Tema 10 -

1) $m = 343$

$p = 48731$

$g = 443$

$x = 7$

Cheia secretă a lui Alice este $a = 242$

a) $g = 7^{\frac{(48731-1)}{443}} \pmod{48731} = 7^{110} \pmod{48731} = 5260 \pmod{48731}$

$\alpha = 5260^{242} \pmod{48731} = 3438$

Cheia publică $(48731, 443, 4260, 3438)$

$p \quad g \quad \beta \quad \alpha$

2) $m = 11111$

$Ke = (n = 28829, e)$

Det semnătura

$S = m^e \pmod{n} = 11111^e \pmod{28829}$

$n = 28829$

$[\sqrt{(28829)}] = 169$

$t = 170 \Rightarrow 170^2 - n = 28900 - 28829 = 71$

$t = 171 \Rightarrow 171^2 - n = 29241 - 28829 = 412$

$t = 172 \Rightarrow 172^2 - n = 29584 - 28829 = 755$

$t = 173 \Rightarrow 173^2 - n = 29929 - 28829 = 1100$

$t = 174$

$t = 175$

$t = 176$

$t = 177 \Rightarrow 177^2 - n = 31329 - 28829 = 2500 = 50^2$

$\Rightarrow S^2 = 50^2$

$\Rightarrow S = 50$

$n = (177 - 50)(177 + 50) = 227 \cdot 127$

3. $p = 1223$

$q = 1987$

$Ke = (n = p \cdot q = 2430101,\ e = 948047)$

Determinați semnătura pentru mesajul $m = 1070777$

$S = m^e \pmod n$

$d \cdot e = 1 \pmod{f(n)}$

$f(n) = (p-1)(q-1) = 1222 \cdot 1986 = 2426892$

$d = e^{-1} \pmod{f(n)} = 948047^{-1} \pmod{2426892}$

$2426892 = 2 \cdot 948047 + 530798$

$\Rightarrow x_{530798} = x_{2426892} - 2 \cdot x_{948047} = (1,0) - 2 \cdot (0,1) = (1,-2)$

$948047 = 1 \cdot 530798 + 453249 \Rightarrow x_{453249} = (0,1) - (1,-2) = (1,3)$

$530798 = 1 \cdot 453249 + 77549 \Rightarrow x_{77549} = (1,-2) - (1,3) = (0,-5)$

$453249 = 5 \cdot 77549 + 65354 \Rightarrow x_{65354} = (1,3) - 5 \cdot (0,-5) = (1,28)$

$77549 = 1 \cdot 65354 + 12195 \Rightarrow x_{12195} = (0,-5) - (1,28) = (-1,32)$

$65354 = 5 \cdot 12195 + 4379 \Rightarrow x_{4379} = (1,28) - 5(-1,-32) = (6,188)$

$12195 = 2 \cdot 4379 + 3437 \Rightarrow x_{3437} = (-1,-32) - 2 \cdot (6,188) = (-13,-408)$

$4379 = 1 \cdot 3437 + 942 \Rightarrow x_{942} = (6,188) - (-13,-408) = (19,596)$

$3437 = 3 \cdot 942 + 611 \Rightarrow x_{611} = (-13,-408) - 3 \cdot (19,596) = (-70,-2196)$

$942 = 1 \cdot 611 + 331 \Rightarrow x_{331} = (19,596) - (-70,-2196) = (89,2792)$

$611 = 1 \cdot 311 + 280 \Rightarrow x_{280} = (-70,-2196) - (89,2792) = (-259,$
$-4988)$

$331 = 1 \cdot 280 + 51 \Rightarrow x_{51} = (89,2792) - (-259,-4988) = (348,7780)$

$280 = 5 \cdot 51 + 25 \Rightarrow x_{25} = (-259,-4988) - 5 \cdot (348,7780) = (-1999,-43888)$

$51 = 2 \cdot 25 + 1 \Rightarrow x_1 = (348,7780) - 2 \cdot (-1999,-43888) = (4346,95556)$

$\Rightarrow d = 95556$

$S = m^d \pmod n = 1070777^{95556} \pmod{2430101} = 66406$

4. $p = 21739$

$g = 7$

$a = 15140$

a) Det cheia lui Alice pt criptosist. El Gamal

$\alpha = g^a \pmod p$

$\alpha = 7^{15140} \pmod{21739} = (7^2)^{7570} \pmod{21739} = (49^2)^{3785} =$

$= (2401)^{3785} = 2401 \cdot (2401)^{3784} = 2401\,(5764801)^{1892} =$

$= (2401)(3966)^{1892} = 2401 \cdot (15725156)^{946} = 2401\,(11859)^{94}$

$= (2401)(6290)^{473} = 2401 \cdot 6290\,(6290)^{472}$

$= 2401 \cdot 6290\,(14122)^{236} = 15424 \cdot 14122 \cdot (12469)^{118}$

$= 4356 \cdot 12469\,(20342)^{59} = 10942 \cdot 20342\,(20342)^{28}$

$= 20457 \cdot (20879)^{14} = 20457 \cdot 9035 \cdot (9089)^6 =$

$= 8925 \cdot 9689 \cdot 9689^2 = 18322 \cdot 7719 = 15323$

cheia publică : $(p; g; \alpha) \Rightarrow (21739, 7, 15323)$