Experiment 5

Student Name: Rajiv Paul
UID: 20BCS1812
Branch: BE CSE
Section/Group: 702-A
Semester: 5th
Date of performance: 02/11/2022
Subject: Web and Mobile Security Lab
Subject Code: 20CSP_338

Aim/Overview of the Practical:

Message digest using SHA / MD5 Algorithm.

Task to be done / Which logistics used:

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

Software / Hardware Requirements:

Windows 7 and above version.

Tools to be used:

1. Eclipse IDE
2. JDK (Java Developer Kit)
3. IntelliJ IDE

Introduction:

Message Digest is used to ensure the integrity of a message transmitted over an insecure channel where the contents of the message can be changed. The message is passed through a cryptographic hash function. This function created a compressed image of the message called digest.

Steps for experiment/practical/Code:

1. Initialize the algorithm in static method called getInstance().

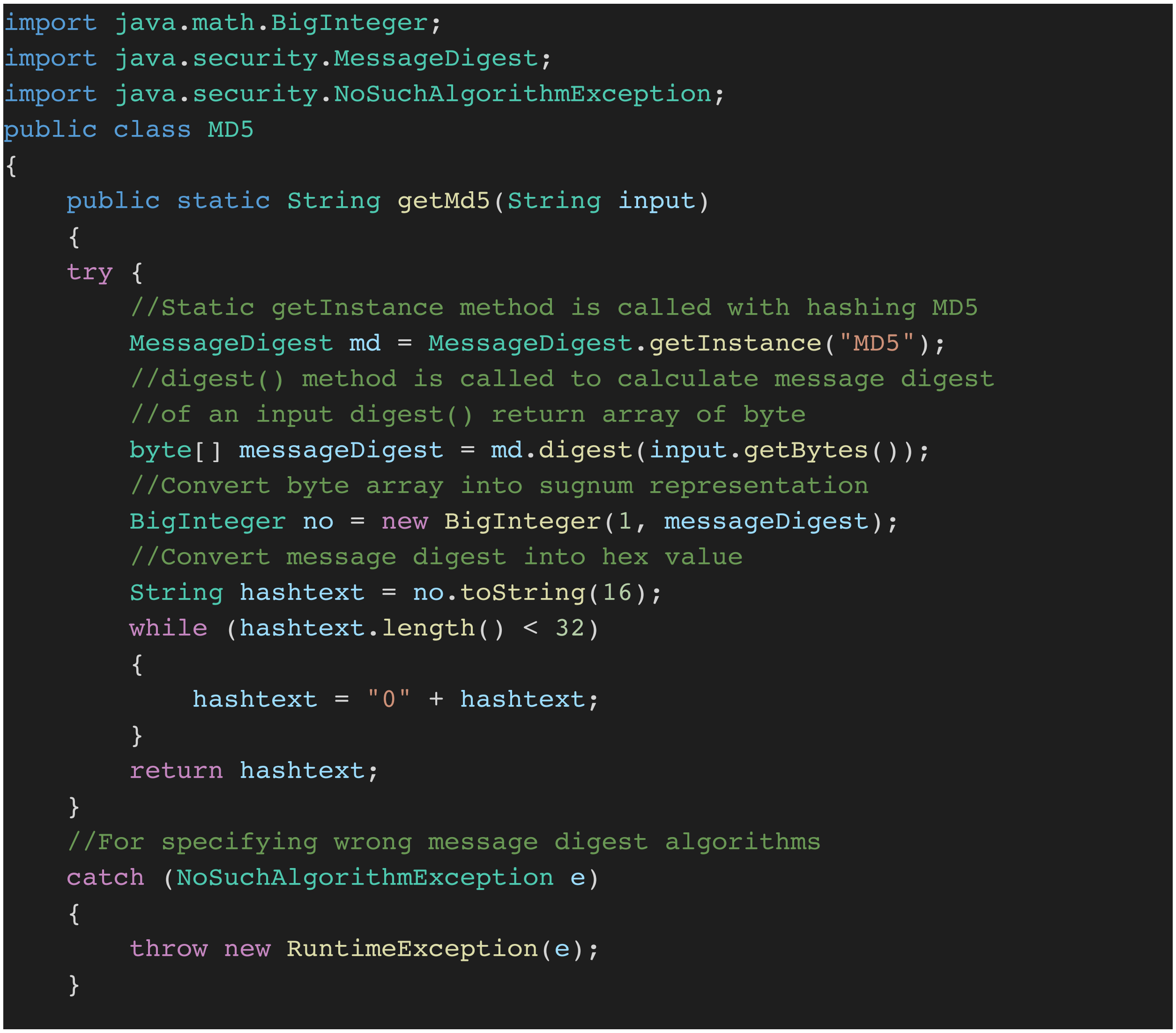
2. After selecting the algorithm it calculate the digest value and return the results in byte array.

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:

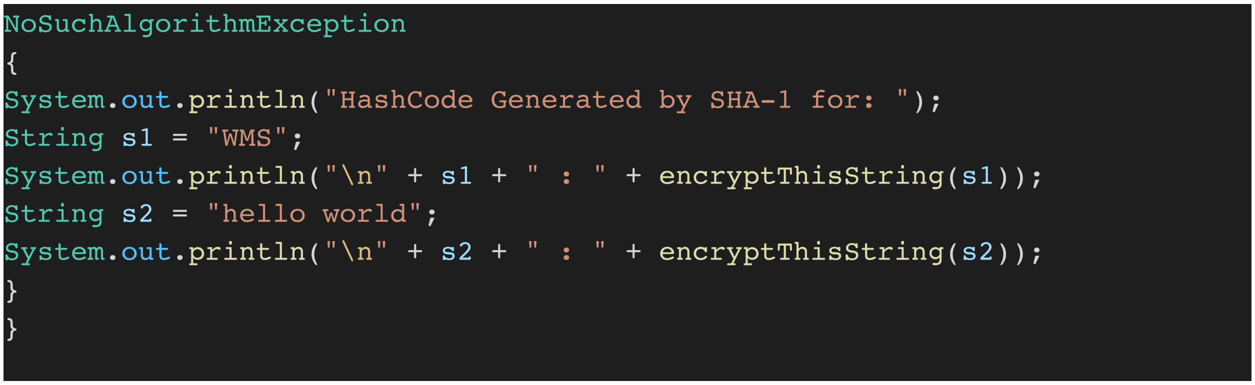
1. **MD5 algorithm:**



```
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
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 sugnum 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);
    }
}
public static void main(String args[]) throws NoSuchAlgorithmException
{
    String s = "Hello world";
    System.out.println("Your hashcode generated by MD5 is:" + getMd5(s));
}
}
```

SHA Algorithm:

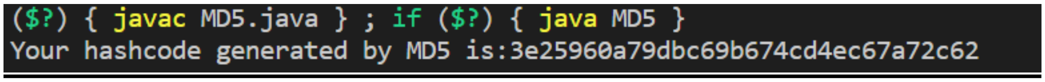
```
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
public class SHA {
public static String encryptThisString(String input)
{
try {
// getInstance() method is called with algorithm SHA-1
MessageDigest md = MessageDigest.getInstance("SHA-1");
// 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 = "WMS";
System.out.println("\n" + s1 + " : " + encryptThisString(s1));
String s2 = "hello world";
System.out.println("\n" + s2 + " : " + encryptThisString(s2));
}
}
```

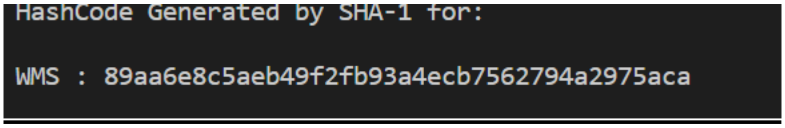
Result/Output/Writing Summary:

MD5 Algorithm



```
($?) { javac MD5.java } ; if ($?) { java MD5 }
Your hashcode generated by MD5 is:3e25960a79dbc69b674cd4ec67a72c62
```

SHA Algorithm



```
HashCode Generated by SHA-1 for:

WMS : 89aa6e8c5aeb49f2fb93a4ecb7562794a2975aca
```

Learning outcomes (What I have learnt):

a. Output is known as hash values, hash codes, message digest.

b. The length of output hashes is generally less than its corresponding input message length.