IIT MADRAS

Indian Institute of Technology Madras

M.Tech Computer Science Information security.

Cryptography Basic.(CS6530)

Assignment-4. (C language Program for implementation of ElGamal algorithm for encryption and decryption.)

Roll Number - CS21M515

Name – Ayub Shaikh.

Batch Year-2021

Faculty : Honorable Pandu Rangan Sir

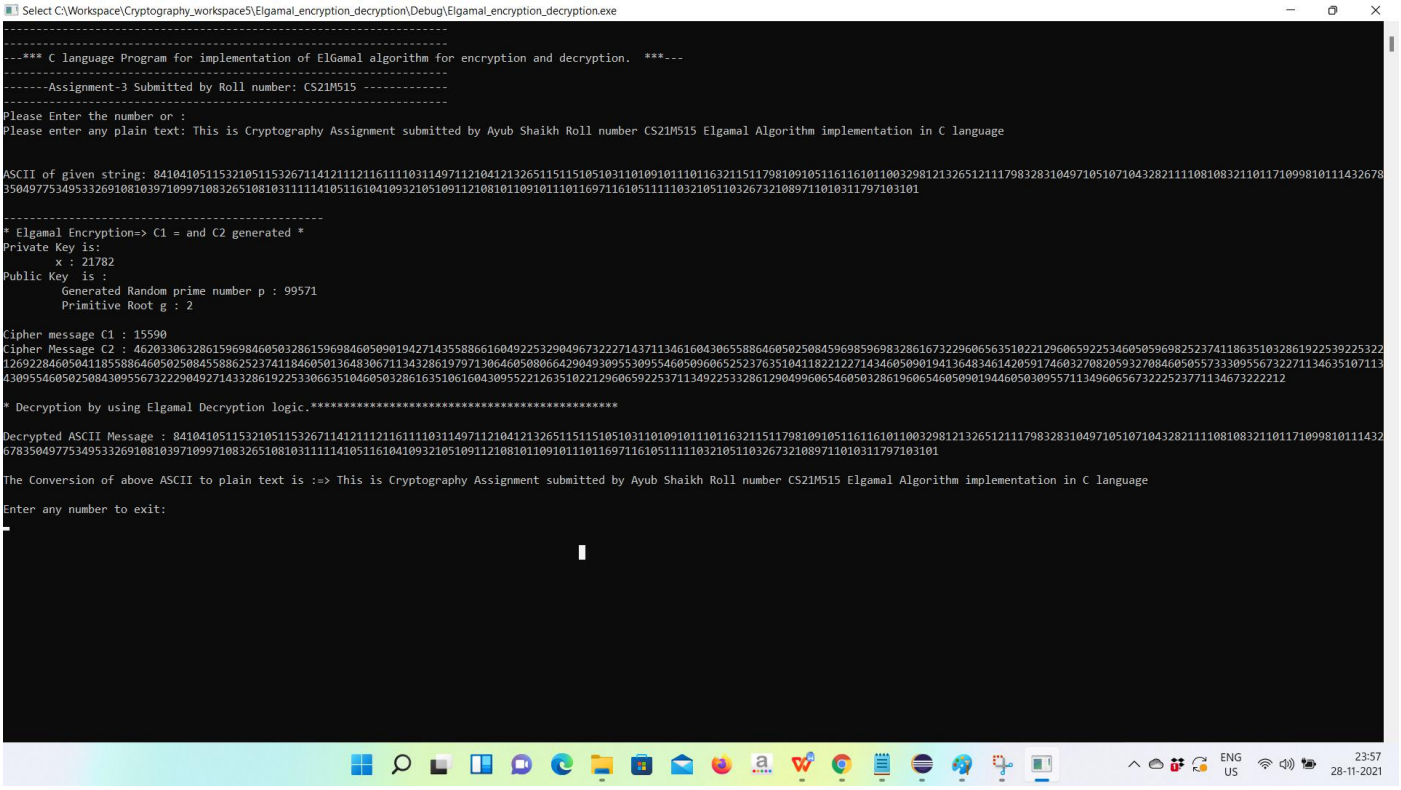
TA : Honorable Venkatakrishnan Sutharsan Sir

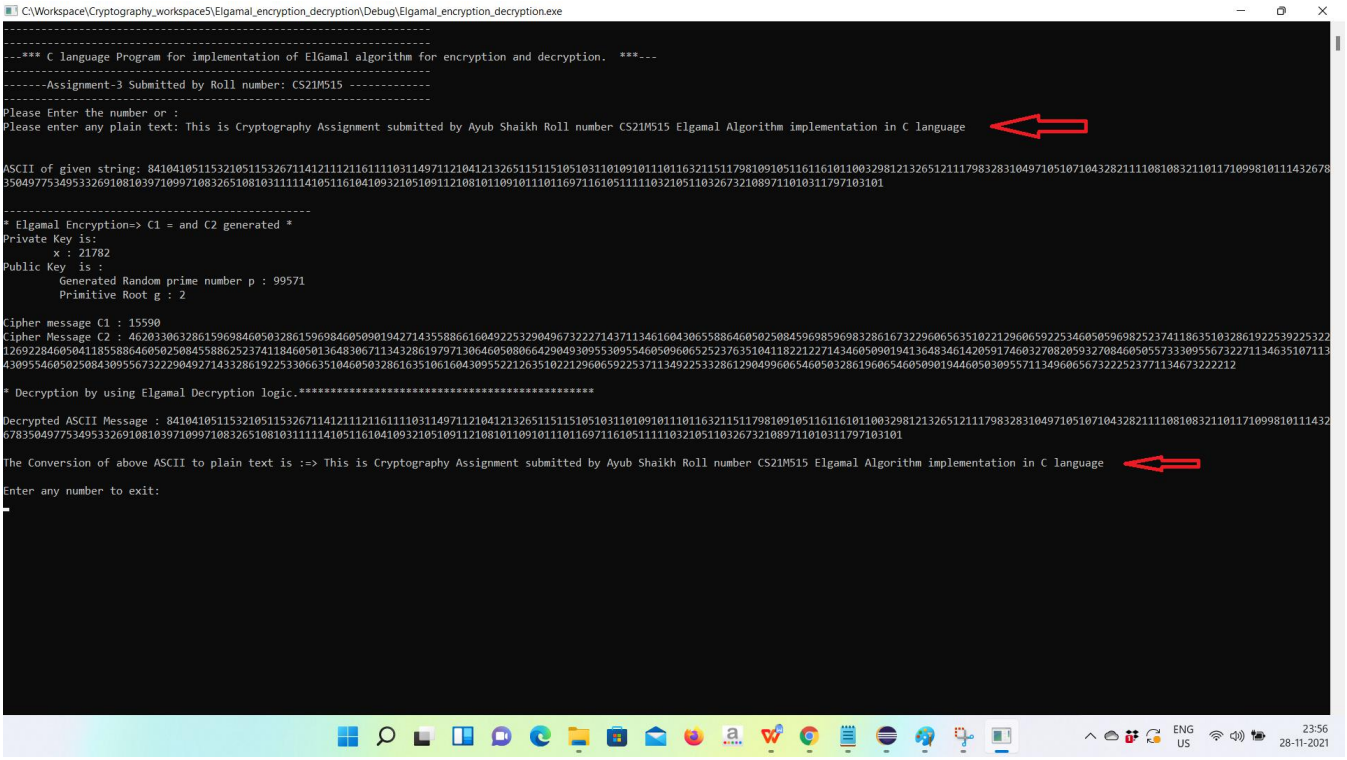
Program Solution and Explanations:-

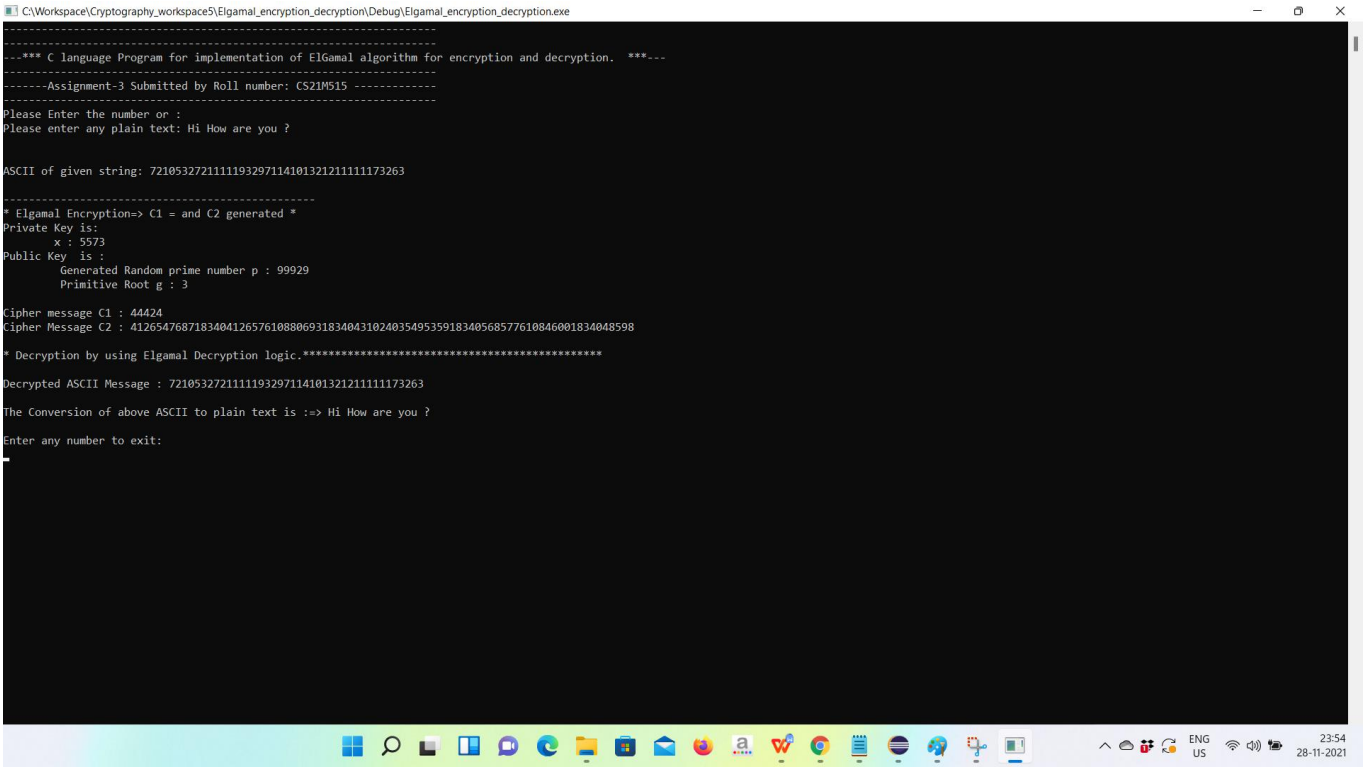
I Have did the above example by using the C program.

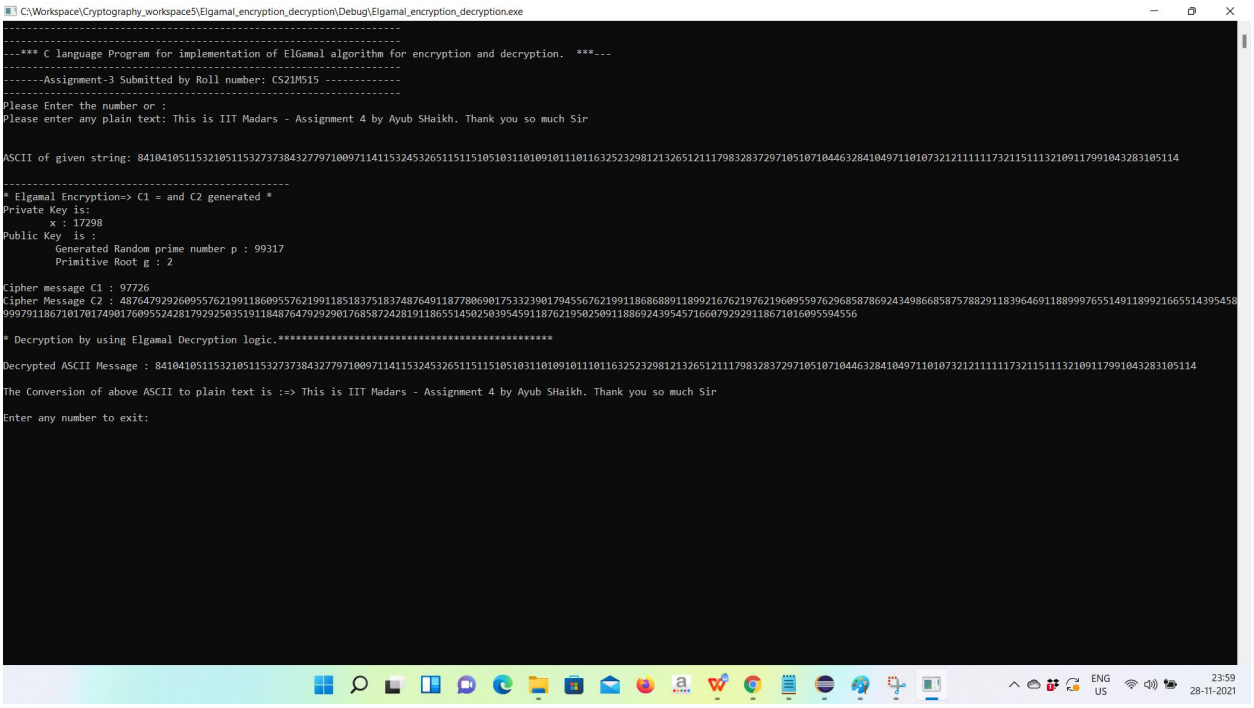
And .exe is shared in the Github and also the program is shared.

Below are the screen shots of the C programm executed .




C:\Workspace\Cryptography_workspace5\Elgamal_encryption_decryption\Debug\Elgamal_encryption_decryption.exe
---*** C language Program for implementation of ElGamal algorithm for encryption and decryption. ***---
-------Assignment-3 Submitted by Roll number: CS21M515 ------------
Please Enter the number or :
Please enter any plain text: This is Cryptography Assignment submitted by Ayub Shaikh Roll number CS21M515 Elgamal Algorithm implementation in C language
ASCII of given string: 84104105115321051153267114121112116111031149711210412132651151151051031101091011101163211511798109105116116101100329812132651211179832831049710510710432821111081083211017109981011143267835049775349533269108103971099710832651081031111141051161041093210510911210810110910111011697116105111103210511032673210897110103117971031
* Elgamal Encryption=> C1 = and C2 generated *
Private Key is:
x : 21782
Public Key is :
Generated Random prime number p : 99571
Primitive Root g : 2
Cipher message C1 : 15590
Cipher Message C2 : 46203306328615969846050328615969846050901942714355886616049225329049673222714371134616043065588646050250845969859698328616732296065635102212960659225346050596982523741186351032861922539225322126922846050411855886460502508455886252374118460501364830671134328619797130646050806642904930955309554605096065252376351041182212271434605090194136483461420591746032708205932708460505573330955673227113463510711343095546050250843095567322290492714332861922533066351046050328616351061604309552212635102212960659225371134922533286129049960654605032861960654605090194460503095571134960656732225237711346732222 12
* Decryption by using Elgamal Decryption logic.**********
Decrypted ASCII Message : 84104105115321051153267114121112116111103114971121041213265115115105103110109101110116321151179810910511611610110032981213265121117983283104971051071043282111108108321101171099810111432678350497753495332691081039710997108326510810311111410511610410932105109112108101109101110116971161051111103210511032673210897110103117971031
The Conversion of above ASCII to plain text is :=> This is Cryptography Assignment submitted by Ayub Shaikh Roll number CS21M515 Elgamal Algorithm implementation in C language
Enter any number to exit:
ENG
US
23:56
28-11-2021


C:\Workspace\Cryptography_workspace5\Elgamal_encryption_decryption\Debug\Elgamal_encryption_decryption.exe
---*** C language Program for implementation of ElGamal algorithm for encryption and decryption. ***---
-------Assignment-3 Submitted by Roll number: CS21M515 ------------
Please Enter the number or :
Please enter any plain text: Hi How are you ?
ASCII of given string: 721053272111119329711410132121111173263
* Elgamal Encryption=> C1 = and C2 generated *
Private Key is:
x : 5573
Public Key is :
Generated Random prime number p : 99929
Primitive Root g : 3
Cipher message C1 : 44424
Cipher Message C2 : 41265476871834041265761088069318340431024035495359183405685776108460018340485 98
* Decryption by using Elgamal Decryption logic.**********
Decrypted ASCII Message : 721053272111119329711410132121111173263
The Conversion of above ASCII to plain text is :=> Hi How are you ?
Enter any number to exit:
ENG
US
23:54
28-11-2021



ElGamal algorithm for encryption and decryption Explanations and Program Logical Steps Explanations :-

Key- Generation Algorithm:

Let A be a person creates key:

1. Select large number p and large number g.

   p is prime,

   g is generator.

2. Selects random x in Z^*_p

3. $y = g^x \bmod p$.

$(p, g, y) \longrightarrow$ (public key)

$x \longrightarrow$ (secret / private key)

Finding x for given p, g, y is computationally infeasible as of now.

(where x can not be 1 or $p-1$)

a) a dozen croissants?

Encryption under k :

1) Choose a random r $1 < r < (p-1)$

2) $C_1 = g^r \bmod p$

3) $C_2 = m \cdot y^r \bmod p$. (m is message $m < p$)

(See it is $(g^x \bmod p)^r \bmod p$ that $(g^{xr}) \bmod p$)

p is 1024 bits

m is 1023 bits

C_1 , C_2 are Cipher text.

[For RSA, the relation between c and m are fixed but for Elgamal, c and m are not fixed]

Decryption :

$(C_1\ C_2 \quad (P, g, y), \quad x)$

↑ Private Key.

using this decrypting $c_1 = g^r \bmod P$,

$c_2 = m y^r \bmod p$ is impossible for Decryptor/ owner of the key too.

So other way is (all are mod P)

$$y^r = g^{xr} = (g^r)^x = C_1^{\ x}$$

So Decrypting C_1

① compute $C_1^{\ x} \bmod P$

② compute $m = \dfrac{C_2}{C_1^{\ x}}$

$$m = C_2 (C_1^{\ x})^{-1} \bmod P$$

By Eudid Extended Algorithm.

we can find m.

Program Logical Steps:-

```
 * *
 *  Program Logic
 *  1) Take large prime numbers p and g (g <p, g is preferably the prime root of p)

Note: If g is a prime root of the prime number p, then g mod p, g^2 mod p, …, g^p-1
mod p are permutations from 1 to p-1

2) Randomly select an integer x (2 <= x <= (p-2), (p, g, x) is the private key)

3) Calculate y = g^x (mod p) ((p, g, y) is the public key)



2. Encryption process

1) Randomly select an integer k (2 <= k <= (p-2) and k and (p-1) are relatively prime)

2) Calculate a = g^k mod p, b = m*y^k mod p (m is the plaintext to be encrypted)

3) Ciphertext C = (a, b)



3. Decryption process

1. m = b * a^(-x) mod p

Note: b * a^(-x) mod p = m * y^k * g^(-xk) = m * g^(xk) * g^(-xk) = m
```

THANK You Sir …. ☺☺☺