PAGE NO.: 20
DATE .: / / 20

Practical No. 10

Aim:- To write a program to implement SHA algorithm.

Theory:- The secure hash algorithm is widely ~~use~~ known as SHA. It is a cryptographic hash function. A cryptographic hash function is an algorithm that randomly takes data as input without a specific reason and produces an output of text in a coded form ("Hash-Value". The coded text will be stored instead of the password that is used to verify that the user and this enciphered text is used to verify the user instead of the password. There are several different forms of SHA are:

1) SHA - 1
2) SHA - 2
3) SHA - 256
4) SHA - 512
5) SHA - 224
6) SHA - 384

Various applications also uses SHA, they are:-

1) Secure ~~Shee~~ Shell protocol (SSH) applications.
2) Secure Multipurpose Internet Mail Extensions (S-MIME)
3) Intrusion Prevention System (IPS)

Algorithm ⇒ To begin using SHA in jave, the 'java.security' package must be imported into the program.

1) After importing the above package into a Java program, the "message digest" class is used in Java for calculating the value of cryptographic hash function.
2) The secure hash Algorithms are always initiated in a static method called "getInstance()".
3) A preferred SHA form must be selected after the initiate to calculate the message digest.
4) The results return a byte array value after the message digest

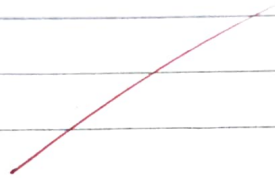
Amar KRISH

Teacher's Signature _____

is calculated.

5. The byte array is converted into its sign form by using a "Big Integer" class.
6. At last, the sign form is turned into a hexadecimal format which is our required hash value i.e. message digest.

Conclusion ⇒ A program to implement SHA algorithm has been executed successfully.



Teacher's Signature _____

Program:

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

public class SHA {
    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 {
        Scanner scanner = new Scanner(System.in);
        String s1, s2;
        System.out.println("\n HashCode Generated by SHA-1: ");
        System.out.print("\n Message: ");
        s1 = scanner.nextLine();
        System.out.println("\n Encrypted data: " + encryptThisString(s1));
    }
}
```

Output: