Criptografierea datelor

Asigurarea secretului informațiilor conținute în secvența de date transmisă (**criptografierea** sau **cifrarea** datelor) și **autentificarea** sunt funcții complementare într-un sistem de comunicații digitale. Serviciile de tip poștă electronică, în general de comunicație prin intermediul rețelelor publice (de calculatoare sau chiar pe linie telefonică) necesită aplicarea unor metode de criptografiere și autentificare altfel un receptor neautorizat poate intercepta mesajele fie pentru a extrage informații utile, fie pentru a le falsifica.

Criptografierea datelor reprezintă operația care asigură secretul de transmisie într-un sistem digital de comunicații astfel încât pentru un receptor neautorizat mesajul transmis să fie neinteligibil.

Circuitul respectiv de codare și de decodare se numește **criptosistem**.

Secvența utilizată pentru codarea ori decodarea datelor într-un criptosistem se numește **cheie** de transmisie.

Autentificarea este funcția care asigură proveniența corectă de la sursa autorizată a mesajului recepționat excluzând posibilitatea primirii unor informații false. Autenticitatea datelor este dovedită de o **semnătură digitală** care nu poate fi falsificată datorită unor caracteristici comune ale acesteia cu sistemul de decodare.

În continuare ne vom referi la sistemele de criptografiere a datelor (în format binar sau multibit), nu la eventuala prelucrare a unui set de caractere de tip alfanumeric.

Există trei tipuri majore de criptosisteme:

I. **Criptosistemul convențional** utilizează o așa-numită **cheie secretă** și anume o funcție E_k inversabilă, cunoscută doar de utilizatori. Cheia transmisă pe canalul de comunicații secret (Fig.1) poate fi chiar indicele k specificând funcția dintr-un set de funcții cunoscut doar în sistemele autorizate.

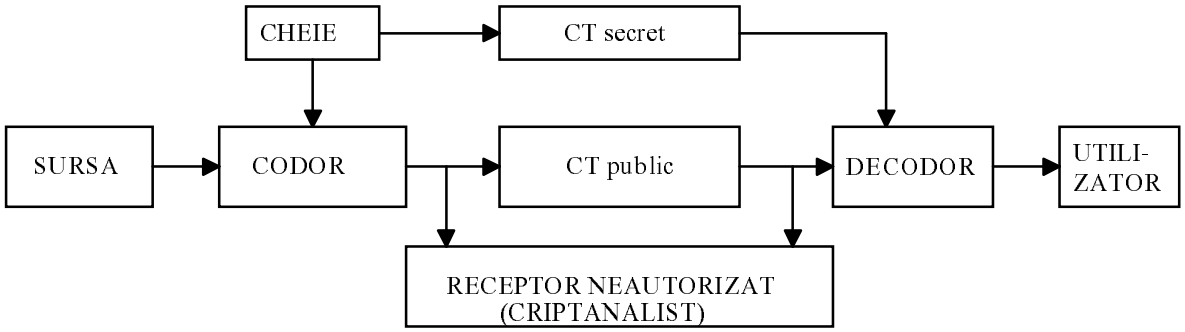

Fig.1 Criptosistem cu cheie secretă

Este evident faptul că o transmisie cu grad ridicat de securitate are un cost mult mai mare decât una efectuată într-o rețea publică de comunicații. Astfel durata transmisiei pe canalul de comunicații secretizat trebuie să fie mult redusă comparativ cu cea din rețeaua publică.

Funcția utilizată pentru criptare poate fi liniară sau neliniară, eventual dependentă de un parametru care poate fi chiar cheia de transmisie:

$$\bar{c} = E_k(\bar{d}) \qquad (1)$$

unde $\bar{c}$ - este secvența codată (cifrată) iar $\bar{d}$ este secvența de date.

Decodarea se realizează prin aplicarea funcției inverse:

$$E_k^{-1}(\bar{c}) = E_k^{-1}(E_k(\bar{d})) = \bar{d} \qquad (2)$$

Dezavantajul criptosistemelor cu cheie secretă constă în probabilitatea mare de deducere a cheii de transmisie de către criptanalist pe baza redundanței crescute a semnalului codat (având în vedere faptul că lungimea cheii este inferioară lungimii mesajului) ori de interceptare a acesteia chiar pe canalul de comunicații de securitate maximă.

✍ **T1.** Scrieți ecuații de criptare și de decriptare în GF(N) de forma:

- codare: $c = k_1 a$

- decodare: $d = k_2 c$

unde (k_1, k_2) este o pereche de numere inverse unul altuia din GF(N) reprezentând cheile de codare și de decodare; ***a*** este simbolul de intrare; ***c*** este simbolul codat; ***d*** este simbolul decodat (N = 8 sau 16). Operațiile de multiplicare se efectuează în GF de definiție a codului. Determinați coeficienții polinoamelor de ieșire în funcție

de coeficienții polinoamelor de intrare în codor, respectiv decodor. Scrieți și testați în MATLAB algoritmii de criptare-decriptare pentru valorile-cheie alese.

❖ Utilizați funcția *prodgf* din MATLAB (Anexa I) și tabelele cu elemente inverse deduse pentru câmpurile GF(8) și GF(16).

II. **Criptosistemul cu cheie publică** (Fig.2) utilizează o cheie de transmisie mai puțin obișnuită denumită. Este vorba de o funcție inversabilă într-un singur sens (*one-way function*) a cărei inversă nu poate fi calculată practic întrucât acest calcul implică depășirea fie a capacității sistemelor de calcul utilizate, fie a timpului în care informațiile transmise sunt valabile și considerate secrete. În fapt, cheia de transmisie a fost dedusă relativ simplu și într-un timp rezonabil din inversa sa în sistemul autorizat. Lungimea cheii trebuie să fie comparabilă cu cea a mesajului. Funcția inversă reprezentând cheia de decodare este deja cunoscută de utilizator și aplicată pentru implementarea decodorului.

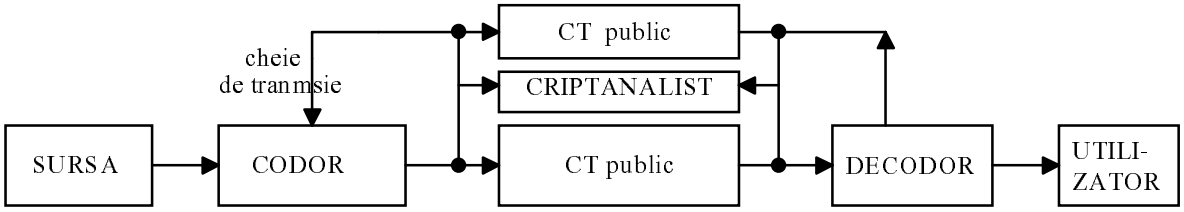

Fig.2 Criptosistem cu cheie publică

✍ **T2.** Să se determine inversa funcției *f(x)* definite în GF(8) (cu max. 8 termeni):
$f(x) = 1 + 2x$.

Utilizați tabelele de sumare și multiplicare în GF(8). Funcția *f(x)* constituie cheia publică a sistemului. Inversa cheii publice, respectiv cheia de decodare, va fi de forma:

$f^{-1}(x) = 1 + 2x + 4x^2 + c_3x^3 + c_4x^4 + c_5x^5 + c_6x^6 + c_7x^7 + c_8x^8$.

Limitarea numărului de termeni ai inversei a fost impusă pentru simplificarea calculului. În caz real lungimea inversei va fi egală sau mai mare decât cea a mesajului ce urmează a fi codat.

✍ **T3.** Scrieți algoritmii de criptare și de decriptare cu cheie publică în GF. Polinomul corespunzător secvenței de date de intrare în codor este multiplicat cu cheia *f(x)*. Coeficienții polinomului obținut reprezintă secvența codată transmisă.

Decodorul (soft sau hard) va efectua produsul dintre polinomul asociat secvenței recepționate și funcția inversă. Testați algoritmii pe o secvență de 8 simboluri din GF(8).

❖ În MATLAB este definită funcția *polgf* (Anexa I) de multiplicare a două polinoame într-un GF dat. Polinoamele sunt introduse în program prin vectorii coeficienților citiți în ordinea crescătoare a puterilor variabilei.

III. **Criptosistemul cu spectru extins** se bazează pe metodele de extensie a spectrului semnalului transmis pe un canal de comunicații digital astfel încât orice receptor neautorizat să primească doar o versiune 'foarte zgomotoasă' a acestuia, fiind practic imposibilă detecția semnalului util sub o valoare critică a raportului de puteri semnal/zgomot.

Observație: Există multe alte metode de criptare a informației, prin permutări aleatoare de caractere, substituții ale acestora și altele care obligă criptanalistul să deducă secvența de date doar prin încercări. Evident numărul combinațiilor posibile trebuie să fie suficient de mare (ex. 10! = 3628800) astfel încât timpul necesar decodării prin încercări, chiar a unei secvențe relativ scurte, să depășească intervalul critic în care informațiile respective sunt utile adversarului. Pe de altă parte, decodorul autorizat trebuie să dispună de un algoritm rapid de decodare pe baza secvenței-cheie publice transmise.

Un astfel de criptosistem este cel denumit '**rucsacul capcană**" și folosește o așa-numită secvență monotonă de simboluri $\{b_0, b_1, \ldots b_N\}$, rapid crescătoare (*superincreasing*), adică:

$$b_k > \sum_{i=0}^{k-1} b_i \;\forall k = 1...N. \qquad (3)$$

Această secvență utilizată pentru codarea datelor urmează a fi codată pe baza unei **chei secrete** în vederea transmisiei pe canalul public de comunicații a unei secvențe aleatoare nemonotone ce constituie **cheia publică**.

Pentru exemplificare să considerăm secvența rapid crescătoare:

$\{b_0, b_1, b_2, b_3\}=\{2; 3; 6; 14\}$.

Se va lucra în câmpul GF(16). Fie vectorul de intrare:

$\bar{a} = [1\,0\,1\,1\,0\,1\,0\,1]$

Se codează succesiv câte N = 4 biți de intrare conform relației:

$$c = \sum_i a_i b_i \qquad (4)$$

(Operațiile sunt efectuate în sistemul zecimal.)

Rezultă:

$c_1 = 2 \cdot 1 + 3 \cdot 0 + 6 \cdot 1 + 14 \cdot 1 = 22 = 10110_{(2)}$

$c_2 = 2 \cdot 0 + 3 \cdot 1 + 6 \cdot 0 + 14 \cdot 1 = 17 = 10001_{(2)}$

Se transmite vectorul codat: $\bar{c} = 1011010001$ cu o rată de codare 4:5.

Codarea cheii inițiale se va face cu o pereche de numere inverse unul altuia din GF(16), de exemplu (2; 9), conform relațiilor:

$$b_k' = 2 \cdot b_k;\ b_k = 9 \cdot b_k' \qquad (5)$$

cu multiplicare în GF(16).

Observație: Se pot aplica și alte tehnici de codare a secvenței-cheie, de exemplu sumare în GF cu un simbol din acest câmp, același și la emisie, și la recepție.

Cheia publică transmisă conform relației (5) este:

$\bar{b}' = \{1; 6; 12; 15\}$.

Algoritmul rapid de decodare necesită exact N pași. Prin comparări succesive ale valorilor vectorilor recepționați (de 5 biți) exprimate în zecimal cu sumele parțiale ale secvenței-cheie se obțin biții de date:

1. Dacă $c_{(10)} > \sum_{i=1}^{3} b_i \rightarrow a_4 = 1$, în caz contrar rezultă $a_4 = 0$.

2. Dacă $c_{(10)} - b_4 a_4 > \sum_{i=1}^{2} b_i \rightarrow a_3 = 1$ și în caz contrar $a_3 = 0$. ș.a.m.d.

.....

Pentru secvența de cod considerată se obține:

$22 > 2 + 3 + 6 \rightarrow 1$

$22 - 1 \cdot 14 > 2 + 3 \rightarrow 1$

$22 - 1 \cdot 14 - 1 \cdot 6 \le 2 \rightarrow 0$

$22 - 1 \cdot 14 - 1 \cdot 6 - 3 \cdot 0 = 2 \cdot 1 \rightarrow 1$ Deci primii biți de date sunt: 1 0 1 1.

$17 > 11 \rightarrow 1$

$17 - 1 \cdot 14 \le 5 \rightarrow 0$

$17 - 1 \cdot 14 - 0 \cdot 6 > 2 \rightarrow 1$

$17 - 1 \cdot 14 - 0 \cdot 6 - 1 \cdot 3 = 2 \cdot 0$ Rezultă un alt grup de biți: 0 1 0 1.

Se reconstituie vectorul datelor: 1 0 1 1 0 1 0 1.

Să încercăm decodarea cu secvența b_k':

$22 > 1 + 6 + 12 \rightarrow 1$

$22 - 15 \cdot 1 \le 1 + 6 \rightarrow 0$

$22 - 15 \cdot 1 - 12 \cdot 0 > 1 \rightarrow 1$

$22 - 15 - 0 - 6 \cdot 1 = 1 \cdot 1 \rightarrow 1$

adică primul grup de biți decodați ar fi fost: 1 1 0 1 în loc de 1 0 1 1. Rezultă deja 2 erori de decodare.

❖ În MATLAB sunt realizați algoritmii de criptare și de decriptare, funcțiile *encript* și *decript* (Anexa III), cu o cheie publică și una secretă, cu operare în GF(16).

✍ **T4.** Codați și decodați pe baza algoritmilor sus-menționați secvența:

0 0 1 0 1 1 1 0 1 1 0 0.

Ce chei de transmisie se utilizează?

Modificați secvențele-cheie și testați algoritmii în acest caz.