Algoritmul RSA [Prelegerea 10 rsa]pag.1

1. **I. Генерирование ключей Generarea cheilor**
2. p= 13, q=19 secrete
3. n= p\*q= 13\*19=247--- PUBLICA
4. **Согласно формуле Эйлера**. Aplicam formula lui Euler

Φ(n)= (p-1) (q-1) = 12\*18=216

1. **Выбираем публичный ключ**. Alegem cheia publica (un număr prim)

e ∈ (1, Φ(n)), **e=29** , (2 ; 216) )), **e=29- cheie publica**

1. **Вычисляем секретный ключ**. Calculam cheia secreta d. Aplicam Teorema Mica Fermat

**e \* d mod Φ(n) = 1,**

**d** = **e^(-1) mod(Φ(n)),**

d = **29**^(-1) mod 216 = 149. **d=149.**

1. **Шифрование сообщение m. Criptarea mesajului m-message**

****m = Q[ASCII] = 81, m = 81 n=247

c= 81^29 mod 247 = **139**

139 mod 256 = 139 =>[ASCII]=> “i“

1. **Дешифрование Decriptarea**



139^149 mod 247 = 81=>[ASCII]=> “Q”

Cuvant tehnic TELEFON

P=1331 , Q=3271

e=? prostoe cislo numar prim

d=?

**Электронная подпись RSA. Semnatura digitala cu RSA**

1. **Генерирование ключей Generarea cheilor**
2. p= 13, q=19
3. n= p\*q= 13\*19=247
4. Aplicam formula lui Euler

Φ(n)= (p-1) (q-1) = 12\*18=216

1. Alegem cheia publica

e ∈ (1, Φ(n)), **e=29**

1. Calculam cheia secreta d. Aplicam Teorema Mică Fermat

e \* d mod Φ(n) = 1

d = e^(-1) mod(Φ(n))

d = 29^(-1) mod 216 = **149**

1. **Создание подписи. Crearea Semnaturii**

Fie m– mesaj care trebuie semnat,

m = O[ASCII] = 79 HASH(79)=79. HASH CRC16 (79) =( 22d6)16

Semnatura s = 79 **d** mod n = 79149  mod 247 = 53 =>[ASCII]=> “**5**”

1. **Проверка подписи. Verificarea semnaturii**

VerifS = 53e mod n = 5329 mod 247 = 79 => [ASCII]=> “**O”**

**Подпись верна.** **Semnatura este validă.**