Centurion
UNIVERSITY
Shaping Lives
Empowering Communities...

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

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

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

Date: ....

Classroom Learning

(Learning by Listening and Observations)

Name of the Topic: Digital Signature

Learning Outcome:

Concepts learned (Mention 2/3 principles):

Based on the classwork, the principal concepts I have learned include:

1. The fundamental concept of a digital signature as a cryptographic mechanism that provides authentication, data integrity, and non-repudiation for a digital message or document.
2. The complete architecture of how digital signatures are generated using a private key and verified by anyone using the corresponding public key.
3. The characteristics that make digital signatures secure, including their reliance on mathematical one-way functions and the practical impossibility of forging a signature without the private key

* New techniques learned:

Additionally, I have acquired new knowledge in the following areas:

1. Techniques for generating a digital signature by first creating a hash of the message and then encrypting that hash with the sender's private key.
2. Procedures for signature verification, which involves decrypting the signature with the sender's public key to obtain a hash and comparing it to a newly generated hash of the received message.
3. The process of how digital signatures are implemented in blockchain protocols (e.g., using ECDSA) to prove ownership of funds and authorize transactions without revealing the private key.
4. Methods for understanding the difference between a digital signature and a simple cryptographic hash, highlighting the added layer of authentication.

* Related Project/Practice work experienced and learned:

During the practice sessions of the lab work, I engaged in and developed proficiency with programs and simulations in the following areas:

1. Writing a Python program using the cryptography library to generate a public/private key pair, sign a message, and then verify the signature.
2. Manually verifying a digital signature step-by-step using OpenSSL commands to understand the underlying mathematical operations.
3. Analyzing a real Bitcoin transaction on a block explorer to see the ECDSA digital signature in the scriptSig field.
4. Simulating a man-in-the-middle attack to demonstrate how an altered message will fail signature verification, thus ensuring data integrity.

New Software/Machine/Tool/Equipment/Experiment learned:

During the lab session, I used **OpenSSL** in the command line to generate keys and signatures, **Python with cryptography libraries** for scripting, and **Blockchain Explorers** (Etherscan, Blockchain.com) to observe real-world digital signatures on the blockchain.

Application of concept(s) (preferably real life scenario):

1. **Blockchain Transactions:** Used to authorize the transfer of cryptocurrencies, proving that the owner of the private key approves the transaction, which is fundamental to all blockchain operations.
2. **Software Distribution:** Developers sign software updates with their private key, and users' systems verify the signature with the public key before installation, ensuring the code has not been tampered with.
3. **Secure Communication:** Protocols like SSL/TLS use digital signatures to authenticate servers to clients, ensuring users are connecting to the legitimate website and not an imposter.

* Case Studies/Examples:

1. **Bitcoin Transactions:** Every Bitcoin transaction includes a digital signature from the sender, which is verified by every node on the network before the transaction is confirmed, preventing unauthorized spending.
2. **Digital Document Signing**: Platforms like DocuSign use digital signatures to legally bind electronic documents, providing a secure and efficient alternative to wet signatures for contracts.
3. **Secure Booting:** Modern devices (phones, hardware wallets) use digital signatures to verify the integrity and authenticity of the bootloader and operating system during startup, preventing the execution of malicious firmware.

Assessment:

Marks Obtained: .... / 10

Signature of the Faculty:

Signature of the Student:

Name : PN Archana

Regn. No. : 240720100147

*** *As applicable according to the topic.***
One sheet per topic (10-20) to be used.