Shankar Narayanan S
312217104146
30-10-2020

SSN COLLEGE OF ENGINEERING
Department of Computer Science and Engineering
IT 8761 - Security Lab

Exercise 8 : To implement the Message Digest SHA-1

CODE :

```
// Java program to calculate SHA-1 hash value

import java.util.*;
import java.lang.*;
import java.io.*;
import java.math.*;
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

class SHA1{
   public String encryptThisString(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);
        }
    }
}

public class SHADriver2 {

    // Driver code
    public static void main(String args[]) throws
                                                        NoSuchAlgorithmException
    {
        Scanner in = new Scanner(System.in);

        String ptext;
        System.out.println("Enter the String to hash : ");

        ptext = in.nextLine();

        SHA1 sha = new SHA1();
        System.out.println("HashCode Generated by SHA-1 : ");

        System.out.println(sha.encryptThisString(ptext)+"\n\n");
    }
}
```

OUTPUT :

(base) Shankars-MacBook-Pro:Ex14 shankar99$ java SHADriver2

Enter the String to hash :
The enemy has landed on the east

HashCode Generated by SHA-1 :
cbe5d368403e454000dd0f98a299c28e0fc154e3

(base) Shankars-MacBook-Pro:Ex14 shankar99$

Result : Have implemented the SHA-1 algorithm on given input to produce a 160 bit hash.