14

Tema 8
Valachi Emilia, M532

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

a) Determinați cheia publică a Anei.

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T
20	21	22	23	24	25	26	27	28	29
U	V	W	X	Y	Z	?	!	.	1
30	31	32	33	34	35	36	37	38	
2	3	4	5	6	7	8	9	spațiu?	

$p = 71$, $g = 33$, $a = 34$

$g \in \mathbb{Z}_{71}^*$

Ana generează: $p \neq$ prim

$g \in \mathbb{Z}_p^*$

$q_A \in (0, p-1)$

publică: $K = (p, g, \alpha = g^{q_A})$

privată: $k_d = q_A$

$g = 33$

$q_A = 34$

$g^{q_A} \pmod p = 33^{34} \pmod{71} = (33^8 \cdot 33^8 \cdot 33^8 \cdot 33^8 \cdot 33^2) \pmod{71} =$

$33^2 \pmod{71} = 1088 \pmod{71} = 24 \pmod{71}$

$33^4 \pmod{71} \equiv$ [illegible] $\pmod{71}$

$33^8 \pmod{71} \equiv 64 \pmod{71}$

$= (64^4 \cdot 24) \pmod{71} = (45^2 \cdot 24) \pmod{71} = (58 \cdot 24) \pmod{71}$

$= 43 \pmod{71}$

$\Rightarrow$ cheia publică: $(71, 33, 43)$

b) Bob alege $k = 3$ pentru a-i transmite Ani mesajul (AZI.)

Știind că k se păstrează, lung. blocurilor în clar este 1, criptate - 2, determinați mesajul criptat.

- Bob obț. cheia publică $K_e = (p, g, y)$ = $(71, 33, 43)$
- Alege k la întâmplare.
- Trimite $u = g^{k} \pmod p$, $v = m \cdot \alpha^{k} \pmod p$ $\xrightarrow{(u,v)}$ Ana

α^k - mesaj g^k - cheie

$k = 3 \Rightarrow u = 33^3 \pmod{71} \Rightarrow \underline{u = 11 \pmod{71}}$

$v = m \cdot 43^3 \pmod{71}$ $w = u^{p-1-a} \pmod p$ $m' = v \cdot w \pmod p$

$AZ = 0 \cdot 39 + 25 = 25 \Rightarrow v_1 = 25 \Rightarrow m_1 = 11 \cdot 25 \pmod{71}$

$= 62 \pmod{71}$

I (stație?) $= 8 \cdot 39 + 38 = 350 \pmod{71} = 66 \pmod{71}$

$\underline{w = 11^{38} \pmod{71} = 60 \pmod{71}}$

$m_1' = v_1 \cdot w \pmod p = 60 \cdot 62 \pmod{71} = 28 \longrightarrow$.

$m_2' = 60 \cdot 66 \pmod{71} = 55$

Am ajuns unde trebuie. :)