

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 între conceptele matematice din teoria numerelor și algoritmi 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, militarie, 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 cercetărilor 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 și se bazează pe ”dificultatea” calculării valorilor logaritmilor discreți pe așa structuri algebrice precum corpuri finite. Acesta include: algoritmul de criptare El Gamal și 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 între numerele respective: teoremele lui Euclid, Ferma, Wilson, Frobenius, Hopf și 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. Relația de bază între numerele întregi care ne interesează este relația de divizibilitate. Să ne reamintim că proprietățile adunării (asociativitatea și comutativitatea, existența elementului nul 0, existența elementului opus $-n$ pentru fiecare număr întreg n), proprietățile înmulțirii (asociativitatea și comutativitatea, existența elementului neutru 1), împreună cu distributivitatea înmulțirii față de adunare, fac din mulțimea numerelor întregi un inel (comutativ) – notat cu Z . În acest inel doar numerele 1 și -1 au invers.

Definiția 1. Fie $n, m \in \mathbb{Z}$. Spunem că n îl divide pe m sau m este divizibil cu n , dacă există un unic $p \in \mathbb{Z}$ astfel încât $np = m$. Vom nota acest fapt $n|m$ sau $n:m$.

Se observă că dacă acceptăm această definiție, atunci 0 este divizibil cu orice număr nenul, dar nu divide nici un număr. Relația de divizibilitate între numere întregi are o serie de proprietăți, care se demonstrează foarte simplu dacă ținem cont de teorema împărțirii întregi.

Teorema 2. (Teorema împărțirii întregi). Fie $a, b \in \mathbb{Z}$, $b > 0$ (să-l numim pe a deîmpărțit, iar pe b , împărțitor). Atunci există două numere întregi $q, r \in \mathbb{Z}$, (numite cât, q respectiv rest, r) astfel ca 1) $a = b \cdot q + r$, 2) $0 \leq r < b$, și aceste două numere sunt și unice cu aceste proprietăți.

Clar lucru, dacă restul r este nul, atunci $b|a$, și invers, dacă $b|a$, atunci restul este nul. Să enumerăm acum proprietățile relației de divizibilitate între numere întregi.

Relația de divizibilitate între numere întregi are următoarele proprietăți:

1. $a|a$ pentru orice număr nenul $a \in \mathbb{Z}$ (reflexivitate)
2. dacă $a|b$ și $b|a$, atunci $a = b$ sau $a = -b$ (antisimetrie, pentru numere pozitive)
3. dacă $a|b$ și $b|c$, atunci $a|c$ (tranzitivitate)
4. dacă $1|a$ și $-1|a$ atunci pentru orice număr $a \in \mathbb{Z}$
5. dacă $a|b$ și $a|c$, atunci $a|b \pm c$
6. dacă $a|b$, atunci $a|bc$ pentru orice număr $c \in \mathbb{Z}$
7. dacă $a|b$, atunci $ac|bc$ pentru orice număr $c \in \mathbb{Z}$.

Definiția 3. Un număr $n \in \mathbb{N}$ este "prim" dacă are doi și numai doi divizori distincți. Un număr care are mai mult de doi divizori se numește "compus".

Observația 4.

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

Lema 5. Dacă n este prim și $n|ab$, atunci $n|a$ sau $n|b$.

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

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

Problema factorizării constă în determinarea tuturor divizorilor primi ai unui număr $n \in \mathbb{N}$.

Teorema 8. (Teorema fundamentală a aritmeticii). Fie $n \in \mathbb{N}$, $n > 1$. Atunci n admite o descompunere unică în produs de factori primi (ridicați la diverse puteri).

Teorema 9. (Euclid) Mulțimea numerelor prime este infinită.

2.2. Congruențe și inelul Z_n

Conceptul de “congruență” a fost introdus de Gauss și 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.

Congruențele constituie un mod ingenios și eficace de a transforma mulțimea infinită a întregilor într-o mulțime finită de întregi, cu păstrarea tuturor proprietăților celor două operații între întregi.

Definiția 10. Fie $n \geq 2$ un număr întreg. Relația între numerele întregi, definită prin $x \sim y$ dacă $n|x - y$, este o relație de echivalență compatibilă cu adunarea și înmulțirea întregilor, numită relație de congruență modulo n .

Clasele de echivalență se numesc clase de resturi modulo n , iar apartenența la aceeași clasă se mai notează $x \equiv y \pmod{n}$.

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

$$x = y \pmod{n}.$$

Compatibilitatea cu adunarea și înmulțirea întregilor înseamnă (modulul n fixat):

- a) $x_1 \sim y_1$ și $x_2 \sim y_2$ implică $x_1 + x_2 \sim y_1 + y_2$
- b) $x_1 \sim y_1$ și $x_2 \sim y_2$ implică $x_1 \cdot x_2 \sim y_1 \cdot y_2$ (1.58)

Datorită acestei compatibilități, operația de adunare și înmulțire între clase de echivalență prin intermediul a câte unui reprezentant arbitrar ales al clasei, funcționează, este bine definită: altfel spus, nu depinde de alegerea reprezentanților claselor. Prin urmare congruențele modulo n au următoarele proprietăți:

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

1. $x = x \pmod{n}$ pentru orice număr întreg x ;
2. $x = y \pmod{n}$ dacă și numai dacă $y = x \pmod{n}$, pentru orice numere întregi x, y ;
3. dacă $x = y \pmod{n}$ și $y = z \pmod{n}$ atunci $x = z \pmod{n}$, \forall numere întregi x, y, z ;
4. $x_1 = y_1 \pmod{n}$ și $x_2 = y_2 \pmod{n}$ implică $x_1 + x_2 = y_1 + y_2 \pmod{n}$;
5. $x_1 = y_1 \pmod{n}$ și $x_2 = y_2 \pmod{n}$ implică $x_1 \cdot x_2 = y_1 \cdot y_2 \pmod{n}$;
6. $x = 0 \pmod{n}$ înseamnă $x = kn$ pentru o valoare potrivită a lui k , sau pur și 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 operațiile de adunare și înmulțire există între numerele întregi, văzută doar pe ultima cifră a numerelor, își păstrează toate proprietățile avute: adunarea este asociativă, există element nul, 0 , fiecare număr k , ($0 \leq k \leq n-1$) are opus ($-0 = 0$ respectiv $-k = n - k$), și așa mai departe. Ba chiar proprietățile se pot îmbunătăți: dacă modulul n este ales număr prim, atunci devine posibilă și împărțirea necondiționată.

Exemplul 12. Deoarece $3|(10 - 1)$, vom avea $10 \equiv 1 \pmod{3}$. Dacă $11|(16 - (-6))$, atunci $16 \equiv -6 \pmod{11}$. Avem că $7|(16 - 2)$, atunci $16 \equiv 2 \pmod{7}$.

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:

$a \equiv 7 \pmod{11}$; $b \equiv 7 \pmod{11}$; $c \equiv 7 \pmod{11}$.

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 $7 \pmod{11} \equiv 18 \pmod{11} \equiv 29 \pmod{11}$.

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 $a \in \mathbb{Z}$ este congruent modulo n cu un singur întreg din mulțime.*

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

Exemplul 16. Există patru congruențe modulo 4:

- 1) $\{0\} = \{\dots, -4, 0, 4, 8, \dots\}$,
- 2) $\{1\} = \{\dots, -3, 1, 5, \dots\}$,
- 3) $\{2\} = \{\dots, -2, 2, 6, \dots\}$,
- 4) $\{3\} = \{\dots, -1, 3, 7, \dots\}$.

Fiecare număr întreg (element din \mathbb{Z}) se află în exact una din aceste mulțimi. Pentru două mulțimi $A, B \subseteq \mathbb{Z}$ pot fi definite operațiile $A \pm B = \{x \pm y \mid x \in A, y \in B\}$, $AB = \{x \cdot y \mid x \in A, y \in B\}$.

Propoziție 17. *$\mathbb{Z}/n\mathbb{Z}$ este inel unitar, numit “inelul claselor de resturi” modulo n .*

Teorema 18. *(Teorema chineza a resturilor). Fie $n \geq 2$ un număr natural și x_1, x_2, \dots, x_n numere întregi prime între ele două câte două și a_1, a_2, \dots, a_n numere întregi oarecare. Atunci există o soluție pentru sistemul de congruențe: $x \equiv a_1 \pmod{x_1}, x \equiv a_2 \pmod{x_2}, \dots, x \equiv a_n \pmod{x_n}$.*

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

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

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

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

Proprietățile evidențiate până la acest moment pot fi reformulate mai elegant folosind proprietăți 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 împărți cu orice întreg nenul, astfel ca este valabilă "proba" împărțirii, iar câtul și restul sunt unici, dacă restul este între 0 și modulul împărțitorului minus 1 (este valabilă teorema împărțiri întregi).
- Inelul întregilor este inel cu ideale principale: orice ideal este format din toți multiplii unui număr.
- În inelul întregilor orice pereche de numere (nu ambele nule) are un cel mai mare divizor comun (și un cel mai mic multiplu comun).
- Mulțimea 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 și 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 n_1, n_2, \dots, n_k sunt relativ prime două câte două, atunci inelele $Z_n \equiv Z_{n_1} \oplus Z_{n_2} \oplus \dots \oplus Z_{n_k}$, sunt izomorfe, unde am notat $n = n_1 \cdot n_2 \cdot \dots \cdot n_k$. Aceasta este o reformulare a teoremei chinezești a resturilor.

2.3. Rădăcini primitive ale unui număr prim

Definiția 22. Fie $n \geq 2$ un număr natural și a un număr prim cu n . Numim ordinul lui a modulo n cel mai mic număr k ce satisface congruența $a^k \equiv 1 \pmod{n}$.

Fie $n \geq 2$ un număr natural fixat și a un număr întreg prim cu n . Definim mulțimea:

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

Conform teoremei lui Euler, $\phi(n) \in E$, deci $E \neq \emptyset$. În 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 $\text{ord}_n(a)$.

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 $\text{ord}_7(2) = 3$.

Pentru a caracteriza mulțimea E introdusă mai sus (și implicit toate soluțiile congruenței $a^x \equiv 1 \pmod{n}$ cu a și n date), sunt demonstrate mai multe proprietăți care se utilizează în teoria criptografiei.

Definiția 23. Fie $n \geq 2$ un număr natural și a un număr întreg prim cu n . Atunci a se numește rădăcină primitivă modulo n dacă $\text{ord}_n(a) = \phi(n)$.

Fie $n = 7$. Pentru $a = 3$, vom avea: $3^1 \equiv 3 \pmod{7}$, $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 \equiv 4 \pmod{7}$, $3^5 \equiv 5 \pmod{7}$, $3^6 \equiv 1 \pmod{7}$, așa dar $\text{ord}_7(3) = 6$. Astfel, deoarece $\text{ord}_7(3) = 6 = \phi(7)$ putem afirma că 3 este o rădăcină 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 $y = g^x \text{ mod } p$;
- 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 $a = g^k \text{ mod } p$ și $b = y^k M \text{ mod } p$.
- 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: $M = b(a^x)^{-1} \pmod{p}$.

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

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 $y = g^x \pmod{p} = 2^5 \pmod{7} = 32 \pmod{7} = 4$
- 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 $a = g^k \pmod{p} = 2^4 \pmod{7} = 2$.
- 2.4. Se calculează $b = y^k M \pmod{p} = 4^4 3 \pmod{7} = 768 \pmod{7} = 5$
- 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 $M = ba^{(p-1-x)} \pmod{p} = 5 \times 2^{(7-1-5)} \pmod{7} = 10 \pmod{7} = 3$.

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 $y = g^x \pmod{p} = 3^6 \pmod{11} = 729 \pmod{11} = 3$.
- 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 creeze 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 în 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 $M = ba^{(p-1-x)} \bmod p$	$B=8 \times 4^4 \bmod 11=2$	$A=9 \times 4^4 \bmod 11=1$	$C=1 \times 4^4 \bmod 11=3$

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 în 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 implementări 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 în Criptografia Funcții Criptografice, Fundamente Matematice și Computaționale. Timișoara: 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.