Program: 11 **Implementation of MD5 Algorithm**

Date:

**AIM**

**ALGORITHM**

**CODE**

import java.math.BigInteger;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

import java.security.SecureRandom;

import java.util.Scanner;

public class MD5 {

public static byte[] getSalt() throws NoSuchAlgorithmException {

SecureRandom sr = SecureRandom.getInstance("SHA1PRNG");

byte[] salt = new byte[15];

sr.nextBytes(salt);

return salt;

}

public static String getMd5(String input, Integer hasSalt) {

try {

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

if (hasSalt != 0) {

byte[] salt = getSalt();

msgDst.update(salt);

BigInteger bi = new BigInteger(1, salt);

String salttxt = bi.toString(16);

System.err.println("Salt used: " + salttxt);

}

byte[] msgArr = msgDst.digest(input.getBytes());

BigInteger bi = new BigInteger(1, msgArr);

String hshtxt = bi.toString(16);

while (hshtxt.length() < 32) {

hshtxt = "0" + hshtxt;

}

return hshtxt;

} catch(NoSuchAlgorithmException abc){

throw new RuntimeException(abc);

}

}

public static void main(String[] var0) throws NoSuchAlgorithmException {

Scanner sc = new Scanner(System.in);

System.out.print("Enter the text to encrypt: ");

String var1 = sc.nextLine();

System.out.print("Enter 0 for not including salt, 1 for including salt: ");

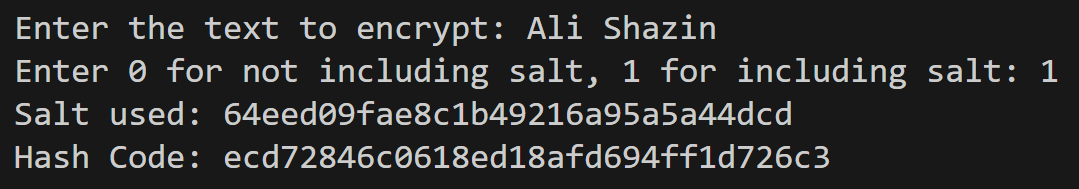
String var2 = getMd5(var1, sc.nextInt());

System.out.println("Hash Code: " + var2);

}

}

**OUTPUT**



**RESULT**

Thus, the program to implement MD5 Algorithm to generate a hash code is successfully executed.