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 Signatures Demo**

## Objective/Aim:

To demonstrate how **Elliptic Curve Digital Signature Algorithm (ECDSA)** is used to create and verify digital signatures for secure blockchain transactions.

## Apparatus/Software Used:

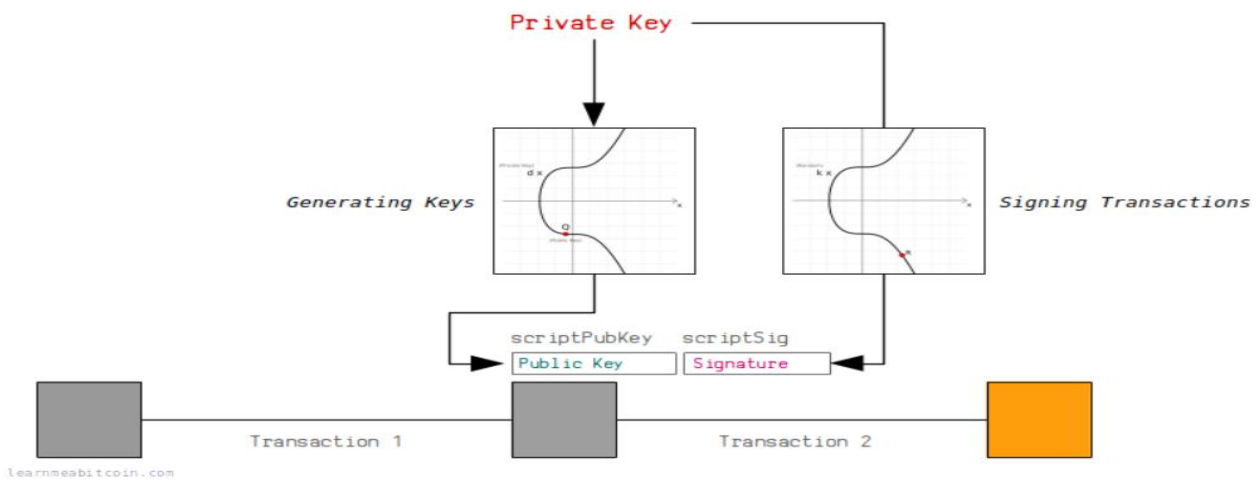
- Text editor
- Brave for searching

## Theory concept:

**What is ECDSA:**

ECDSA (Elliptic Curve Digital Signature Algorithm) is a cryptographic algorithm used for creating and verifying digital signatures based on elliptic curve mathematics. It provides a secure way to prove ownership without revealing the private key. In Bitcoin and other cryptocurrencies, ECDSA is essential for verifying transactions: a user generates a private key (a secret number) and derives a public key from it using elliptic curve multiplication. When a transaction is signed with the private key, the network uses the corresponding public key to verify the signature's validity, ensuring that only the rightful owner can authorize spending of funds.

Visit this website to explore how can we generate public and private key and our digital signature:-
https://learnmeabitcoin.com/technical/cryptography/elliptic-curve/ecdsa/




Bitcoin uses a digital signature system called ECDSA (Elliptic Curve Digital Signature Algorithm) to manage the ownership of bitcoins. This system works by allowing users to create a pair of keys: a private key, which must be kept secret, and a public key, which can be shared openly. The private key is used to generate digital signatures that prove ownership of the corresponding public key without revealing the private key itself.

# Procedure:

ECDSA uses elliptic curve cryptography as the foundation for its digital signature system. In simple terms, public keys and signatures are points on an elliptic curve. If both the public key and the signature are generated from the same private key (a large secret number), there exists a geometric relationship between these points that proves ownership. The main mathematical operation involved is elliptic curve multiplication, which means repeatedly adding a point on the curve to itself a certain number of times to reach a new point. This operation is easy to perform in one direction but practically impossible to reverse, making it highly secure. Because of this property, elliptic curves are widely used in cryptography for generating keys and digital signatures.

**Key Generation**

Private Key [↑]

**EC Multiply**

Multiply a point on the *secp256k1* elliptic curve.

Generator Point | Random Point

Point 1

x: 0d 23739427886711485218638084450247759734409109163193371052940366296847665295586

y: 0d 100647920449908968938962477935397960745018344376152854961407455453111497843747

Multiplier

0d 726195168401444737024569713756089465731612278212397429212765003401935317483 71 +1 Random

Point 1 x Multiplier

x: 0d 88292561464989308344709104806864106177111152001814995991502960645554147313268

y: 0d 32999371027532285095723912844762984307821224901245822680175669491185865644835

# Observation:

- ECDSA uses elliptic curve cryptography to generate a public key from a private key using a one-way multiplication function, making it secure.
- The signing process creates a digital signature (r, s) that proves ownership without revealing the private key. Verification only requires the public key, message hash, and signature, ensuring the private key remains confidential.
- Reusing the same nonce during signing can compromise security by exposing the private key, so randomness is critical..

## 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 :***

***Signature of the Faculty:***

***Regn. No. :***



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