TEMA 8

Ex. El Gamal. Ama cheia priv. kd = (p=71, g=33, a=34)

a) cheia publică = ?

b) k=3 m = AZi

Det mesj. criptat

a) p=71, g=33, a=34 $g^a \pmod p = 33^{34} \pmod{71}$

$g^a \pmod p = (33^2)^{17} \pmod{71} = 1089^{17} \pmod{71} = 24^{17} \pmod p$

$= 24 \cdot (24^2)^8 \pmod{71} = 24 \cdot 8^8 \pmod p = 24 (8^4)^2 =$

576 4096

$= 24 \cdot 49^2 \pmod{71} = 24 \cdot 58 \pmod{71} = 43$

cheia publică: (71, 33, 43)

b) lungimea sir clar 1 ; cele criptate = 2

m = AZi

$u = g^k \pmod p = 33^3 \pmod p = 24 \cdot 33 \pmod{71} = 11$

$v = m \cdot \alpha^k \pmod p$

alfabet° =

A = (0) = 30 · 30° = 0.

Z = (25) = 25 · ..° = 25

i = (8) = 8 · ..° = 8