NAME - RAM CHANDRA JANGIR

ROLL NO - CS21M517

Subject - CS6530 Assignment - 5

Elgamal in Elliptic curve cryptography.

(i) Introduction-

(ii) What is elliptic curve cryptography used for

(iii) How ECC works

(iv) Elgamal ECC program output

(i) Introduction

Elliptic curve cryptography (ECC) is a key based ~~tec~~ technique for encrypting data. ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.

It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.

The elliptic curve equation is $y^2 = x^3 + ax + b$

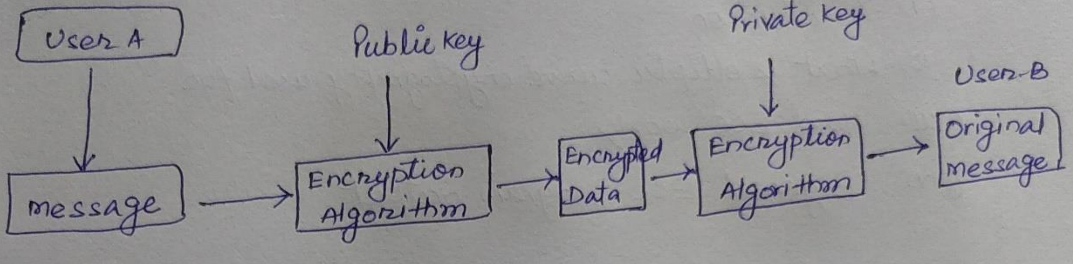
(ii) What is elliptic curve cryptography used for:

A common use of ECC is to encrypt data so that only authorized parties can decrypt it. This has several obvious use cases, but is most commonly used to encrypt internet traffic.

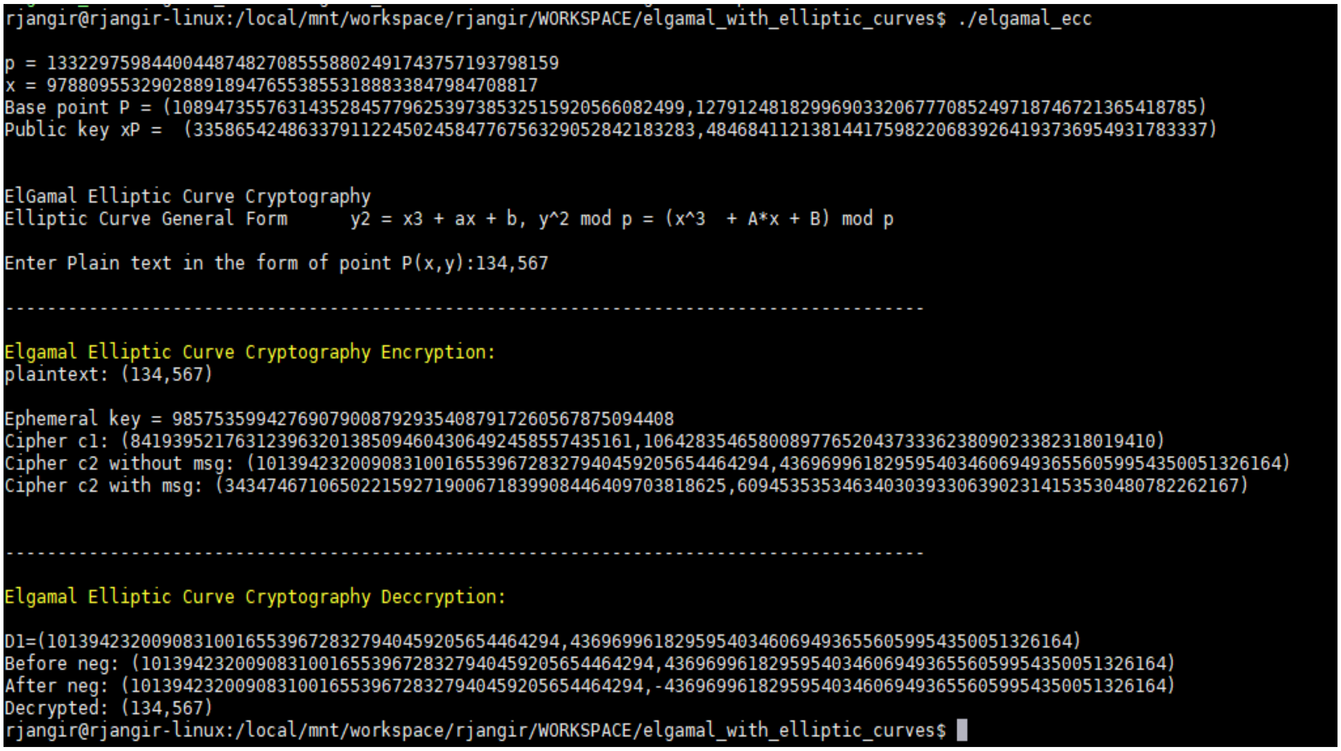
(iii) How ECC works -

We create two keys, a public key and a private key. The public key is given freely, and any party can encrypt data by using it.

However the private key is kept secret and only those who hold it will have the ability to decrypt the data.



(iv) ElGamal Elliptic Curve Cryptography Program Output:



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

p = 1332297598440044874827085558802491743757193798159
x = 97880955329028891894765538553188833847984708817
Base point P = (1089473557631435284577962539738532515920566082499,127912481829969033206777085249718746721365418785)
Public key xP =  (335865424863379112245024584776756329052842183283,484684112138144175982206839264193736954931783337)


ElGamal Elliptic Curve Cryptography
Elliptic Curve General Form      y2 = x3 + ax + b, y^2 mod p = (x^3  + A*x + B) mod p

Enter Plain text in the form of point P(x,y):134,567

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

Elgamal Elliptic Curve Cryptography Encryption:
plaintext: (134,567)

Ephemeral key = 985753599427690790087929354087917260567875094408
Cipher c1: (841939521763123963201385094604306492458557435161,1064283546580089776520437333623809023382318019410)
Cipher c2 without msg: (1013942320090831001655396728327940459205654464294,436969961829595403460694936556059954350051326164)
Cipher c2 with msg: (343474671065022159271900671839908446409703818625,609453535346340303933063902314153530480782262167)


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

Elgamal Elliptic Curve Cryptography Deccryption:

D1=(1013942320090831001655396728327940459205654464294,436969961829595403460694936556059954350051326164)
Before neg: (1013942320090831001655396728327940459205654464294,436969961829595403460694936556059954350051326164)
After neg: (1013942320090831001655396728327940459205654464294,-436969961829595403460694936556059954350051326164)
Decrypted: (134,567)
rjangir@rjangir-linux:/local/mnt/workspace/rjangir/WORKSPACE/elgamal_with_elliptic_curves$ 
```