|  |  |
| --- | --- |
| **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. 09**

**Title –** Calculate the message digest of a text using the SHA-1 algorithm

**Objectives:**

To understand and implement the **SHA-1 (Secure Hash Algorithm 1)** for generating a fixed-length message digest from a given input text. The goal is to demonstrate how data integrity can be maintained and verified using cryptographic hash functions.

**Problem Statement:**

In digital communications and data storage, ensuring the integrity of data is crucial. One common approach to verifying that a message has not been altered is to compute a **message digest**—a fixed-size string that uniquely represents the input data.

Implement a program that:

1. Accepts a **text input** from the user.
2. Calculates the **SHA-1 hash** (message digest) of the input text using a cryptographic library or custom logic.
3. Outputs the **SHA-1 digest** in **hexadecimal format**.
4. Demonstrates that any change in the input results in a completely different message digest, highlighting the **avalanche effect** of the hash function.

Additionally, briefly explain the role of SHA-1 in real-world applications, such as digital signatures, checksums, and data integrity verification.

**Equipment/Tools: Theory:**

**Procedure:**

**Steps:**

**Observations and Conclusion:**