Centurion University
Shaping Lives... Empowering Communities...

School: ..... Campus: .....

Academic Year: ..... Subject Name: ..... Subject Code: .....

Semester: ..... Program: ..... Branch: ..... Specialization: .....

Date: .....

Applied and Action Learning

(Learning by Doing and Discovery)

Name of the Experiement : ECDSA workshop – Digital Signature Demo

Coding Phase: Pseudo Code / Flow Chart / Algorithm :

1. Start
2. Import the ECDSA library or open an online digital signature tool
3. Generate a private key (used to sign the message)
4. Derive the public key from the private key
5. Enter or create a message (e.g., “Hello Blockchain”)
6. Use the private key to sign the message and produce a digital signature
7. Use the public key to verify the signature
8. Display whether the signature is valid or invalid
9. End

Apparatus/Software Used:

Computer System / Laptop

ECDSA Library

Operating System: Windows / Linux / macOS

Internet Browser

Theory/Concept:

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic algorithm used to ensure data integrity and authentication in blockchain systems.

It is based on elliptic curve cryptography (ECC), which provides strong security using smaller key sizes compared to traditional algorithms like RSA.

In ECDSA:

A private key is used to sign a message, creating a unique digital signature.

A corresponding public key is used to verify that signature.

If the message or signature is altered, verification will fail — ensuring that the message has not been tampered with.

Procedure:

1. Start the system and open the Python IDE (or any online ECDSA demo tool).
2. Import the ECDSA library into your Python program.
3. Generate a private key using the SECP256k1 elliptic curve.
4. Derive the corresponding public key from the private key.
5. Enter or define a message (e.g., “Hello Blockchain”).
6. Use the private key to sign the message and produce a digital signature.
7. Use the public key to verify the signature.
8. Observe whether the verification output shows “Signature Verified Successfully.”
9. Record the results in the observation table.
10. End the process.

Observation:

In this experiment, we successfully demonstrated the ECDSA digital signature process, showing how a message can be securely signed and verified using elliptic curve cryptography.

ASSESSMENT

Rubrics	Full Mark	Marks Obtained	Remarks
Concept	10		
Planning and Execution/ Practical Simulation/ Programming	10		
Result and Interpretation	10		
Record of Applied and Action Learning	10		
Viva	10		
Total	**50**		

Signature of the Student:

Name :

Regn. No. :

Signature of the Faculty:

**As applicable according to the experiment. Two sheets per experiment (10-20) to be used.*