Lënda :Siguri e të dhënave

Kërkesa e detyrës:

1) Duke përdorë kriptosistemin RSA të kryhen

a) Le të jenë n=253 dhe e=31 çelës publik. Enkripto m=10, dhe gjejë p, q dhe d. Pastaj dekripto c=35 ?

b) Le të jenë p=67, q=73 dhe e=89. Enkripto tekstin SIGURI me gjatësi të bllokut 2 ?

Zgjidhje:

a) $c = m^e \ mod \ n$

$c = 10^{31} \ mod \ 253$

***c*=43**

p=11 **q=23**

n=p*q=253

Φ(n)=(p-1)(q-1)=10*22=220

$$e * d \equiv 1(mod\ 220)$$
$$31d \equiv 1(mod\ 220)\ /* 7$$
$$217d \equiv 7(mod\ 220)$$
$$220d - 3d \equiv 7(mod\ 220)$$
$$-3d \equiv 7(mod\ 220)\ /* (-1)$$
$$3d \equiv -7(mod\ 220)$$
$$3d \equiv 213(mod\ 220)/\ 3$$
$$d \equiv 71(mod\ 220)$$

d=71

m=156

(Mënyrë alternative Algoritmi i zgjeruar i Euklidit)

b) Secilës shkronjë I'a asocojmë vlerën në decimale (1-26) meqë RSA funksionon me numra të plotë.

S->19 I->09 G->07 U-> 21 R->18 I->09 n=p*q=4891

Meqë gjatësia e bllokut 2 mesazhet qe do të enkriptohen janë m1=1909, m2=0721, m3=1809.

***c3*=3618**

$c = m^e \ mod \ n$

$c = 1909^{89} \ mod \ 4891$

***c1*=0555**

$c = m^e \ mod \ n$

$c = 0721^{89} \ mod \ 4891$

***c2*=2490**

Mesazhi I enkriptuar:

05 55 24 90 36 18

Punuan: Dafina Sopa

Elvira Jahaj

Elsa Tafilaj