**Lucrare de laborator: Metoda de criptare asimetrica ElGamal**

**Considerente teoretice.**

Descrierea algoritmului de criptare El Gamal Sistemul de criptare El Gamal se bazează pe problema logaritmului discret, care este următoarea:

Fie p număr prim și α, β ∈ Zp, β . Să se determine a ∈ Zp−1 astfel ca α a ≡ β (mod p).

alpha- element primiti pentru p. Beta= α a mod p

Acest ˆîntreg a – dacă exista– este unic și se noteaza logαβ mod(p)=a.

**Notă:** Pentru problema logaritmului discret, nu este obligatoriu ca p să fie număr prim. Important este ca α să fie rădăcină primitivă de ordinul p − 1 a unităt¸ii: ∀i (0 < i < p − 1), αi ≠1 (mod p). Teorema lui Fermat asigură α p−1 ≡ 1 (mod p).

La o alegere convenabilă a lui *p*, problema este NP - complet. Pentru siguranță, *p* se alege de minim 512 bit¸i2 iar *p − 1* să aibă cel puțin un divizor prim ”mare”. Pentru un astfel de modul p, spunem că problema logaritmului discret este dificilă în Zp.

**Descrierea Sistemului de criptare El Gamal**

Fie p număr prim pentru care problema logaritmului discret în Zp este dificilă, și α ∈ Z∗p primitiv.

Fie P= Z∗p , C= Z ∗ p × Z ∗ p și K= {(p, α, a, β)| β ≡ α a (mod p)}.

Valorile p, α, β sunt publice, iar **a** este secret.

Pentru *K = (p, α, a, β)* și k ∈ Zp−1 aleator (secret) se definește eK(x, k) = (y1, y2)

unde y1 = α k (mod p), y2 = x · β k (mod p).

Pentru y1, y2 ∈ Z ∗ p se definește dK(y1, y2) = y2 · (y1 a ) −1 (mod p).

***Indicații:*** 1. Un dezavantaj al sistemului El Gamal constă în dublarea lungimii textului criptat (comparativ cu lungimea textului clar).

2. Indicatția ca pentru criptarea a două texte diferite să se folosească valori diferite ale parametrului k este esențială: astfel, să prsupunem că mesajele m1, m2 au fost criptate în (y1, y2) respectiv (z1, z2) folosind același k. Atunci y2/z2 = m1/m2 și cunoașterea unuia din mesaje îl determină imediat pe celălalt.

**Mersul lucrării**

Fie date valorile p=67- numar prim.

Elementul primitive al acestui numar prim 7. (primitive root of 67 =7 in volfram alpha)

Se allege un numar secret a=5.

Aplicati algorimul asimetric ElGamal pentru:

a)Criptatarea unui mesaj scurt,

b)Decriptati mesajul ales.

c)Semnați acest mesaj cu cheile generate la punctul a).

d)Verificați semnătura.

**Lucrarea se efectează după urmatorul model:**

**Generarea cheilor**:

Fie p = 67 un numar prim (pentru care problema logaritmilor discreti in Zᵨ este dificila) si αZp\*=Zp\{0},

7 un element primitive. Se ia:

P=Zp\*, A=Zp\*xZp-1, K={(p,)}. logαβ mod(p)=a.

Valorile p, sunt publice, iar a este secret.

a = 5.

=

**Criptare:**

Se ia mesajul x = B –ASCII> 66. H (Bit)= AdlerHASH = (020f0120)16=( 34537760 )10  H(x)= 34537760

Pentru K = (p,), k = 17 (secret) se defineste:

Criptul este acelasi cu semnatura sigK(x,k) = (), unde

⁻¹(mod p - 1). ⁻¹(mod p - 1). 34537760⁻¹(mod p - 1).

𝜸 = 717 mod 67 **= 44.**

= (66-5\*44)17⁻¹ mod 66=-154\*35 mod 66=-5390 mod 66= 66 - (5390 mod 66)= **22**

**Criptul si sigK(66,17)= (44,22) (coincid)**

**Descriptare:** (\*-operatia de inmultire)

Pentru 𝜸,δ se defineste: dK(𝜸,δ) = δ \* (𝜸ᵅ)ˉ¹ mod p

dK(𝜸,δ) = 22 \*(445)ˉ¹ mod 67 = 66 –ASCII > B

**Semnătura:**

= 717 mod 67 = 44.

⁻¹(mod p - 1) = (66-5\*44)\*17-1(mod 66) = - 154 \* 35 mod 66 = 22

**Verificarea Semnăturii:**

Pentru a verifica semnătura, calculăm:

verK(x,) = T <=> mod p

mod p = 57444422 mod 67 = 29 \* 37 mod 67 = 1.

αᵡ mod p = 766 mod 67 = 1. 1=1 rezulta ca

Semnătura este deci validă.

**Concluzie:**

Conform algoritmului El Gamal am obținut la decriptare mesajul ales în text clar.

Semnătura creată în baza algoritmului El Gamal utilizând cheile generate la criptare, este validă.

**Referințe:**

Prelegerea 12 Elgamal. (Din conspect).

Lucrarea: model criptare(semnare)/decriptare-verificarea semnaturii cu algoritmul ElGamal

**Limbajul de programarela alegere**