Tema 8

a) Determinarea cheii publice a Anei

Cheia publică în ElGamal se determină astfel:

- pp: un număr prim
- gg: o bază (un element primitiv al grupului multiplicativ modulo pp)
- $y=ga \mod py=g_a \mod p$

Ana are cheia privată $Kd=(p=71,g=33,a=34)K_d=(p=71,g=33,a=34)$.

Calculăm yy:

$$y=ga \mod p=3334 \mod 71y=g_a \mod p=33_{34} \mod 71$$

Pentru a calcula $3334 \mod 7133_{34} \mod 71$, vom folosi exponențierea modulară rapidă:

1. $332 \mod 71=1089 \mod 71=2533_2 \mod 71=1089 \mod 71=25$
2. $334 \mod 71=(332)2 \mod 71=252 \mod 71=625 \mod 71=6533_4 \mod 71=(33_2)_2 \mod 71=25_2 \mod 71=625 \mod 71=65$
3. $338 \mod 71=(334)2 \mod 71=652 \mod 71=4225 \mod 71=2833_8 \mod 71=(33_4)_2 \mod 71=65_2 \mod 71=4225 \mod 71=28$
4. $3316 \mod 71=(338)2 \mod 71=282 \mod 71=784 \mod 71=233_{16} \mod 71=(33_8)_2 \mod 71=28_2 \mod 71=784 \mod 71=2$
5. $3332 \mod 71=(3316)2 \mod 71=22 \mod 71=433_{32} \mod 71=(33_{16})_2 \mod 71=2_2 \mod 71=4$
6. $3334 \mod 71=3332 \cdot 332 \mod 71=4 \cdot 25 \mod 71=100 \mod 71=2933_{34} \mod 71=33_{32} \cdot 33_2 \mod 71=4 \cdot 25 \mod 71=100 \mod 71=29$

Deci, $y=29y=29$.

Cheia publică a Anei este: $Kp=(p=71,g=33,y=29)K_p=(p=71,g=33,y=29)$

b) Criptarea mesajului "AZI"

Folosim $k=3k=3$ pentru criptare.

Alfabetul utilizat este: ABCDEFGHIJKLMNOPQRSTUVWXYZ ?!.123456789

Fiecare caracter este mapat la un număr, după cum urmează:

- A = 0, B = 1, ..., Z = 25, ? = 26, ! = 27, . = 28, 1 = 29, ..., 9 = 37

Mesajul "AZI" devine:

- A = 0
- Z = 25
- I = 8

Criptăm fiecare caracter separat.

Pentru fiecare caracter mm:

1. Calculăm $c1=gk\text{mod } pc_1=g_k\text{mod}p$.
2. Calculăm $c2=m\cdot yk\text{mod } pc_2=m\cdot y_k\text{mod}p$.

Cu $k=3k=3$:

$$c1=333\text{mod } 71=35937\text{mod } 71=47c_1=33_3\text{mod}71=35937\text{mod}71=47$$

Pentru fiecare caracter:

1. $m=0m=0$:

$$c2=0\cdot 293\text{mod } 71=0c_2=0\cdot 29_3\text{mod}71=0$$

2. $m=25m=25$:

$$c2=25\cdot 293\text{mod } 71=25\cdot 24389\text{mod } 71=25\cdot 49\text{mod } 71=1225\text{mod } 71=17c_2=25\cdot 29_3\text{mod}71=25\cdot 24389\text{mod}71=25\cdot 49\text{mod}71=1225\text{mod}71=17$$

3. $m=8m=8$:

$$c2=8\cdot 293\text{mod } 71=8\cdot 24389\text{mod } 71=8\cdot 49\text{mod } 71=392\text{mod } 71=37c_2=8\cdot 29_3\text{mod}71=8\cdot 24389\text{mod}71=8\cdot 49\text{mod}71=392\text{mod}71=37$$

Deci, mesajul criptat "AZI" devine perechile $(c1,c2)(c_1,c_2)$:

$$(47,0),(47,17),(47,37)(47,0),(47,17),(47,37)$$

Mesajul criptat este:

$$(47,0),(47,17),(47,37)(47,0),(47,17),(47,37)$$

Folosind notația alfabetului, acesta se scrie ca:

$$470,4717,4737470,4717,4737$$

Astfel, mesajul "AZI" este criptat ca $(47,0),(47,17),(47,37)(47,0),(47,17),(47,37)$.