UNIVERSITY INSTITUTE OF ENGINEERING

Department of Computer Science & Engineering

Subject Name: WEB AND MOBILE SECURITY LAB

Submitted to:

Er. Mandeep Kaur

Submitted by:

Name: Ruchika Raj

UID: 20BCS9285

Section: 20BCS615

Group: B

Experiment-2.1

Student Name: Ruchika Raj
UID: 20BCS9285
Branch: BE-CSE
Section/Group: 20BCS_WM_615-B
Semester: FIFTH
Date of Performance: 09/11/22
Subject Name: WMS LAB

Aim:

Write a program to generate message digest for the given message using the SHA/MD5 algorithm and verify the integrity of message.

Software/Hardware Requirements:

window 7 and above version **Tools to**

be used:

1. Eclipse IDE
2. JDK (Java Development kit)
3. IntelliJ IDEA

Steps/Method/Coding:

To calculate cryptographic hashing value in Java, **MessageDigest** Class is used, under the package java.security.

MessageDigest Class provides following cryptographic hash function to find hash value of a text as follows:

- MD2
- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

1.This Algorithms are initialize in static method called **getInstance()**.

2. After selecting the algorithm it calculate the **digest** value and return the results in byte array.

3. BigInteger class is used, which converts the resultant byte array into its **sign-magnitude representation**.

4.This representation is then converted into a hexadecimal format to get the expected MessageDigest.

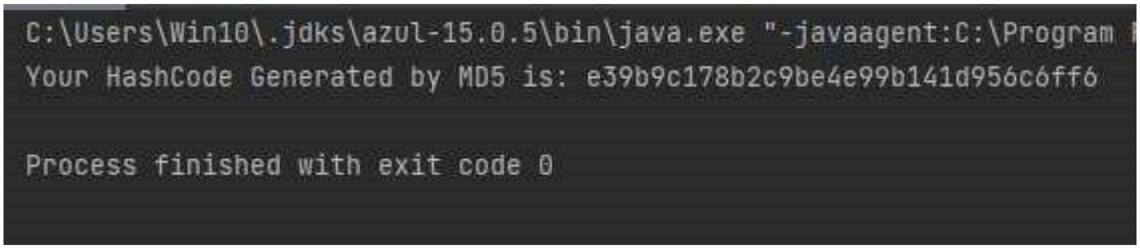
Code (MD5 algorithm):

```
package com.company;

import java.math.BigInteger; import
java.security.MessageDigest;
import java.security.NoSuchAlgorithmException; //
Java program to calculate MD5 hash value public
class MD5 {
   public static String getMd5(String input)
   {        try
{
         // Static getInstance method is called with hashing MD5
         MessageDigest md = MessageDigest.getInstance("MD5");
         // digest() method is called to calculate message digest
// of an input digest() return 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);           while
(hashtext.length() < 32) {
hashtext = "0" + 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 s = "GeeksForGeeks";
        System.out.println("Your HashCode Generated by MD5 is: " +    getMd5(s));
    }
}
```

Output: (Screenshots)



```
C:\Users\Win10\.jdks\azul-15.0.5\bin\java.exe "-javaagent:C:\Program
Your HashCode Generated by MD5 is: e39b9c178b2c9be4e99b141d956c6ff6

Process finished with exit code 0
```

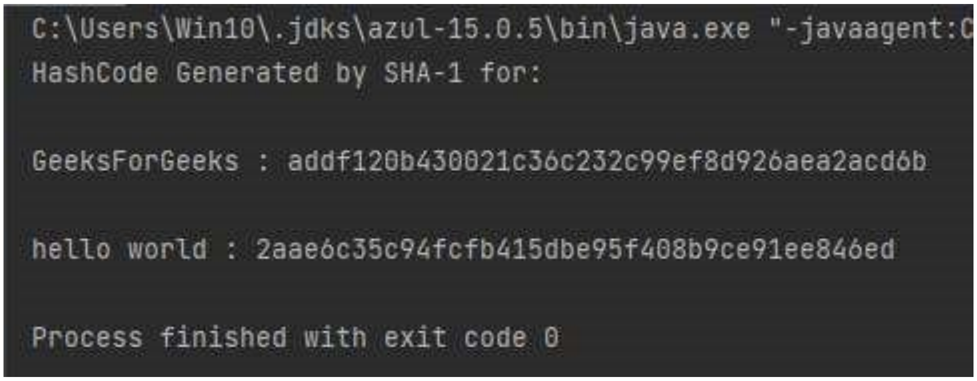
Code (SHA Algorithm):

```
package com.company;

import java.math.BigInteger; import
java.security.MessageDigest; import
java.security.NoSuchAlgorithmException; public class
GFG {
    public static 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);
        }
    }
    // Driver code      public static void
main(String args[]) throws
            NoSuchAlgorithmException
    {
        System.out.println("HashCode Generated by SHA-1 for: ");

        String s1 = "GeeksForGeeks";
        System.out.println("\n" + s1 + " : " + encryptThisString(s1));
        String s2 = "hello world";
        System.out.println("\n" + s2 + " : " + encryptThisString(s2));
    }
}
```

Output (Screenshots):



```
C:\Users\Win10\.jdks\azul-15.0.5\bin\java.exe "-javaagent:C
HashCode Generated by SHA-1 for:

GeeksForGeeks : addf120b430021c36c232c99ef8d926aea2acd6b

hello world : 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed

Process finished with exit code 0
```

Learning Outcomes:

Output is often known as hash values, hash codes, message digest. The length of output hashes is generally less than its corresponding input message length.