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

Objective/Aim:

To understand and demonstrate the Elliptic Curve Digital Signature Algorithm (ECDSA) used in blockchain networks like Ethereum for securing transactions and verifying identity.

Apparatus/Software Used:

- Ethereum Development Environment (e.g., Remix IDE or local testnet)
- MetaMask or other Ethereum wallet
- Node.js or web3.js library for signing and verifying messages
- Sample private and public keys for demonstration

Theory/Concept:

ECDSA is a cryptographic algorithm that enables the creation of digital signatures using elliptic curve cryptography. It is fundamental to blockchain security, allowing users to sign transactions or messages with their private keys and enabling others to verify the authenticity and integrity of these signatures with the corresponding public keys. ECDSA ensures non-repudiation and prevents forgery, forming the backbone of identity verification and transaction authenticity on Ethereum and many other blockchains.

When a transaction is signed, the signature proves that the transaction was authorized by the owner of the wallet's private key, without exposing the private key itself. This signature is included in the transaction data on the blockchain, where nodes validate it before execution, ensuring decentralized trust and security.

Procedure:

- Generate a private-public key pair or use existing Ethereum wallet keys.
- Use a cryptographic library or web3.js to sign a sample message or transaction data with the private key.
- Obtain the digital signature (r, s, v values) generated by the signing algorithm
- Use the public key or Ethereum address to verify the signature against the original message
- Observe how any modification in the message or signature invalidates verification
- Deploy or simulate the verification process within a smart contract or client-side script to demonstrate verification efficacy

Observation:

- Digital signatures uniquely link a message to a signer while preserving message integrity
- Signatures are verifiable by anyone with the public key, ensuring transparency on the blockchain
- Any tampering with the signed message or signature invalidates the verification, protecting against fraud
- ECDSA is efficient and secure, making it suitable for decentralized application transactions and identity authentication

ASSESMENT

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.