ELGAMAL CRYPTOSYSTEM

- Elagamal cryptosystem is based on the discrete logarithm problem.

- Let p be a very large prime number, e_1 is a primitive root in group $G = < Zp^* ,\times >$ and d is an integer, then it's easy to compute $e_2 = e_1^{\,d} \bmod p$

- Given e_1 ,e_2 , p it's computationally infeasible to calculate $d= \log_{e1} e_2 \bmod p$.

KEY GENERATION

Algorithm 10.9 *ElGamal key generation*

ElGamal_Key_Generation

{

Select a large prime p

Select d to be a member of the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$ such that $1 \leq d \leq p - 2$

Select e_1 to be a primitive root in the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$

$e_2 \leftarrow e_1^{\,d} \bmod p$

Public_key $\leftarrow (e_1, e_2, p)$ // To be announced publicly

Private_key $\leftarrow d$ // To be kept secret

return Public_key and Private_key

}

ENCRYPTION

Algorithm 10.10 *ElGamal encryption*

ElGamal_Encryption (e_1, e_2, p, P) // P is the plaintext

{

Select a random integer r in the group $\mathbf{G} = < \mathbf{Z}_p{}^*, \times >$

$C_1 \leftarrow e_1{}^r \bmod p$

$C_2 \leftarrow (P \times e_2{}^r) \bmod p$ // C_1 and C_2 are the ciphertexts

return C_1 and C_2

}

DECRYPTION

Algorithm 10.11 *ElGamal decryption*

```
ElGamal_Decryption (d, p, C1, C2)                    // C1 and C2 are the ciphertexts
{
    P ← [C2 (C1^d) ^-1] mod p                        // P is the plaintext
    return P
}
```

- *Example :Bob chooses p = 11 and e_1 = 2 and d = 3 $e_2 = e_1^d$ = 8. So the public keys are (2, 8, 11) and the private key is 3. Alice chooses r = 4 and calculates C1 and C2 for the plaintext 7.*

Plaintext: 7

$C_1 = e_1^{\,r} \bmod 11 = 16 \bmod 11 = 5 \bmod 11$

$C_2 = (P \times e_2^{\,r}) \bmod 11 = (7 \times 4096) \bmod 11 = 6 \bmod 11$

Ciphertext: (5, 6)

$[C_2 \times (C_1^{\,d})^{-1}] \bmod 11 = 6 \times (5^3)^{-1} \bmod 11 = 6 \times 3 \bmod 11 = 7 \bmod 11$

Plaintext: 7

SECURITY OF ELGAMAL

- **Low modulus attack**: if p is small, can solve the discrete log to find d or r.
- $d = \log_{e1} e2 \bmod p$
- $r = \log_{e1} C_1 \bmod p$

- **Known Plain text attack**:If using the same r for P and P', the intruder can discover P' if P is known. Assume that $C_2 = P \times (e_2^r) \bmod p$ and $C2' = P' \times (e_2^r) \bmod p$ then he can find P' as
- $(e_2^r) = C_2 \times P^{-1} \bmod p$
- $P' = C_2' \times (e_2^r)^{-1} \bmod p$

- For the security of Elgamal system p must be atleast 300 digits and r must be new for each encipherment.