

Experiment No. 4

Aim: For varying message sizes, test integrity of message using MD-5, SHA-1, and analyze the performance of the two protocols. Use crypt APIs

Code:

```
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.Scanner;

public class Main {
    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 String encryptThisString(String input) {
        try {
            MessageDigest md = MessageDigest.getInstance("SHA-1");
            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 {
    System.out.println("\nHashCode Generated by SHA-1 for: ");
    Scanner sc = new Scanner(System.in);
    String str = sc.nextLine();
    System.out.println("\n" + str + " : " + encryptThisString(str));
    System.out.println("\nHashCode Generated by MD5 for: ");
    System.out.println("\n" + str + " : " + getMd5(str));

    sc.close();
}
}

```

Output:

```

PROBLEMS  DEBUG CONSOLE  OUTPUT  PORTS  SEARCH ERROR  COMMENTS  TERMINAL
Microsoft Windows [Version 10.0.22621.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Documents\Hem32> cmd /C "C:\Users\student\AppData\Roaming\Code\User\globalStorage\pleiades.java-extension-pack-jdk\java\17\bin\java.exe -XX:+ShowCodeDetailsInExceptionMessages -cp C:\Users\student\AppData\Roaming\Code\User\workspaceStorage\15aeebde02684bffc014e3011dbcb1b\redhat.java\jdt_ws\Hem32_c7c4ac65\bin Main "

HashCode Generated by SHA-1 for:
Hello World

Hello World : a4d55a8d778e5022fab701977c5d840bbc486d0

HashCode Generated by MD5 for:
Hello World : b10a8db164e0754105b7a99be72e3fe5

C:\Users\student\Documents\Hem32>

```