|  |  |
| --- | --- |
| **Walchand College of Engineering, Sangli**  *(Government Aided Autonomous Institute)* | |
| **AY 2025-26** | |
| **Course Information** | |
| **Programme** | B.Tech. (Computer Science and Engineering) |
| **Class, Semester** | Final Year B. Tech., Sem VII |
| **Course Code** | 6CS451 |
| **Course Name** | Cryptography and Network Security Lab |

**Experiment No. 10**

**Title** Implement the SIGNATURE SCHEME – Digital Signature Standard

**Objectives:**

To implement the **Digital Signature Standard (DSS)** using the **Digital Signature Algorithm (DSA)** to create and verify digital signatures, thereby ensuring the authenticity and integrity of electronic messages or documents.

**Problem Statement:**

In digital communication, ensuring the authenticity of a sender and the integrity of the message is critical. A **digital signature** serves as a cryptographic technique to validate both.

Design and implement a system using the **Digital Signature Standard (DSS)** that performs the following tasks:

# Key Generation:

* + Generate a private key (used for signing) and a public key (used for verifying).
  + Use parameters such as large prime numbers and hash functions (e.g., SHA-1 or SHA-256) as required by DSA.

# Message Signing:

* + Accept a message (text input).
  + Use the private key to generate a **digital signature** for the message using the DSA algorithm.

# Signature Verification:

* + Use the corresponding public key to verify the **digital signature** against the original message.
  + Confirm whether the signature is valid or has been tampered with.

# Demonstrate Security:

* + Show that any alteration in the message or signature results in a failed verification.
  + Explain how this ensures **message integrity**, **authentication**, and **non-repudiation**.

The system should simulate a real-world use case where one party signs a message and another party verifies it, highlighting how digital signatures help in secure digital communications, such as email signing, legal document authentication, or secure software distribution.

**Equipment/Tools: Theory:**

**Procedure:**

**Steps:**

**Observations and Conclusion:**