**Criptarea/decriptarea cu RSA**

I.Generarea cheilor:p=31, q=13

p-1 = 30; q -1= 12;

n = p\*q = 31\*13 = 360;

f(n) = (p-1)\*(q-1) = 29\*11 =319; interv 2…317

A alege e = 29; publica

Calculalam ch. Secr. d = e^(-1) mod f(n) = 29^(-1) mod 319 =183;

II.Criptarea

m = 95;

A calculează C=m^e mod n = 95^29 mod 360 =335; 335mod 256=9 (tab oriz)

B calculează C^d mod n= 335^183 mod 360 =.215

**Semnătura RSA**

Generarea cheilor:p=31, q=13

p-1 = 30; q -1= 12;

n = p\*q = 31\*13 = 360;

f(n) = (p-1)\*(q-1) = 29\*11 =319; interv 2…317

A alege e = 25; publica

Calculalam ch. Secr. d = e^(-1) mod f(n) = 25^(-1) mod 319 = 268;

m = 95;

A calculează S=m^d mod n = 95^268 mod 360 = 265; 265mod 256=9 (tab oriz)

B calculează S^e mod n= 265^25 mod 360 = 265.