NAME- RAM CHANDRA JANGIR
ROLL NO. - CS21M517
Subject - CS6530 - Assignment-4.

Elgamal Algorithm

(i) Introduction
(ii) Key generation
(iii) Encryption
(iv) Decryption

(i) Introduction:

The Elgamal encryption algorithm is an asymmetric key encryption algorithm for public-key cryptography, which is based on the Diffie-Hellman key exchange. It can be defined over any cyclic group G. It's security depends upon the difficulty of a certain problem in G related to computing discrete algorithm.

(ii) Key Generation :

(A) select a large prime p, it will be the first part of Enc. key.

(b) select d to be a member of the group $G = < Z_p^*, x >$ such that $1 \leq d \leq p-2$

(c) select the second part of our encryption key i.e. E1

(d) compute the third part of our encryption key i.e. E2

$e_2 \leftarrow e_1^d \bmod p$

Now Public key $\leftarrow (e_1, e_2, p)$

Private key $\leftarrow d$

(iii) Elgamal Encryption:

(a) select a random integer R

(b) First part of the encryption is:

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

(c) Second part of the encryption is:

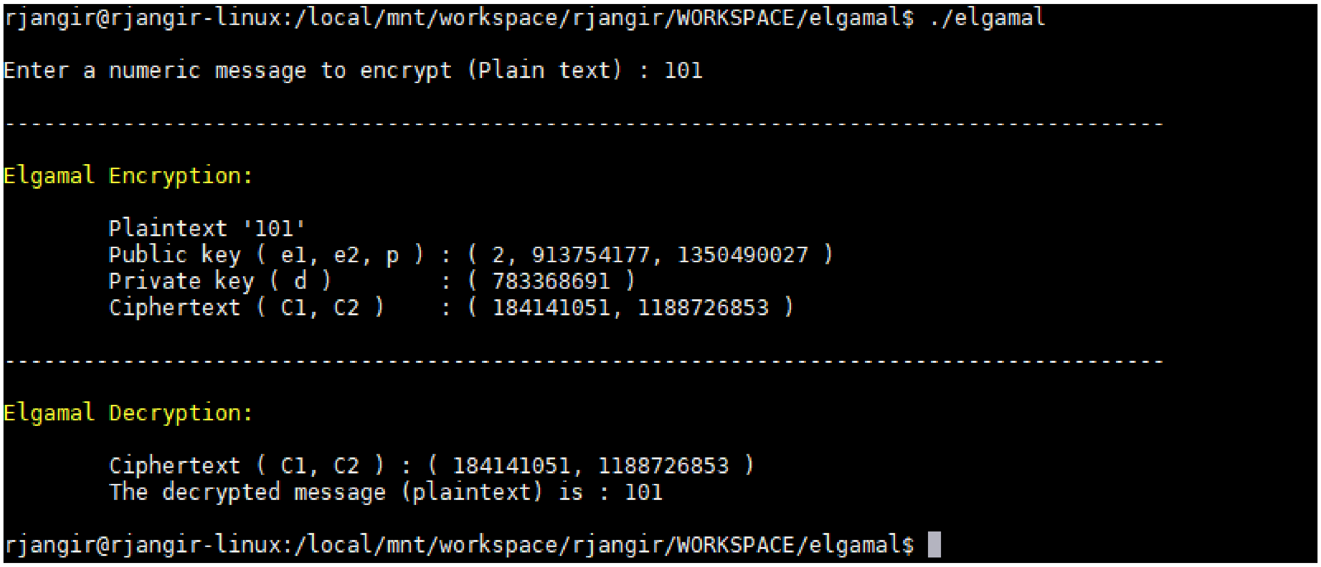
$$C2 \leftarrow (P \times e_2^{r}) \bmod p$$ where P is plaintext

(d) Final ciphertext is (C1, C2)

(iv) Elgamal Decryption:

$$\text{Plaintext} = C2 \cdot C1 \wedge (D-1) \bmod p$$

My Elgamal algorithm Program Output:



```
rjangir@rjangir-linux:/local/mnt/workspace/rjangir/WORKSPACE/elgamal$ ./elgamal

Enter a numeric message to encrypt (Plain text) : 101

----------------------------------------------------------------------------------------

Elgamal Encryption:

        Plaintext '101'
        Public key ( e1, e2, p ) : ( 2, 913754177, 1350490027 )
        Private key ( d )        : ( 783368691 )
        Ciphertext ( C1, C2 )    : ( 184141051, 1188726853 )

----------------------------------------------------------------------------------------

Elgamal Decryption:

        Ciphertext ( C1, C2 ) : ( 184141051, 1188726853 )
        The decrypted message (plaintext) is : 101

rjangir@rjangir-linux:/local/mnt/workspace/rjangir/WORKSPACE/elgamal$
```