Assignment no ICS 2

Roll no 41239

Title: Implementation of ECC algorithm.

Problem Definition: Implementation of ECC Algorithm

Software Requirements:

Python 3.7,Colab

Hardware Requirement:

8GB RAM, 500 GB HDD,Keyboard,Mouse

Learning Objectives:
Learn ECCAlgorithm

Outcomes:
After completion of this assignment students are able to understand the How to encrypt and decrypt message using ECC.

Theory :

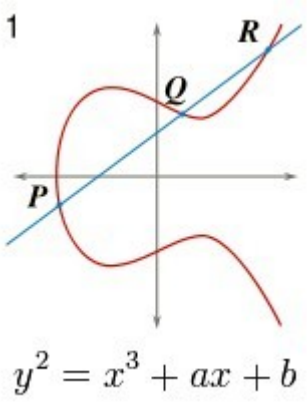
1.The equation of an elliptic curve is given as,

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)



2. Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number 'd' within the range of 'n'.

Using the following equation, we can generate the public key

$Q = d * P$

d= The random number that we have selected within the range of (1 to n-1).P is the point on the curve.

'Q' is the public key nd 'd' is the private key.

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve.

Consider'm' as the point 'M' on the curve E'.Randomly select 'k' from [1 – (n-1)].

Two cipher texts will be generated let it be C1 and C2

$C1 = k*P$

$C2 = M + k*Q$

C1 and C2 will be send.

Decryption

We have to get back the message 'm' that was send to us,

$M = C2 – d * C1$

M is the original message that we have send.

Conclusion:

Thus ECC is used for key generation as well as for encryption and decryption.