Elgamal cryptography

1.ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography .

2. It was described by Taher Elgamal in 1985.

3. Its security depends upon the difficulty of a certain problem in related to computing discrete logarithms.

4. ElGamal encryption consists of three components:

(i) key generator

(ii) Encryption algorithm

(iii) Decryption algorithm.

1. **Key generator:-**
   - (i) Select large prime no(P)
   - (ii) Select decryption key/private key(D)
   - (iii) Select second part of encryption key or public key(E1)
   - (iv) Third part of encryption key or public key(E2) E2=E1 ^ D mod 11
   - (v) Public key (E1,E2,P),private key D

2. **Encryption:-**
   - **(i)** Select random integer(R)
   - **(ii)** $C1=E1^{R} \bmod P$
   - **(iii)** C2=(P.T. * E2 ^R) mod P

(iv) C.T.=(C1,C2)

3. **Decryption:-**

(i) **P.T=[C2*(C1 ^D) ^ -1] mod P**

Example:

1. **Key generator:-**

(i) Select large prime no(P) P=11

(ii) Select decryption key/private key(D) D=3

(iii) Select second part of encryption key or public key(E1) E1=2

(iv) Third part of encryption key or public key(E2)

E2=E1 ^ D mod 11

E2=(2) ^ 3 mod 11=8

E2=8

(v) Public key (E1,E2,P),private key D

=(2,8,11), D=3

2. **Encryption:-**

(i) Select random integer(R): R=4

(ii) $C1=E1^{R} \bmod P$

C1=2 ^ 4 mod 11=5

C1=5

(iii) C2=(P.T. * E2 ^R) mod P

Let P.T.=7

C2=(7*(8) ^ 4) mod 11

C2=6

(iv) C.T.=(C1,C2)

C.T=(5,6)

3. Decryption:

(i) P.T=[C2*(C1 ^D) ^ -1] mod P

P.T.=[6*((5^3)^-1)] mod 11

P.T.=(5^3)^-1 mod 11

P.T=(125) ^-1 mod 11

P.T.=(125*x) mod 11=1

P.T.=375 mod 11=1 (x=3)

P.T.=(6*3) mod 11

P.T.=18 mod 11

P.T=7

So the original P.T.=7 then C.T=(5,6) then after again recovered P.T.=7

7------→(5,6)-------→7

P.T C.T. P.T.

SECURITY OF ELGAMAL:-

Recall the two different strategies for trying to “break” RSA:

1. Trying to decrypt a ciphertext without knowledge of the private key

2. Trying to determine the private key.