in G$ și $ab\neq ba$, cât și elementul $w\in G$. Se cere să se elaboreze un algoritm privind generarea unor chei publice care ar permite interlocutorilor *A* și *B* să genereze chei secrete și să facă schimb de chei.

Prezentăm mai jos ***algoritmul Stickel - Shpilrain*** pentru generarea cheilor.

Pasul 1. Interlocutorul *A* alege aleator două numere naturale secrete *n, m* astfel, încât

$n < N$ și $m < M$, selectează un element $c_1 \in Z(G)$ și transmite public interlocutorului *B*,

$$r(A) = c_1 a^n w b^m .$$

Pasul 2. Interlocutorul *B* alege aleator două numere naturale secrete *r*, *s* astfel, încât $r<N$ și $s<M$, selectează un element $c_2 \in Z(G)$ și transmite public interlocutorului *A*,

$$r(B) = c_2 a^r w b^s.$$

Pasul 3. Interlocutorul *A* calculează $K_A = c_1 a^n r(B) b^m = c_1 c_2 a^{n+r} w b^{m+s}$.

Pasul 4. Interlocutorul *B* calculează $K_B = c_2 a^r r(A) b^s = c_1 c_2 a^{n+r} w b^{m+s}$.

În așa mod, interlocutorii *A* și *B* posedă unul și același element al grupului *G*, cheia secretă $CS = K_A = K_B$.

Exemplu 5. Fie $G = D8$ grup neabelian finit și public și elementele $a=3$, $b=2$ din *G* și $ab \neq ba$ și $w=7$ din *G*. Aplicând Algoritmul Stickel - Shpilrain se cere să se elaboreze un algoritm privind generarea unor chei publice care ar permite interlocutorilor *A* și *B* să genereze chei secrete și să facă schimb de chei.

Soluție.

Avem că $ord(3)=N=4$, $ord(2)=M=2$ și $w=7$.

Pasul 1. Interlocutorul *A* alege aleator două numere naturale secrete *n, m* astfel, încât $n=3<N$ și $m=1<M$, selectează un element $c_1=4 \in Z(G)=\{4,1\}$ și transmite public interlocutorului *B*,

$$r(A) = c_1 a^n w b^m = 4 \cdot 3^3 \cdot 7 \cdot 2^1 = 4 \cdot 5 \cdot 7 \cdot 2 = 3 \cdot 7 \cdot 2 = 8 \cdot 2 = 5.$$

Pasul 2. Interlocutorul *B* alege aleator două numere naturale secrete *r*, *s* astfel, încât $r=2<N$ și $s=1<M$, selectează un element $c_2 =4 \in Z(G)$ și transmite public interlocutorului *A*,

$$r(B)=c_2 a^r w b^s=4 \cdot 3^2 \cdot 7 \cdot 2^1=4 \cdot 4 \cdot 7 \cdot 2=1 \cdot 7 \cdot 2=7 \cdot 2=4.$$

Pasul 3. Interlocutorul *A* calculează:

$K_A = c_1 a^n r(B) b^m=4 \cdot 3^3 \cdot 4 \cdot 2^1 =3 \cdot 4 \cdot 2=8$ ori $c_1 c_2 a^{n+r} w b^{m+s}=4 \cdot 4 \cdot 3^5 \cdot 7 \cdot 2^2 =8$.

Pasul 4. Interlocutorul *B* calculează $K_B = c_2 a^t r(A) b^s = c_1 c_2 a^{n+r} w b^{m+s}$.

$K_B = c_2 a^r r(A) b^s =4 \cdot 3^2 \cdot 5 \cdot 2^1 =1 \cdot 5 \cdot 2=8$ ori $c_1 c_2 a^{n+r} w b^{m+s}=4 \cdot 4 \cdot 3^5 \cdot 7 \cdot 2^2 =8$.

În așa mod, interlocutorii *A* și *B* posedă unul și același element al grupului *G*, cheia secretă $CS=K_A =K_B =8$.

9. Atacul de tip „man-in-the-middle” - amenințarea la securitatea protocolului Diffie-Hellman-Merkle

În descrierea inițială, schimbul Diffie-Hellman-Merkle nu oferea autentificarea părților care comunică și poate fi vulnerabil la un atac de tip „man-in-the-middle” (om în poziția de mijloc). Astfel, un atacator activ (răufăcătorul *R*) care lansează atacul „man-in-the-middle”, poate realiza două schimburi de chei distincte, unul cu interlocutorul *A* și celălalt cu interlocutorul *B*, ”mascându-se”, în calitate de interlocutor *A* pentru *B* și „prefăcându-se” ca interlocutor *B* pentru *A*. Acest rol îi permite răufăcătorului *R* să

intercepteze, să decripteze, apoi să reia procesul de criptare, în raport cu mesajele trimise reciproc de *A* și *B*.

Este necesar de menționat că răufăcătorul *R*, în acest atac, trebuie să se plaseze în calitate de intermediar „ascuns” (la mijloc) din startul procesului și să continue să se implice activ în schimbul de mesaje dintre interlocutorii *A* și *B*, decriptând și re-criptând mesajele interceptate.

Atacul „man-in-the-middle” nu poate reuși în situația când atacatorul *R* începe a interveni:

(1) după ce cheile deja au fost generate și

(2) conversația criptată dintre interlocutorii A și B a început deja.

Să explicăm mai profund acest proces. Reamintim că procedura schimbului de chei se produce în două etape centrale:

1. **Configurare unică**. Se definesc parametrii publici care sunt utilizați de toți cei implicați.

2. **Protocol**. Pentru a genera noi chei secrete, se rulează un protocol de schimb de chei cu două mesaje. Acest proces se realizează folosind numere prime și proprietăți ale aritmeticii modulare.

Care este amenințarea la securitate protocolului Diffie-Hellman-Merkle?

Să presupunem că atacatorul *R* cunoaște elementele *p* și *g* făcute public, ca și interlocutorii *A* și *B*. Totodată, din anumite surse, atacatorul *R* află și despre valorile schimbate de interlocutorii *A* și *B*: $g^a \bmod p$ și $g^b \bmod p$.

Cu toate cunoștințele și informația pe care le posedă atacatorul *R*, nu poate imediat calcula cheia secretă *KS*, chiar dacă *p* și *g* sunt alese corect.

De exemplu, atacatorul *R* poate aplica direct metoda „brute force”, prin intermediul căruia se încearcă toate opțiunile posibile. Dar, după cum se știe, calculul logaritmului discret, atunci când trebuie de aflat $g^a \bmod p$ și $g^b \bmod p$ este foarte lent, în mod special când numerele implicate sunt foarte mari.

Dacă *p* și *g* au mii de biți, atunci cei mai cunoscuți algoritmi pentru calculul logaritmului discret vor necesita foarte mult timp pentru determinarea valorilor căutate.

Chiar dacă algoritmul Diffie-Hellman-Merkle este „rezistent” la intervenția „brute force”, protocolul respectiv este mai vulnerabil la atacul de tip „man-in-the-middle”. De ce? Să examinăm mai atent acest tip de atac.

Atacatorul *R* care se află în poziția „man-in-the-middle”, poate manipula comunicațiile dintre interlocutorii *A* și *B* și poate ”sparge” securitatea schimbului de chei. Astfel:

Pasul 1. Convenția asupra numerelor

Fie că sunt făcute publice numerele selectate *p* și *g*, unde *p* este un număr prim, numit „*modulo*”, iar *g* este numit generator.

Pasul 2. Selectarea numerelor private

Fie interlocutorul *A* alege un număr aleatoriu privat *a* și interlocutorul *B* alege un număr aleatoriu privat *b*. Admitem că atacatorul *R* alege 2 numere aleatoare *c* și *d*.

Pasul 3. Interceptarea mesajelor publice

Fie atacatorul *R* interceptează valoarea publică a lui *A,* $g^a \ mod \ p$, și nu-i mai transmite lui *B* mesajul respectiv. În schimb, atacatorul *R*, îi trimite interlocutorului B propria valoare publică $g^c \ mod \ p$. Similar, printr-o modalitate oarecare atacatorul *R* interceptează valoarea publică a lui *B*, $g^b \ mod \ p$. Atacatorul *R* blochează (reține) mesajul și nu permite ca să ajungă la interlocutorul *A*. În schimb, îi trimite interlocutorului *A,* propria valoare publică, mesajul $g^d \ (mod \ p)$.

Pasul 4. Calcularea cheii secrete

În așa mod interlocutorul *A* va calcula cheia $KS1=g^{da} \ (mod \ p)$, iar *B* va calcula o cheie diferită $KS2=g^{cb} \ (mod \ p)$.

Pasul 5. Comunicare deturnată

Dacă interlocutorul *A* folosește *KS1* în calitate de cheie secretă pentru a cripta un mesaj adresat lui *B*, atacatorul *R* îl poate decripta, și poate sa-l re-cripteze folosind *KS2,* pentru ca ulterior să-l transmită lui *B*. Interlocutorii *B* și *A* nu vor observa imediat nicio problemă și consideră că comunicarea lor este securizată. Dar, în realitate, răufăcătorul *R* poate decripta, citi, modifica și apoi re-cripta toată comunicarea lor.

În contextul celor examinate mai sus, pentru că algoritmul Diffie-Hellman-Merkle privind schimbul de chei să fie un algoritm securizat, informațiile schimbate ar trebui să fie protejate, de exemplu, cu o funcție *Hash*. Din această perspectivă algoritmii Diffie-Hellman pot fi încorporați într-un protocol care asigură autentificarea. Pentru a preveni un atac de tip „man-in-the-middle” se poate utiliza una din metodele de autentificare a părților care comunică între ele.

Algoritmul clasic Diffie-Hellman nu presupune autentificarea părților. Din variantele mai sigure ale protocolului Diffie-Hellman, este protocolul Station-to-Station (*STS*), care poate fi utilizat în scopul evitării atacurilor de tipul „man-in-the-middle”. Protocolul *STS* reprezintă o schemă de acord privind schimbul de chei criptografice. Algoritmul *STS* se bazează pe protocolul clasic Diffie–Hellman și oferă în plus autentificare reciprocă a cheilor obținute și entităților implicate.

Spre deosebire de algoritmul clasic Diffie-Hellman, care nu este sigur împotriva unui atac de tip „man-in-the-middle”, acest protocol presupune că părțile au chei de semnătură, care sunt folosite pentru a semna mesajele, oferind astfel securitate împotriva atacurilor „man-in-the-middle”.

În plus, față de protejarea cheii stabilite împotriva unui atacator, protocolul *STS* nu folosește marcaje temporale și oferă securizare perfectă pentru transmitere. De asemenea, implică confirmarea explicită a cheii în două sensuri, asigurând ca schimbul de chei să fie

autentificat cu protocolul de confirmare.

Menționăm faptul că protocolul *STS* a fost lansat în premieră în 1987 în contextul securizării de atacurile de tipul „man-in-the-middle” și finalizat complet în 1989. Protocolul respectiv a fost prezentat de Whitfield Diffie, Paul C. van Oorschot și Michael J. Wiener în anul 1992.

Articol realizat în cadrul proiectului de cercetări științifice „Metodologia implementării TIC în procesul de studiere a științelor reale din perspectiva conceptului STEAM și Inteligenței Artificiale”, codul 040101, din cadrul Programului instituțional de cercetare (2024-2027), aprobat prin Ordin MEC nr. 102 din 01.02.2024

Bibliografie

1. DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. În: IEEE *Transactions on Information Theory*, 1976.
2. MERKLE, R. C. A digital signature based on a conventional encryption function. In: *Advances in Cryptology* - CRYPTO 87, pp. 369-378, LNCS 293, Springer-Verlag, 1987.
3. MERKLE, R. C. *Secrecy, authentication, and public key systems* (Computer science). UMI Research Press, 1982. ISBN 0-8357-1384-9.
4. RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. In: *Communications of the ACM*, 1978.
5. YAN, S Y. *Primality Testing and Integer Factorization in Public- Key Cryptography*. Springer, 2003. 256 p. ISBN 1402076495.
6. ELGAMAL, T. *A public key cryptosystem and a signature scheme based on discrete logarithms*. IEEE Transactions on Information Theory, 1985.
7. STICKEL, E. A new Method for Exchanging Secret Keys. In: *Proc. Of the Third International Conference on Information Technology and Applications* (ICITA05) 2, 2005, pp. 426-430.
8. SHPIRILAN, V. *Cryptoanalysis of Stickel’s Key Exchange Scheme*. Conference Paper June, 2008.
9. CHIRIAC, L.; DANILOV, A. Abordări metodice în studierea sistemului criptografic asimetric Merkle–Hellman. În: *Acta Et Commentationes. Sciences of Education*, 2021. nr. 3(25), 2021, pp. 7-23. https://doi.org/10.36120/2587-3636.v25i3.7-23.
10. CHIRIAC, L.; DANILOV, A.; BOGDANOVA, V. Encryption and decryption algorithm based on the Latin groupoid isotopes. In: *Acta et Commentationes, Exact and Natural Sciences*, 2022, Volume 2(14), pp. 117–131, TSU/UPSC, E-ISSN: 2587-3644, CZU 512.548 (043.3), DOI: https://doi.org/10.36120/2587-3644.v14i2.117-131

11. CHIRIAC, L.; DANILOV, A. Aspecte didactice privind studierea algoritmului de criptare RSA, funcțiilor hash și semnăturii digitale. In: *The 29th Conference on Applied and Industrial Mathematics CAIM 2022*. 25-27 august 2022, Chișinău, Republica Moldova: Tiraspol State University, 2022, p. 125-134. ISBN 978-9975-76-401-8. https://ibn.idsi.md/sites/default/files/imag_file/125-134_6.pdf
12. CHIRIAC, L.; DANILOV, A. The methodology of the implementation of groupoid isotopes in the encryption / decryption of texts. În: *Materialele Conferinței științifice internaționale „Abordări inter/transdisciplinare în predarea științelor reale (concept STEAM)”*, ediția a II-a. 28 – 29 octombrie 2022. Chișinău: UST, 2022, p. 256-265. ISBN 978-9975-76-411-7 (PDF). https://drive.google.com/file/d/1xoqDPJ1Hs30JalfhGrWdYRxC1i8416ue/view
13. CHIRIAC, L.; DANILOV, A.; BOGDANOVA, V. Constructing one Symmetric Algorithm based on the Latin Groupoid Isotopes. In: *Conference on Applied and Industrial Mathematics CAIM 2023*. Ediția 30. 2023. Iași, România. p. 65-67. https://ibn.idsi.md/vizualizare_articol/200109
14. CHIRIAC, L.; DANILOV, A.; BOGDANOVA, V. Utilizarea conceptelor din teoria numerelor în elaborarea algoritmilor criptografici asimetrici. In: *Învățământ superior: tradiții, valori, perspective Științe Exacte și ale Naturii și Didactica Științelor Exacte și ale Naturii*. Vol. 1. 2020. Chișinău, Republica Moldova. pp. 239-247. ISBN 978-9975-76-360-8. https://ibn.idsi.md/ vizualizare_articol/114463
15. CHIRIAC, L.; DANILOV, A. Abordări metodice privind aplicarea quasigrupurilor la dezvoltarea unor metode de criptografie. In: *Acta et commentationes (Ştiinţe ale Educaţiei)*. 2020, nr. 4(22), pp. 7-17. ISSN 1857-0623. DOI: https://doi.org/10.36120/2587-3636.v22i4.7-17