-ASSIGNMENT NO	I&CS 5
TITLE	Implementation of ECC
PROBLEM STATEMENT/ DEFINITION	Implementation of ECC
OBJECTIVE	To understand how ECC works
OUTCOME	Understanding and implementation of ECC algorithm
S/W PACKAGES AND HARDWARE APPARATUS USED	Core 2 DUO/i3/i5/i7 64-bit processor OS-LINUX 64-bit OS Editor-gedit/Eclipse S/W- C++/JAVA//Python
REFERENCES	1. Bernard Menezes, "Network Security and Cryptography", Cengage Learning India, 2014, ISBN No.: 8131513491 2. Nina Godbole, Sunit Belapure, "Cyber Security", Wiley India, 2014, ISBN No.: 978-81-345-2179-1 3. Atul Kahate, "Cryptography and Network Security", Mc Graw Hill Publication, 2nd Edition, 2008, ISBN: 978-0-07-064823- 4. William Stallings, "Cryptography and network security Principles and practices", Pearson, 6th Edition, ISBN: 978-93-325-1877-3 5. Forouzan, "Cryptography and Network Security (SIE)", Mc Graw Hill, ISBN 007070208X, 9780070702080
STEPS	1. Input n 2. Select d in the range of n 3. **Key generation** compute Q using Q = d*p 4. **Encryption** 1. Input message m 2. Select k in [1- n-1] 3. Compute C1= k*P and C2 = M + k*Q 5. **Decryption** 1. Compute M = C2 – d * C1
INSTRUCTIONS FOR WRITING JOURNAL	1. Date 2. Assignment No. 3. Problem Definition

	4. Learning Objective 5. Learning Outcome 6. Concepts Related Theory 7. Algorithm 8. Test Cases 9. Conclusion/Analysis

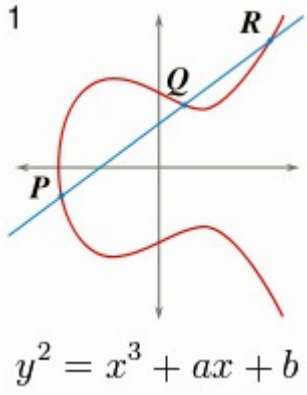
Pr-requisites: Number theory, Discrete mathematics and any programming language C++/Java/Python.

Concepts Related Theory:
The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,

E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number)



The figure shows a simple elliptic curve.

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’.R*andomly 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.