Name: Sohel Momin

Roll No:1513126/a4

CSS EXPERIMENT 9

**Program:**

**%% Elgamal Cryptosystem**

% checkPrime.m, modexpo.m should be in the same folder !!!

clc;clear variables;close all;

**%% Getting Valid prime p larger than 127 (max ASCII) eg 131,137,139 ..etc**

p = -1;

while (p == -1)

temp = input('Enter a distinct prime no. p');

if checkPrime(temp) && temp>127

p = temp;

end

end

phi = p-1;

**%% Getting Valid d**

d = randperm(p-2,1);

**%% Getting Valid e1 (smallest valid)**

for i=2:phi-1

for j=2:phi

k = modexpo(i,j,p);

if k==1 && j~=phi

break

end

end

if k==1 && j==phi

e1 = i;

break

end

end

**%% Getting e2**

e2 = modexpo(e1,d,p);

**%% Getting plaintext**

P = double(input('Enter the message to be encrypted by 2nd party -> ','s'));

**%% Elgamal Encryption using public key (e1,e2,p)**

r = randperm(phi,1);

C1 = modexpo(e1,r,p);

C2 = mod(P\*modexpo(e2,r,p),p);

**%% Elgamal Decryption using private key (d)**

D = mod(C2\*modexpo(C1,phi-d,p),p);

fprintf('The message decrypted is -> %s \n',char(D));

**OUTPUT :**

Enter a distinct prime no. p

137

Enter the message to be encrypted by 2nd party ->

The quick brown fox jumps over lazy dog

The message decrypted is -> The quick brown fox jumps over lazy dog