Government College of Engineering, Jalgaon
(An Autonomous Institute of Govt. of Maharashtra)

Name:	**PRN:**
Class: L.Y	**Semester:** VII
Batch: B	
Date of Performance: ______________	**Date of Completion:** _______________
Subject: CO407U CNSL	**Subject Teacher:** Ms. Shrutika Mahajan

Practical – 11

Aim: Calculate the message digest of a text using the SHA-1 algorithm in any programming language.

Software Used:

Operating system: ubuntu
Programming Language: Python3

Theory:

What is SHA-1?

SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function that takes an input (or "message") and produces a fixed-size, 160-bit (20-byte) hash value known as a message digest. SHA-1 is commonly represented as a 40-character hexadecimal number. It was developed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) in 1995 as part of the U.S. government's Secure Hash Standard.

Characteristics of SHA-1:

- **Fixed Output Length:** The algorithm always produces a 160-bit hash value, regardless of the input size.
- **One-Way Function:** It is computationally infeasible to reverse-engineer the original input from the output hash.
- **Collision Resistance (formerly):** Ideally, two different inputs should not produce the same output hash, although this property is compromised for SHA-1 due to advances in cryptanalysis.

Applications of SHA-1:

- **Data Integrity Verification:** Ensuring data has not been altered during transmission.
- **Digital Signatures:** Used in some cryptographic algorithms for verifying the authenticity of messages.
- **Checksum and Fingerprinting:** Validating file contents.

How SHA-1 Works:

SHA-1 processes data by breaking it into chunks of 512-bit blocks and padding the last block if necessary. The algorithm involves several rounds of bitwise operations, including rotations, logical functions, and modular additions.

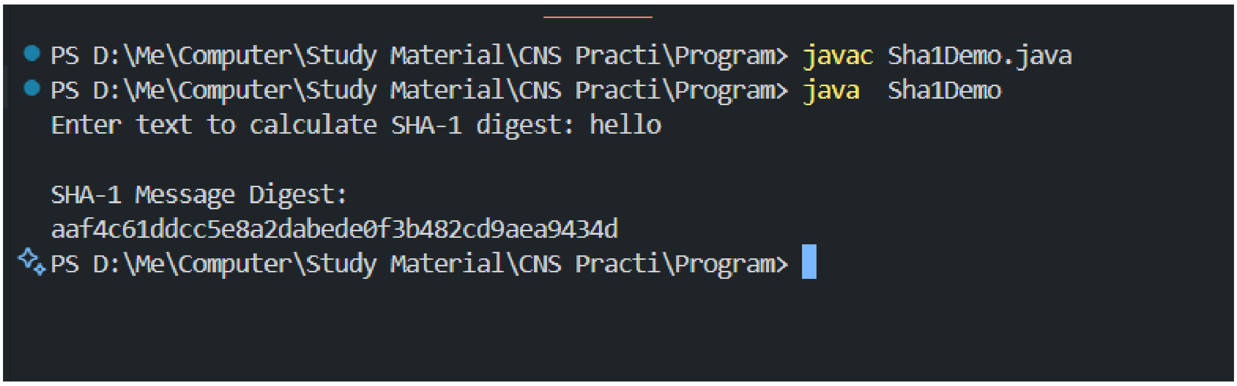
Steps in SHA-1 Algorithm:

1. **Preprocessing:**
    - **Padding:** The message is padded so that its length is congruent to 448 modulo 512. Padding consists of a single '1' bit followed by '0' bits.
    - **Length Appending:** The original message length (in bits) is appended to the end of the padded message, making the total length a multiple of 512 bits.
2. **Message Processing:**
    - **Initialization:** SHA-1 starts with five 32-bit initial hash values.
    - **Processing in Rounds:** The message is processed in blocks of 512 bits, with operations including bitwise logical functions, rotations, and modular additions.
    - **Compression Function:** The intermediate hash values are updated in each round through 80 iterations.
3. **Output:** The result is a 160-bit message digest, represented in hexadecimal form.

Code:

```
import java.nio.charset.StandardCharsets;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.Scanner;
public class Sha1Demo {
    // convert bytes to hex string
    private static String bytesToHex(byte[] bytes) {
        StringBuilder sb = new StringBuilder(bytes.length * 2);
        for (byte b : bytes) {
            sb.append(String.format("%02x", b & 0xff));
        }
        return sb.toString();
    }
    public static void main(String[] args) {
        Scanner scanner = new Scanner(System.in);
        System.out.print("Enter text to calculate SHA-1 digest: ");
        String text = scanner.nextLine();
        scanner.close();
        try {
            MessageDigest md = MessageDigest.getInstance("SHA-1");
            byte[] digestBytes =
md.digest(text.getBytes(StandardCharsets.UTF_8));
            String digestHex = bytesToHex(digestBytes);
            System.out.println("\nSHA-1 Message Digest:");
            System.out.println(digestHex);
        } catch (NoSuchAlgorithmException e) {
            // SHA-1 is always available in standard JVMs, but handle just in case
            System.err.println("SHA-1 algorithm not available: " + e.getMessage());
        }
    }
}
```

<u>Output:</u>



```
● PS D:\Me\Computer\Study Material\CNS Practi\Program> javac Sha1Demo.java
● PS D:\Me\Computer\Study Material\CNS Practi\Program> java  Sha1Demo
  Enter text to calculate SHA-1 digest: hello

  SHA-1 Message Digest:
  aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d
  PS D:\Me\Computer\Study Material\CNS Practi\Program>
```

<u>Conclusion:</u>

The SHA-1 algorithm generates a fixed 160-bit hash value that uniquely represents the input text, ensuring data integrity verification.

Course Teacher
Ms. Shrutika Mahajan