Criptografie - Tema 9

Popescu Paul - Constantin
Facultatea de Matematică

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		?	!	.
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

1. Implementaţi criptosistemul Massey-Omura

```
#include "cripto_tools.hpp"

int MasseyOmura(int p, int eA, int eB, int m) {
    if (eA > p - 1 || eB > p - 1) {
        std::cerr << "Numar e introdus invalid.\n";
        return 1;
    }

    int dA = invers(eA, p - 1);
    int dB = invers(eB, p - 1);

    int C1 = a_la_b_mod_c(m, eB, p);
    int C2 = a_la_b_mod_c(C1, eA, p);
    int C3 = a_la_b_mod_c(C2, dB, p);
    int Cmes = a_la_b_mod_c(C3, dA, p);

    std::cout << "Mesajul este: " << Cmes << "\n";
    return Cmes;
}
```

2. Alice și Bob doresc să stabilească o cheie secretă k (pe care să o cunoască doar ei) folosind criptosistemul Diffie-Hellman. Ei aleg numărul prim $p = 17$ și generatorul $g = 5$ al lui $\mathbb{Z}_{17}$. Alice alege exponentul secret $a = 3$, iar Bob alege exponentul secret $b = 6$. Determinați cheia k.

$$u = g^a = 5^3 (\text{mod} 17) = 6, v = g^b = 5^6 (\text{mod} 17) = 2$$
$$k = v^a (\text{mod} p) \Rightarrow k = 2^3 (\text{mod} 17) = 8$$
$$k = u^b (\text{mod} p) \Rightarrow k = 6^6 (\text{mod} 17) = 8$$

$$\Rightarrow k = 8$$

3. Alice utilizează un criptosistem El Gamal și are cheia publică $(31, 3, 19)$. Bob dorește să-i trimită mesajul X și alege parametrul $k = 3$. Să se determine mesajul criptat. Alfabetul folosit are 30 de caractere.

$$u = g^k (\text{mod} p) = 3^3 (\text{mod} 31) = 27$$
$$X = 23 \Rightarrow v = 23 \times 19^3 (\text{mod} 31) = 29$$

$$\Rightarrow (u, v) = (27, 29)$$

4. Fie $(53, 2, 30)$ cheia publică a lui Alice într-un criptosistem El Gamal. Bob utilizează această cheie ca să genereze mesajul criptat $(24, 37)$. Determinați mesajul în clar corespunzător.

Trebuie să gasim a astfel incat $2^a \equiv 30(\text{mod}53)$. Prin forta bruta, gasim $a = 13$

Mesajul X se calculeaza prin $X = v \cdot (u^a)^{-1}(\text{mod}p) = 37 \cdot (24^{13})^{-1}(\text{mod}53)$

$24^{13} \equiv 10(\text{mod}53) \quad 10^{-1} \equiv 16(\text{mod}53) \quad 37 \cdot 16 \equiv 9(\text{mod}53)$

$\Rightarrow X = 9$

5. Alice primește mesajul $(30, 7)$, obținut cu ajutorul unui criptosistem El Gamal. Decriptați mesajul, cunoscând cheia publică lui Alice $(p = 43, g = 3)$.

6. Ana și Bob folosesc criptosistemul ElGamal. Ana are cheia privată $Kd = (p = 71, g = 33, a = 34)$.

a) Determinați cheia publică a Anei.

b) Bob alege $k = 3$ pentru a-i transmite Anei mesajul **AZI**

Știind că k se păstrează, lungimea blocurilor în clar este 1 și a celor criptate este 2, determinați mesajul criptat. Alfabetul folosit este: ABCDEFGHIJKLMNOPQRSTUVWXYZ ?!.1234567890

$$\textbf{AZI} \rightarrow (0)(25)(8)_{(40)}$$

a) Mai intai calculam $u = g^k(\text{mod}p) = 33^3(\text{mod}71) = 11$ si $\beta^k(\text{mod}p) = 43^3(\text{mod}71) = 58$

b) Acum vom putea cripta fiecare caracter in parte:

$A : v = 0 \cdot 58(\text{mod}71) = 0 \qquad Z : v = 25 \cdot 58(\text{mod}71) = 30 \qquad I : v = 8 \cdot 58(\text{mod}71) = 38$

Mesajul criptat este: $(0)(30)(38)_{(40)} = A19_{(40)}$