CZU: 378.147:004+51

UTILIZAREA CONCEPTELOR DIN TEORIA NUMERELOR IN ELABORAREA ALGORITMILOR CRIPTOGRAFICI ASIMETRICI

Liubomir CHIRIAC, doctor habilitat, profesor universitar
Aurel DANILOV, doctorand
Violeta BOGDANOVA, doctorand
Universitatea de Stat din Tiraspol

Abstract. În lucrare autorii abordează problema pregătirii specialiștilor informaticieni, specializați în criptografie, în domeniul algebrei abstracte și teoriei numerelor. Sunt scoase în evidență, interconexiunile existente intre conceptele matematice din teoria numerelor și algoritmii criptografici de ultimă oră. Este demonstrat din punct de vedere metodologic, necesitatea studierii conceptelor matematice, de către informaticieni, pentru înțelegerea funcționării, utilizării și aplicării sistemului criptografic asimetric El Gamal.
Cuvinte cheie: informatică, algoritm, criptare, decriptare, Algoritmul El Gamal, congruențe, rădăcină primitivă.

Abstract. In the paper, the authors address the issue of training computer specialists, specializing in cryptography, in the field of abstract algebra and number theory. The existing interconnections between the mathematical concepts of number theory and the latest cryptographic algorithms are highlighted. It is demonstrated from a methodological point of view, the need to study mathematical concepts, by computer scientists, to understand the operation, use and application of the asymmetric cryptographic system El Gamal.
Keywords: computer science, algorithm, encryption, decryption, El Gamal Algorithm, congruences, primitive root.

1. Algoritmii criptografici

În trecutul apropiat criptografia era utilizată de un număr restrâns de experți, care reprezentau instituțiile de importanță majoră pentru stat, precum: guvern, bănci, militărie, etc. În prezent însă tehnicile de criptare sunt omniprezente și sunt utilizate, în realizarea diverselor operațiuni cotidiene: securizarea plăților on line, asigurarea confidențialității discuțiilor prin intermediul telefoanelor mobile, securizarea operațiunilor efectuate prin intermediul cardurilor bancare, securizarea implementării votului electronic. Cei mai siguri algoritmi criptografici au la bază o serie de concepte matematice. Astfel, pentru a înțelege funcționarea acestor algoritmi este necesară înțelegerea conceptelor matematice respective. Așa cum în viitorul apropiat centrul de greutate a cercetările în domeniul informaticii se va transfera pe segmentul algoritmilor criptografici, este necesar de menționat faptul că pregătirea specialiștilor informaticieni de clasă înaltă presupune, în opinia noastră, pregătirea fundamentală în domeniul algebrei abstracte și teoriei numerelor. Aplicații practice, în acest sens, adică elaborarea și implementarea programelor bazate pe concepte matematice moderne va trezi un interes sporit din partea studenților și masteranzilor în raport cu acest domeniu de mare perspectivă. În această lucrare, autorii vor demonstra și

ilustra din punct de vedere metodologic, necesitatea cunoașterii conceptelor matematice pentru înțelegerea funcționării și utilizării unui apreciat sistem criptografic, cunoscut în literatura de specialitate ca sistemul criptografic El Gamal.

Sistemul criptografic El Gamal este cu cheie publică şi se bazează pe ”dificultatea” calculării valorilor logaritmilor discreți pe așa structuri algebrice precum corpuri finite. Acesta include: algoritmul de criptare El Gamal şi algoritmul semnăturii digitale. Sistemul criptografic El Gamal a fost elaborat în anul 1985 de către T. El Gamal [1], care a dezvoltat o variantă a algoritmului Diffie-Hellman [2]. De la publicarea în anul 1976, protocolul propus de Whitfield Diffie¸ și Martin Hellman a devenit unul din cele mai cunoscute și utilizate sisteme criptografice. În versiunea sa de bază, sistemul criptografic Diffie-Hellman permite identificarea unei soluții eficiente pentru rezolvarea problemelor de partajare a cheilor de sesiune între doi participanți. Spre deosebire de algoritmul RSA, algoritmul El Gamal nu a fost patentat și de aceea a devenit o alternativă eficientă și ieftină pentru utilizare, fără ca să fie plătite cotizații pentru licența care ar permite folosirea algoritmului [4-7].

2. Noțiuni și concepte matematice

Pentru a înțelege cum funcționează cripto-sistemului ElGamal vom evidenția noțiunile și teoremele de bază din teoria numerelor necesare pentru explicație și pentru înțelegerea Algoritmului ElGamal.

În primul rând vom porni de la conceptul de număr. Numărul este un concept fundamental în matematică. Evoluția conceptului respectiv coincide cu evoluția întregii matematici. Astfel:

- Evoluția de la număr natural la număr rațional, real, complex. Apoi evoluția de la descoperirea cuaternionilor lui Hamilton, numerele Cayley, la numere p-adice, numerele reale nonstandard, numere algebrice, numere construite ca elemente ale corpurilor finite.
- Demonstrarea unor numeroase teoreme de structură, care arată proprietățile și conexiunile intre numerele respective: teoremele lui Euclid, Ferma, Wilson, Frobenius, Hopf şi Gelfand-Mazur etc. [3].

2.1. Numere întregi și proprietăți

În expunerea algoritmilor criptografici ne va interesa în mod special numerele întregi, congruențe și proprietățile fundamentale care țin de teoria numerelor. Relaţia de bază între numerele întregi care ne interesează este relaţia de divizibilitate. Să ne reamintim că proprietăţile adunării (asociativitatea şi comutativitatea, existenţa elementului nul 0, existenţa elementului opus $-n$ pentru fiecare număr întreg n), proprietăţile înmulţirii (asociativitatea şi comutativitatea, existenţa elementului neutru 1), împreună cu distributivitatea înmulţirii faţă de adunare, fac din mulţimea numerelor întregi un inel (comutativ) – notat cu Z. În acest inel doar numerele 1 şi -1 au invers.

Definiţia 1. *Fie n, m ∈ Z. Spunem că n îl divide pe m sau m este divizibil cu n, dacă există un unic p ∈ Z astfel încât np = m. Vom nota acest fapt n|m sau n:m.*

Se observă că dacă acceptăm această definiţie, atunci 0 este divizibil cu orice număr nenul, dar nu divide nici un număr. Relaţia de divizibilitate între numere întregi are o serie de proprietăţi, care se demonstrează foarte simplu dacă ţinem cont de teorema împărţirii întregi.

Teorema 2. *(Teorema împărţirii întregi). Fie a, b ∈ Z, b > 0 (să-l numim pe a deîmpărţit, iar pe b, împărţitor). Atunci există două numere întregi q, r ∈ Z, (numite cât, q respectiv rest, r) astfel ca 1) a = b · q + r, 2) 0 ≤ r < b, şi aceste două numere sunt şi unice cu aceste proprietăţi.*

Clar lucru, dacă restul r este nul, atunci b|a, şi invers, dacă b|a, atunci restul este nul. Să enumerăm acum proprietăţile relaţiei de divizibilitate între numere întregi.

Relaţia de divizibilitate între numere întregi are următoarele proprietăţi:

1. a|a pentru orice număr nenul a ∈ Z (reflexivitate)
2. dacă a|b şi b|a, atunci a = b sau a = −b (antisimetrie, pentru numere pozitive)
3. dacă a|b şi b|c, atunci a|c (tranzitivitate)
4. dacă 1|a şi −1|a atunci pentru orice număr a ∈ Z
5. dacă a|b şi a|c, atunci a|b ± c
6. dacă a|b, atunci a|bc pentru orice număr c ∈ Z
7. dacă a|b, atunci ac|bc pentru orice număr c ∈ Z.

Definiţia 3. *Un număr n ∈ N este "prim" dacă are doi şi numai doi divizori distincţi. Un număr care are mai mult de doi divizori se numeşte "compus".*

Observaţia 4.

- *Divizorii unui număr prim n sunt 1 şi n.*
- *Numărul 1 nu este prim (are un singur divizor!).*
- *Numărul 2 este singurul număr prim par.*

Lema 5. *Dacă n este prim şi n|ab, atunci n|a sau n|b.*

Definiţia 6. *Fie a şi b două numere întregi. Dacă cel mai mare divizor comun al lor este 1, atunci numerele se numesc relativ prime.*

Propoziţia 7. *Două numere întregi a şi b sunt relativ prime dacă şi numai dacă există numerele întregi x, y astfel ca ax + by = 1.*

Problema factorizării constă în determinarea tuturor divizorilor primi ai unui număr n ∈ N.

Teorema 8. *(Teorema fundamentală a aritmeticii). Fie n ∈ N, n > 1. Atunci n admite o descompunere unică în produs de factori primi (ridicaţi la diverse puteri).*

Teorema 9. *(Euclid) Mulţimea numerelor prime este infinită.*

2.2. Congruențe și inelul Z_n

Conceptul de "congruență" a fost introdus de Gauss şi constituie modalitatea principală de calcul în aritmetica pe calculator. Altfel spus, din cauza restricțiilor generate de construcția calculatorului aritmetica respectivă este finită. În așa mod, congruențele reprezintă modalitatea de a transforma mulțimea infinită a întregilor într-o mulțime finită de întregi cu păstrarea proprietăților celor două operații între întregi.

Congruenţele constituie un mod ingenios şi eficace de a transforma mulţimea infinită a întregilor într-o mulţime finită de întregi, cu păstrarea tuturor proprietăţilor celor două operaţii între întregi.

Definiţia 10. *Fie $n \geq 2$ un număr întreg. Relaţia între numerele întregi, definită prin $x \sim y$ dacă $n|x - y$, este o relaţie de echivalenţă compatibilă cu adunarea şi înmulţirea întregilor, numită relaţie de congruenţă modulo n.*

Clasele de echivalenţă se numesc clase de resturi modulo n, iar apartenenţa la aceeaşi clasă se mai notează $\boldsymbol{x \equiv y \bmod n}$.

Deoarece în general este preferabil să apară modulul n explicit în fiecare congruenţă notaţia mai simplă pe care o vom adopta noi nu va produce nici o confuzie:

$$\mathbf{x = y \bmod n}.$$

Compatibilitatea cu adunarea şi înmulţirea întregilor înseamnă (modulul n fixat):

a) $x1 \sim y1$ şi $x2 \sim y2$ implică $x1 + x2 \sim y1 + y2$

b) $x1 \sim y1$ şi $x2 \sim y2$ implică $x1 \cdot x2 \sim y1 \cdot y2$ (1.58)

Datorită acestei compatibilităţi, operaţia de adunare şi înmulţire între clase de echivalenţă prin intermediul a câte unui reprezentant arbitrar ales al clasei, funcţionează, este bine definită: altfel spus, nu depinde de alegerea reprezentanţilor claselor. Prin urmare congruenţele modulo n au următoarele proprietăţi:

Proprietăţi 11. *Fie n un număr întreg fixat $n \geq 2$. Atunci:*

1. *$x = x \bmod n$ pentru orice număr întreg x;*
2. *$x = y \bmod n$ dacă şi numai dacă $y = x \bmod n$, pentru orice numere întregi x, y;*
3. *dacă $x = y \bmod n$ şi $y = z \bmod n$ atunci $x = z \bmod n$, $\forall$ numere întregi x, y, z;*
4. *$x1 = y1 \bmod n$ şi $x2 = y2 \bmod n$ implică $x1 + x2 = y1 + y2 \bmod n$;*
5. *$x1 = y1 \bmod n$ şi $x2 = y2 \bmod n$ implică $x1 \cdot x2 = y1 \cdot y2 \bmod n$;*
6. *$x = 0 \bmod n$ înseamnă $x = kn$ pentru o valoare potrivită a lui k, sau pur şi simplu $n|x$.*

Fie n un număr întreg pozitiv, $n \geq 2$. Cel mai simplu mod de a privi congruențele mod n, este de a considera reprezentarea întregilor în baza n, apoi a renunța la toate cifrele reprezentării, exceptând ultima cifră. Se constată că operaţiile de adunare şi înmulţire existentă între numerele întregi, văzută doar pe ultima cifră a numerelor, îşi păstrează toate proprietăţile avute: adunarea este asociativă, există element nul, 0, fiecare număr k, ($0 \leq k \leq n-1$) are opus ($-0 = 0$ respectiv $-k = n - k$), şi aşa mai departe. Ba chiar proprietăţile se pot îmbunătăţi: dacă modulul n este ales număr prim, atunci devine posibilă şi împărţirea necondiţionată.

Exemplul 12. Deoarece 3|(10 − 1), vom avea 10 ≡ 1 (mod 3). Dacă 11|(16 − (−6)), atunci 16 ≡ −6 (mod 11). Avem că 7|(16 − 2), atunci 16 ≡ 2 (mod 7).

Exemplu 13. Să se găsească 3 numere întregi care sunt congruente cu 7 mod 11.

Soluție. Conform definiției congruenței este necesar să găsim 3 numere întregi a, b, c care sunt congruente cu 7 mod 11. Așa dar, trebuie să găsim 3 numere pentru care:
a ≡ 7 mod 11; b ≡ 7 mod 11; c ≡ 7 mod 11.

Conform definiției congruenței avem 11| (a-7). Astfel, putem nota: 11k = a – 7. De unde rezultă că a = 11k +7. Fie k = 0, 1, 2. Obținem că a = 7, b= 18, c = 29. Astfel, avem 7 mod 11 ≡ 18 mod 11 ≡ 29 mod 11.

Teorema 14. *Congruența este o relație de echivalență.*

Numărul *n* se numește modul, iar mulțimea $a = \{b \mid b \equiv a \pmod n\}$ se numește "clasa de echivalență a lui *a modulo n*".

Definiția 15. *Un sistem complet de resturi modulo n este o mulțime finită de întregi astfel încât orice a ∈ Z este congruent modulo n cu un singur întreg din mulțime.*

În particular, $Z_n = \{0, 1, 2, \ldots n-1\}$ este mulțimea celor mai mici resturi (nenegative) modulo n.

Exemplul 16. Există patru congruențe modulo 4:

1) {0}= {. . . , −4, 0, 4, 8 . . . },
2) {1} = {. . . , −3, 1, 5, . . . },
3) {2} = {. . . , −2, 2, 6, . . . },
4) {3} = {. . . , −1, 3, 7, . . . }.

Fiecare număr întreg (element din Z) se află în exact una din aceste mulțimi. Pentru două mulțimi A, B ⊆ Z pot fi definite operațiile A ± B = {x ± y | x ∈ A, y ∈ B}, AB = {x · y | x ∈ A, y ∈ B}.

Propoziție 17. *Z/nZ este inel unitar, numit "inelul claselor de resturi" modulo n***.**

Teorema 18. *(Teorema chineza a resturilor). Fie n ≥ 2 un numar natural și $x_1, x_2, \ldots, x_n$ numere întregi prime intre ele două câte doua si $a_1, a_2, \ldots, a_n$ numere intregi oarecare. Atunci exista o soluție pentru sistemul de congruente: $x \equiv a_1 \pmod{x_1}$, $x \equiv a_2 \pmod{x_2}$, . . ., $x \equiv a_n \pmod{x_n}$.*

Definiția 19. (*Funcția Euler***).** *Pentru orice n ∈ N, funcția Euler $\phi(n)$ este definită ca numărul valorilor m ∈ N cu m < n si (m; n) = 1 (numărul numerelor mai mici decât n și reciproc prime cu n).*

Dacă p este prim, atunci (p; k) = 1 pentru orice 1 ≤ k < p și în acest caz $\phi(p) = p - 1$.

Teorema 20. *(Teorema lui Euler). Fie n ≥ 2 un număr natural si a un număr întreg prim cu n. Atunci $a^{\phi(n)} \equiv 1 \pmod n$.*

Teorema 21. *(Teorema lui Fermat). Fie p un numar prim si a un număr întreg nedivizibil cu p. Atunci $a^{p-1} \equiv 1 \pmod p$.*

Proprietăţile evidențiate până la acest moment pot fi reformulate mai elegant folosind proprietăţi structurale. Astfel:

• Inelul întregilor Z este inel factorial: orice număr întreg se descompune unic în produs de numere prime (este valabilă teorema fundamentală a aritmeticii).
• Inelul întregilor Z este inel euclidian: orice număr întreg se poate împărţi cu orice întreg nenul, astfel ca este valabilă "proba" împărţirii, iar câtul şi restul sunt unici, dacă restul este între 0 şi modulul împărţitorului minus 1 (este valabilă teorema împărţiri întregi).
• Inelul întregilor este inel cu ideale principale: orice ideal este format din toţi multiplii unui număr.
• În inelul întregilor orice pereche de numere (nu ambele nule) are un cel mai mare divizor comun (şi un cel mai mic multiplu comun).
• Mulţimea claselor de resturi modulo n ($n \geq 2$) formează un inel. El este inelul factor al întregilor cu idealul generat de n. Acest inel se notează cu Z_n.
• În inelul claselor de resturi Z_n un element este inversabil dacă şi numai dacă (a, n) = 1, adică dacă este relativ prim cu modulul.
• Dacă modulul n = p este număr prim, atunci inelul factor Z_p este corp: toate elementele nenule sunt inversabile. Invers toate elementele nenule din Z_n sunt inversabile, doar dacă n este prim.
• Dacă n1, n2, . . . , nk sunt relativ prime două câte două, atunci inelele $Z_n \equiv Z_{n1} \oplus Z_{n2} \oplus . . . \oplus Z_{nk}$, sunt izomorfe, unde am notat $n = n1 \cdot n2 \cdot \cdot \cdot nk$. Aceasta este o reformulare a teoremei chinezeşti a resturilor.

2.3. Rădăcini primitive ale unui număr prim

Definiția 22. *Fie $n \geq 2$ un număr natural si a un număr prim cu n. Numim ordinul lui a modulo n cel mai mic numar k ce satisface congruenta $a^k \equiv 1 \pmod n$.*

Fie *$n \geq 2$* un numar natural fixat si a un numar intreg prim cu n. Definim mulțimea:

$$E = \{k \in N^* | \ a^k \equiv 1 \pmod n\}.$$

Conform teoremei lui Euler, $\phi(n) \in E$, deci $E \neq \emptyset$. In concluzie, E are un cel mai mic element – pe care îl vom numi ordinul lui *a* modulo *n*. Vom nota ordinul lui *a* modulo *n* cu $ord_n(a)$.

De exemplu, pentru a=2 și n= 7 avem că $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$, deci $ord_7(2) = 3$.

Pentru a caracteriza mulțimea E introdusa mai sus (si implicit toate solutiile congruentei $a^x \equiv 1 \pmod n$ cu a si n date), sunt demonstrate mai multe proprietăți care se utilizează în teoria criptografiei.

Definitia 23. *Fie $n \geq 2$ un numar natural si a un numar intreg prim cu n. Atunci a se numeste radacina primitiva modulo n daca $ord_n(a) = \phi(n)$.*

Fie n = 7. Pentru a = 3, vom avea: $3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 6 \pmod 7$, $3^4 \equiv 4 \pmod 7$, $3^5 \equiv 2 \pmod 7$, $3^6 \equiv 1 \pmod 7$, așa dar $ord_7(3) = 6$. Astfel, deoarece $ord_7(3) = 6 = \phi(7)$ putem afirma că 3 este o radacină primitivă modulo 7.

Teorema 24. *Orice număr prim admite o rădăcină primitivă.*

Fiind punctate noțiunile și proprietățile de bază putem prezenta algoritmul de criptare El Gamal.

3. Schema de criptare cu cheie publică El Gamal

Criptarea asimetrică. În cazul criptării asimetrice se utilizează o cheie publică și o cheie privată. Cheile respective pot fi folosite în calitate de:

- Mijloace independente de protecție a informațiilor;
- Instrumente de distribuție;
- Mijloace de autentificare a utilizatorilor.

Criptarea asimetrică are următoarele avantaje:

- Cheia secretă se păstrează doar într-un singur loc;
- Cheia de decriptare este cunoscută doar de un singur interlocutor.

În această situație, cheia publică este trimisă pe un canal deschis și ar putea fi teoretic interceptată de intruși.

Cheia publică este utilizată pentru criptare, iar cheia privată este utilizată pentru a decripta mesajul. Astfel:

1) Primul interlocutor alege algoritmul de criptare și decriptare, cheia publică și cheia privată;
2) Cheia publică este trimisă celei de a doua persoane pe canale deschise;
3) Cel de-al doilea interlocutor criptează informațiile utilizând cheia publică;
4) Trimite informația criptată primului apelant;
5) Primul apelant decriptează mesajul utilizând cheia privată, pe care numai el o cunoaște.

Schema de criptare ElGamal constă din 3 părți:

1. *Algoritmul de generare a cheilor*
   - 1.1. Se generează numărul prim aleator p;
   - 1.2. Se alege numărul întreg g – rădăcina primitivă a lui p;
   - 1.3. Se alege numărul aleator x, astfel încât $1< x < p-1$;
   - 1.4. Se calculează $y = g^X \bmod p$;
   - 1.5. Cheia publică deschisă este y, iar cheia secretă este x.
2. *Algoritmul de criptare*

Mesajul M trebuie să fie mai mic ca numărul prim p. Criptarea se face în felul următor:

- 2.1. Se alege un număr întreg k astfel, încât $1< k < p-1$;
- 2.2. Se calculează $a = g^k \bmod p$ și $b = y^k M \bmod p$.
- 2.3. Perechea de numere (a, b) este textul criptat corespunzător mesajului M.

Este ușor de observat că ”lungimea” textului criptat este de două ori mai mare comparativ cu mesajul inițial M.

3. *Algoritmul de decriptare*

3.1. Cunoscând cheia secretă x, mesajul inițial poate fi calculat din textul criptat (a, b) după relația: $M = b(a^x)^{-1} \bmod p$.

Este ușor de observat că $(a^x)^{-1} = g^{-kx} \bmod p$ și astfel $b(a^x)^{-1} = (y^k M) g^{-xk} \equiv$ $\equiv (g^{xk} M) g^{-xk} \equiv M \pmod p$. În practică pentru a calcula M deseori se utilizează formula: $M = b(a^x)^{-1} = ba^{(p-1-x)} \bmod p$.

Exemplu 1. Interlocutorii A și B sunt într-o discuție secretă. Interlocutorul B solicită o anumită informația secretă M de la interlocutorul A. În acest scop:

1. *Interlocutorul B generează cheia publică și cheia secretă*

1.1. Fie p=7 un număr prim și g = 2 o rădăcină primitivă a numărului p. Alegem un număr aleator x astfel încât $1 < x < p-1$. Fie x = 5.

1.2. Se calculează $y = g^x \bmod p = 2^5 \bmod 7 = 32 \bmod 7 = 4$

1.3. Astfel, tripletul (p, g, y) = (7, 2, 4) este cheia deschisă și cheia secretă x = 5.

1.4. Interlocutorul B transmite interlocutorului A pe canale publice cheia deschisă (7, 2, 4) iar cheia secretă o păstrează doar pentru el.

2. *Criptarea mesajului*

2.1. Interlocutorul A dorește să cripteze mesajul M care conform algoritmului trebuie să fie mai mic ca numărul prim p = 7. Fie M = 3.

2.2. Interlocutorul A alege numărul întreg k pentru care $1 < k < p-1$. Fie k = 4.

2.3. Se calculează $a = g^k \bmod p = 2^4 \bmod 7 = 2$.

2.4. Se calculează $b = y^k M \bmod p = 4^4\ 3 \bmod 7 = 768 \bmod 7 = 5$

2.5. Perechea (a,b) = (2 , 5) este textul criptat.

3. *Decriptarea mesajului*

A decripta textul criptat, de către interlocutorul B, înseamnă a obține mesajul M = 3 luând în considerare textul primit (a,b) = (2 , 5) și cheia secretă x = 5.

3.1. Într-adevăr, conform relației $M= ba^{(p-1-x)} \bmod p = 5x2^{(7-1-5)} \bmod 7 = 10 \bmod 7 =3$.

Așa cum am obținut că M = 3 rezultă că mesajul inițial a fost decriptat de interlocutorul B.

Exemplu 2. Interlocutorii A și B sunt într-o discuție secretă. Interlocutorul B solicită informație secretă complexă M de la interlocutorul A. În acest scop:

1. *Interlocutorul B generează cheia publică și cheia secretă*

1.1. Fie p=11 un număr prim și g = 3 o rădăcină primitivă a numărului p. Alegem un număr aleator x astfel încât $1 < x < p-1$. Fie x = 6.

1.2. Se calculează $y = g^x \bmod p = 3^6 \bmod 11 = 729 \bmod 11 = 3$.

1.3. Astfel, tripletul (p, g, y) = (11, 3, 3) este cheia publică iar cheia secretă este x = 6.

1.4. Interlocutorul B transmite interlocutorului A pe canale publice cheia deschisă (11, 3, 3) iar cheia secretă o păstrează doar pentru el.

2. *Criptarea și decriptarea mesajului*

2.1. Interlocutorul A dorește să cripteze mesajul M={B, A, C} care conform algoritmului fiecărui simbol trebuie să i se pună în corespondență un număr mai mic ca numărul prim p = 7. Fie B = 2, A =1, C=3.

2.2. Interlocutorul A alege numărul întreg k pentru care $1 < k < p-1$. Fie k = 4.

În continuare, procedeele de criptare și decriptare le vom include in tabelul de mai jos.

Textul	**B**	**A**	**C**
Codurile	2	1	3
$a = g^k \bmod p$	$a_1 = 3^4 \bmod 11 = 4$	$a_2 = 3^4 \bmod 11 = 4$	$a_3 = 3^4 \bmod 11 = 4$
$b = y^k M \bmod p$	$b_1 = 3^4\ 2 \bmod 11=8$	$b_2 = 3^4\ 1 \bmod 11=4$	$b_3 = 3^4\ 3 \bmod 11=1$
Textul criptat (a, b)	(4,8)	(4,4)	(4,1)
Mesajul decriptat $M = ba^{(p-1-x)} \bmod p$	$B=8x4^4 \bmod 11=2$	$A=9x4^4 \bmod 11=1$	$C=1x4^4 \bmod 11=3$

Decriptarea mesajului denotă că luând în considerare textele criptate (4,8), (4,4), (4,1) și cheia secretă x = 6, s-a obținut respectiv B=2, A=1 și C=3. Rezultă că mesajul inițial a fost decriptat corect de interlocutorul B. Autorii au elaborat un program C++ care realizează procesul de criptare și decriptare a mesajelor in conformitate cu algoritmul El Gamal.

Concluzii. Dezvoltarea unor algoritmi criptografici performanți necesită cunoștințe profunde în algebra abstractă aplicată și în domeniul teoriei numerelor. Într-o perspectivă apropiată se prefigurează noi imlementări ale criptografiei în domenii care țin de: robotică, Internet of Things, Cloud Computing, securitate casnică, tehnologii SMART, etc. Algoritmii criptografici, în mod special asimetrici, în acest scop, vor asigura confidențialitatea, integritatea și autenticitatea datelor. Din acest punct de vedere, pe piața muncii care ține de domeniul IT, sunt și vor fi căutați informaticieni cu pregătire fundamentală în domeniul fundamentelor algebrice. Acest fapt, presupune revizuirea 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 pieții muncii din domeniul IT.

Bibliografie

1. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31 (1985), p. 469 -472.
2. Diffie W., Hellman M.E. New Directions in Cryptography. IEEE Trans. on Information Theory, vol. IT-22 (1976), p. 644 - 654
3. Popovici C. Teoria numerelor. București: EDP, 1973. 294 p.
4. Horváth A. Introducere în Algebra Computațională. București: EDP, 1973. 190 p.
5. Groza B. Introducere in Criptografia Funcții Criptografice, Fundamente Matematice și Computaţionale. Timişoara: Editura Politehnica, 2012. 200 p.
6. Горбенко И. Д., Штанько И. А. Функции хеширования. Понятия, требования, классификация, свойства и применение В: Радиоэлектроника и информатика, №1, 1998. с.64-69.
7. Романьков В. А. Введение в криптографию. М.: ФОРУМ, 2012. 240 с.