package digitalsignature;

import java.io.StringReader;

import java.io.UnsupportedEncodingException;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

import java.util.logging.Level;

import java.util.logging.Logger;

public class DigitalSignature

{

public static void main(String args[])

{

String dig, longstr,newstr,over;

String password = "ab";

System.out.println("Original String is: "+password);

dig=DigitalSignature1(password);

System.out.println("Hash generated using MD5 : " + DigitalSignature1(password));

//Concatination( string + hash key )

longstr=password+dig;

System.out.println("Sending message with hash key: : " + longstr);

newstr=intigrity(longstr);

System.out.println("");

System.out.println("......... Reach to the Reciever.......... " );

over=receiver(newstr);

// System.out.println("Intigrity Found ");

}

public static String DigitalSignature1(String message)

{

String digest = null;

try

{

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

byte[] hash = md.digest(message.getBytes("UTF-8"));

//converting byte array to Hexadecimal

StringBuilder sb = new StringBuilder(2\*hash.length);

for(byte b : hash)

{

sb.append(String.format("%02x", b&0xff));

}

digest = sb.toString();

}catch (UnsupportedEncodingException ex)

{

Logger.getLogger(StringReader.class.getName()).log(Level.SEVERE, null, ex);

}

catch (NoSuchAlgorithmException ex)

{

Logger.getLogger(StringReader.class.getName()).log(Level.SEVERE, null, ex);

}

return digest;

}

public static String intigrity (String lng)

{

char temp;

// string conversion to array

char arr[]=lng.toCharArray();

//array display

/\*for(char i=0;i<arr.length;i++)

{

System.out.print("arr[]:"+arr[i]+" || ");

}\*/

System.out.println("");

System.out.println(".....Integration in Progress ..... ");

//integrating

//by swapping

temp=arr[0];

arr[0]=arr[2];

arr[2]=temp;

/\*for(char i=0;i<arr.length;i++)

{

System.out.print(" Integrated Message:"+arr[i]);

}\*/

String b=new String(arr);

System.out.println(" Integrated Message:"+b);

return b;

}

public static String receiver(String rec)

{

String b1=null;

String send;

//conversion to array to split message & hash key

char[] arr=rec.toCharArray();

char arr1[]=new char[3];

char arr2[]=new char[31];

for(int i=0;i<3;i++)

{

arr1[i]=arr[i];

// System.out.println("LAST: "+arr1[i]);

}

//Message

String sender=new String(arr1);

//Generating hash key of recieved message

send=DigitalSignature1(sender);

System.out.println("Recieved: "+send);

System.out.print("Original :");

for(int i=3;i<=30;i++)

{

arr2[i]=arr[i];

System.out.print(arr2[i]);

}

//compare sender's & reciever's hash key System.out.println("");

System.out.println("\n Hash kay's are Equal?? : --> "+arr2.equals(send));

return b1;

}

}