**IT8761 – Security Laboratory**

**Reshma Ramesh Babu**

**312217104129**

**Exercise 8**

**Aim:** To implement the message digest SHA1.

**Code:**

import java.math.BigInteger;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

public class SHA1 {

public static String encrypt(String input)

{

try {

// getInstance() method is called with algorithm SHA-1

MessageDigest md = MessageDigest.getInstance("SHA-1");

// digest() method is called

// to calculate message digest of the input string

// returned as array of byte

byte[] messageDigest = md.digest(input.getBytes());

// Convert byte array into signum representation

BigInteger no = new BigInteger(1, messageDigest);

// Convert message digest into hex value

String hashtext = no.toString(16);

// Add preceding 0s to make it 32 bit

while (hashtext.length() < 32) {

hashtext = "0" + hashtext;

}

// return the HashText

return hashtext;

}

// For specifying wrong message digest algorithms

catch (NoSuchAlgorithmException e) {

throw new RuntimeException(e);

}

}

// Driver code

public static void main(String args[]) throws NoSuchAlgorithmException

{

String worda = "67452301";

System.out.println("\nMessage digest of word a " + worda + " : " + encrypt(worda));

String wordb = "efcdab89";

System.out.println("\nMessage digest of word b " + wordb + " : " + encrypt(wordb));

String wordc = "98badcfe";

System.out.println("\nMessage digest of word c " + wordc + " : " + encrypt(wordc));

String wordd = "10325476";

System.out.println("\nMessage digest of word d " + wordd + " : " + encrypt(wordd));

String worde = "c3d2e1f0";

System.out.println("\nMessage digest of word e " + worde + " : " + encrypt(worde));

}

}

**Output:**

