12. Fie p = 65537 și g = 5. Alice primește mesajul (29095, 23846), pe care Bob l-a obținut folosind
criptosistemul El Gamal in Zp cu cheia publică (p, g, ga). Cheia secretă a lui Alice este a = 13908
ABCDEFGHIJKLMNOPQRSTUVWXYZ ?!.123456789

$(p, g, g^a) = (65537, 5$

$g^a = 5^{13908} \pmod{65537} = (5^2)^{7454} = (25^2)^{3727} =$

$= 625 \cdot (625^2)^{1863} = 625 \cdot (390625)^{1863} \equiv 625 \cdot (62940)^{1863} \equiv$

$\equiv 625 \cdot (-2597) \cdot (-2597^2)^{931} =$

$= -1623.125 \cdot (-674409)^{931} = 1623125 \cdot 674409^{931} \equiv$

$1623125 = 50237 = -15300$

$674409 = 59635 = -5902$

$= (-15300)(-5902) \cdot ((-5902)^2)^{465} \equiv 90300600 \cdot 34833604^{465} =$

$90300600 = 56151 = -9386$

$34833604 = 33457$

$= -1 \cdot 9386 \cdot 33457 \cdot (33457^2)^{232} = 25902 \cdot (-1111^2)^{116} =$

$33457^2 = 1119370849 = 64426 = -1111$

$9386 = -25902$

$= 25902 \cdot 1234321^{116} \equiv 25902 \cdot -10882^{116} = 25902 \cdot (10882^2)^{58} =$

$= 25902 \cdot [(-7435)^2]^{29} = 25902 \cdot 31534 \cdot (31534^2)^{14} =$

$= 6037 \cdot 255^{14} = 6037 \cdot 65025^7 = 6037 \cdot (-512) \cdot (512^2)^3 =$

$= -10705 \cdot -4^3 = -10705 \cdot -48 = 513840 = 54829 =$

$= -10744$

7. 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 ,si a celor criptate este 2, determinați mesajul criptat. Alfabetul folosit este

ABCDEFGHIJKLMNOPQRSTUVWXYZ ?!.123456789

8. 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 Z17. Alice alege exponentul secret a = 3, iar Bob alege exponentul secret b = 6. Determinați cheia k.

(7) Cripto. ElG. $K_d = (p=71, g=33, a=34)$

a) cheia publică:

$A = g^a \pmod p = 33^{34} \pmod{71} = (33^2)^{17} \pmod{71} = 1089^{17} \pmod{71} \equiv$

$\equiv 24^{17} \pmod{71} = 24 \cdot (24^2)^8 \pmod{71} = 24 \cdot 576^8 \equiv 24 \cdot 8^8 =$

$= 24 \cdot (8^2)^4 = 24 \cdot (64^2)^2 = 24 \cdot 4096^2 \equiv 24 \cdot 49^2 = 24 \cdot 2401 \equiv$

$= 24 \cdot 58 = 1392 \pmod{71} \equiv 43 \bmod 71 \Rightarrow A = 43$

b) $k=3$, AZI, $A=1, Z=26, I=9$

A = 1: $c_1 = 33^3 \pmod{71} \equiv 11$, $c_2 = 1 \cdot 43^3 (\text{-}''\text{-}) \equiv 58$) (11, 58)

Z = 26: $c_1 = 33^3 \pmod{71} = 11$, $c_2 = 26 \cdot 43^3 (\text{-}''\text{-}) = 17$) (11, 17)

I = 9: $c_1 = 11$, $c_2 = 9 \cdot 43^3 \pmod{71} = 25$) (11, 25)

(8) $A = g^a \pmod p = 5^3 \pmod{17} = 125 = 6 \pmod{17}$

$B = g^b \pmod p = 5^6 \pmod{17} = (5^3)^2 = 6^2 = 36 \equiv 2$

$K = B^a \pmod p = 2^3 = 8$

$K = A^b \pmod p = 6^5 = 6 \cdot (6^2)^2 = 6 \cdot 4^2 = 6 \cdot 8 \equiv 7$