17.12.20 IT 8761 Security Laboratory 312217104039
U.EsakkiMathy.

Aim:

To develop a java program to implement SHA-I algorithm.

Algorithm:

i) SHA-I is a cryptographic hash function. It takes the given message as input and produce hash value (message digest) as output.

ii) It involves appending the padding bits. Padding bits consists of a single 1 bit followed by necessary number of 0 bits.

iii) A 64 bit representation of the length of Message is appended.

iv) 5 MD buffers A, B, C, D, E are initialized and the message is processed as 512 bit blocks.

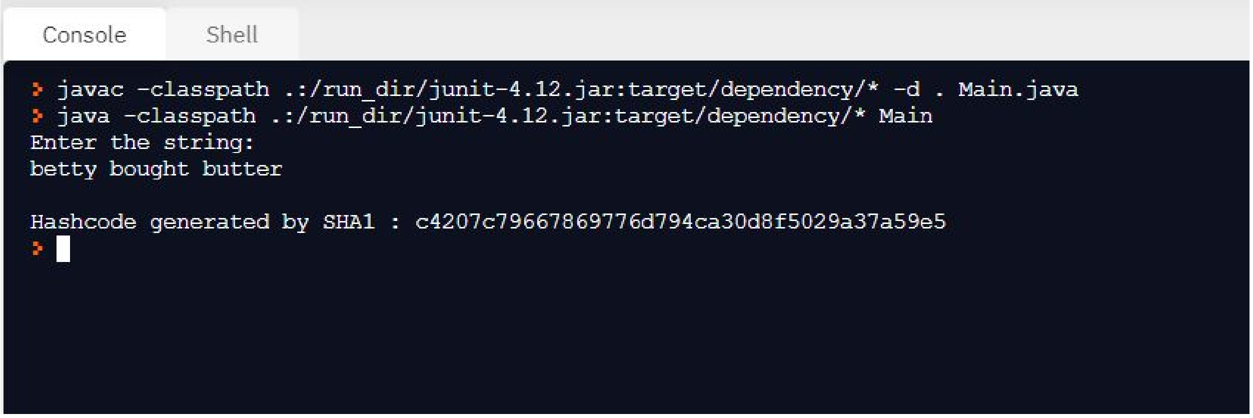
v) After all 512 bit blocks have been processed, the output of 160 bit message digest is produced.

vi) It is then converted into hexadecimal of 40 digits long.

Program:

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

class Main {
 public static String encrypt(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 {
    String s1;
    Scanner s=new Scanner(System.in) ;
    System.out.println("Enter the string: ");
    s1=s.nextLine();
    System.out.println("\nHashcode generated by SHA1 :
"+encrypt(s1));



  }
}
```

Output:



```
> javac -classpath .:/run_dir/junit-4.12.jar:target/dependency/* -d . Main.java
> java -classpath .:/run_dir/junit-4.12.jar:target/dependency/* Main
Enter the string:
betty bought butter

Hashcode generated by SHA1 : c4207c79667869776d794ca30d8f5029a37a59e5
> 
```