Experiment 2.1

Student Name: RAJDEEP JAISWAL. UID: 20BCS2761
Branch: CSE Section/Group: 902 B
Semester: 5th
Subject Name: WMS LAB Subject Code: 20CSP-338

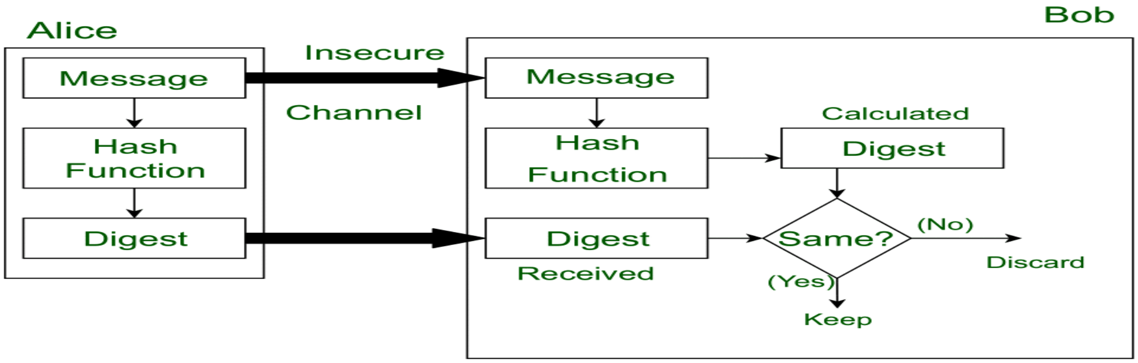
1. **Aim:** Write a program to generate message digest for the given message using the SHA/MD5 algorithm and verify the integrity of message.

2. **Objective:** To understand how to generate message digest for given message.

3. **Software/Hardware Requirements:** window 7 and above version

4. **Tools to be used:**
   - Eclipse IDE
   - JDK (Java Development kit)
   - IntelliJ IDEA

5. **Introduction:**
   Message Digest is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed). The message is passed through a Cryptographic hash function. This function creates a compressed image of the message called **Digest**.



6. Steps, Code and output:

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.

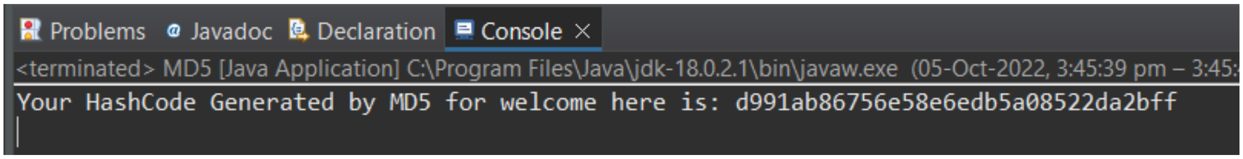
3. BigInteger class is used, which converts the resultant byte array into its **sign-magnitude representation**.

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

Coding (MD5 algorithm):

```
package experiments;
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

public class MD5 {
        public static String getMd5(String input)
        {
                try {

                        MessageDigest md = MessageDigest.getInstance("MD5");

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

                        BigInteger no = new BigInteger(1, messageDigest);

                        String hashtext = no.toString(16);
                        while (hashtext.length() < 32) {
                                hashtext = "0" + hashtext;
                        }
                        return hashtext;
                }
                catch (NoSuchAlgorithmException e) {
                        throw new RuntimeException(e);
                }
        }
        public static void main(String args[]) throws NoSuchAlgorithmException
        {
                String s = "welcome here";
                System.out.println("Your HashCode Generated by MD5 for "+s+" is:
" + getMd5(s));
        }
}
```

OUTPUT:



```
<terminated> MD5 [Java Application] C:\Program Files\Java\jdk-18.0.2.1\bin\javaw.exe  (05-Oct-2022, 3:45:39 pm – 3:45:
Your HashCode Generated by MD5 for welcome here is: d991ab86756e58e6edb5a08522da2bff
```

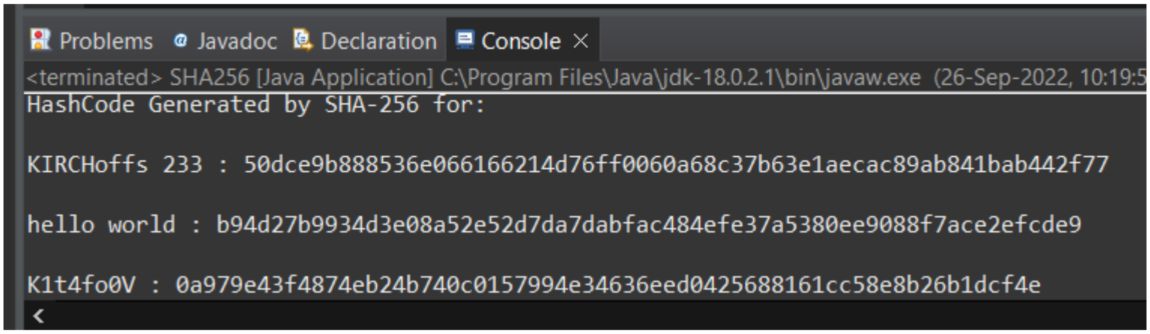
Coding (SHA algorithm):

```
package experiments;
import java.math.BigInteger;
import java.nio.charset.StandardCharsets;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
```

```
class SHA256 {
    publicstatic byte[] getSHA(String input) throws NoSuchAlgorithmException
    {

        MessageDigest md = MessageDigest.getInstance("SHA-256");
        return md.digest(input.getBytes(StandardCharsets.UTF_8));
    }

    public static String toHexString(byte[] hash)
    {
        BigInteger number = new BigInteger(1, hash);

        StringBuilder hexString = new StringBuilder(number.toString(16));

        while (hexString.length() < 64)
        {
            hexString.insert(0, '0');
        }

        return hexString.toString();
    }
    public static void main(String args[])
    {
        try
```

```
                {
                        System.out.println("HashCode Generated by SHA-256 for:");

                        String s1 = "KIRCHoffs 233";
                        System.out.println("\n"+ s1 + " : " + toHexString(getSHA(s1)));

                        String s2 = "hello world";
                        System.out.println("\n"+ s2 + " : " + toHexString(getSHA(s2)));

                        String s3 = "K1t4fo0V";
                        System.out.println("\n"+ s3 + " : " + toHexString(getSHA(s3)));
                }
                catch (NoSuchAlgorithmException e) {
                        System.out.println("Exception thrown for incorrect algorithm: "
+ e);
                }
        }
}
```

OUTPUT:



```
<terminated> SHA256 [Java Application] C:\Program Files\Java\jdk-18.0.2.1\bin\javaw.exe  (26-Sep-2022, 10:19:5
HashCode Generated by SHA-256 for:

KIRCHoffs 233 : 50dce9b888536e066166214d76ff0060a68c37b63e1aecac89ab841bab442f77

hello world : b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

K1t4fo0V : 0a979e43f4874eb24b740c0157994e34636eed0425688161cc58e8b26b1dcf4e
```

LEARNING OUTCOMES:

- Learnt about message digest and its coding algorithm.
- Learnt to code SHA-256 and MD5 algorithm.
- Learnt to use Eclipse IDE.
- Learnt about hashing and hash values.