Semnatura El Gamal

Exemplu 1:

Schema de semnatura ElGamal

•A genereaza nr. Prim p = 1013 si genaratorul a = 2 al gr. Z\*1013.

•A allege cheia a = 1009 si calculeaza y=a^a mod p=2^1009 mod 1013= 380.

•Cheia piblica a lui A este (p=1013, a=2, y=380), iar cheia sa private este a = 1009.

•Pt. a semna mesajul m=1033, A select. Aleator un intreg k=1051,

•Calc. r=a^k mod p=2^1051 mod 1013=736 si k^-1 mod (p-1)=421.

•A calculeaza S=421\*(1033-1009\*736) mod 1012=285.

Semnatura mesajului m=1033 este perechea (r=1490, s=285).

•Pentru verificarea semnaturii, B calculeaza v1=380^736\*736^285 mod 1013=854. H (m) =1033 si v2=2^1033 mod 1013=242.

•Entitatea B nu accepta semnatura deoarece v1!=v2.

Exemplu 2:

Fie p = 67 un numar prim (pentru care problema logaritmilor discreti in Zᵨ este dificila) si αZp\*=Zp\{0}, 11 un element primitive. Se ia:

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

Valorile p, sunt publice, iar a este secret.

a = 13.

=

|  |  |  |
| --- | --- | --- |
| I i | Ci ci | z |
| 3 3 | 1 | 1^2 mod 67 = 1 x 11 mod 67 = 11 |
| 2 2 | 0 1 | 11^2 mod 67 = 54 x 11 mod 67 = 58 |
| 1 1 | 1 0 | 58^2 mod 67 = 14 |
| 0 0 | 1 1 | 2 14^2 mod 67 = 62 x 11 mod 67 = 12 |
|  |  | 11^13 mod 67 = 12 |

Criptare:

Se ia mesajul x = A –ASCII> 65.

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

CRIPT,sigK(x,k) = (), unde

⁻¹(mod p - 1).

𝜸 = 11^17 mod 67 = 18.

|  |  |  |
| --- | --- | --- |
| i | ci | z |
| 3 | 1 1 | 1^2 mod 67 = 1 x 11 mod 67 = 11 |
| 2 | 0 0 | 11^2 mod 67 = 54 |
| 1 | 1 0 | 54^2 mod 67 = 35 |
|  | 0 | 35^2 mod 67 = 19 |
| 0 | 1 1 | 19^2 mod 67 = 26 x 11 mod 67 = 18 |
|  |  | 11^17 mod 67 = 18 |

= (65-13\*18)\*17⁻¹ mod 66=-169\*35 mod 66=-5915 mod 66= 66 - (5915 mod 66)= 25

sigK(65,17)= (18,25)

Verificare:

Pentru a verifica semnatura, calculam:

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

mod p

mod p = 12^18\*18^25 mod 67 = 61 mod 67 = 61.

αᵡ mod p = 11^65 mod 67 = 61.

Semnatura este deci valabila.

Descriptare:

Pentru 𝜸,δ se defineste:

dK(𝜸,δ) = δ \* (𝜸ᵅ)ˉ¹ mod p

dK(𝜸,δ) = 25 \* (18^13)ˉ¹ mod 67 = 65 –ASCII> A