**ТЕМА: Protocolul de semnatura “Fara esec”**

**Protocolul de semnatura “Fara esec”** Fie *p* = 2*q*+1 un numar prim cu *q* prim si Z\**p*un element de ordin **,** *q, = 31.**p = 47, q=23* => 47 = 23 \* 2 + 1



Pentru 10*q*  - 1 se defineste = a0 (mod *p*)



0=13, = 3113 (mod 47) = 30



Valorile *p,q,*, sunt publice si considerate fixe.



Valorile 0 este secreta pentru toata lumea (inclusive Bob)



Fie P=Zq, A=Zq x Zq. O cheie este de forma K =(ϒ1, ϒ2,1,2 ,*b1, b2*), unde



1 ,2 ,*b1, b2Zq,*



1= 21,2 = 18,*b1 = 15, b2= 20.*



ϒ1 = a1 \* a2 (mod *p*) = 3121 \* 3018 (mod 47) = 26,



ϒ2 = b1 \* b2 (mod *p*) = 3115 \* 3020 (mod 47) = 44.



ϒ1 ,ϒ2 sunt publice, iar 1 ,2 ,*b1, b2*  sunt secrete.



Bob allege mesajul: x = 13

Daca xZ q se defineste sig*k*(*x*) = (*y1,y2*) unde *y*1 = a1 + xb1 (mod *q*), y2= a2+xb2(mod *q*).



sig*k*(*x*) = (*y1,y2*) unde y1=a1+ x\*b1(mod *q*) = 21+13\*15(mod 23) = 9,

y2 = a2 + x \* b2(mod *q*) = 18+13\*20(mod 23) =2

Pentru y=(y1, y2) Zq x Zq avem *verk (x,y) = T ↔* ϒ1 ,ϒ2 x = y1 y2 (mod *p*)



ϒ1 ,ϒ2x = 26\*4413 (mod 47) =4,

y1 y2 (mod *p*) = 319 \* 302 (mod 47) = 4



Semnatura este valida, deoarece 4=4.