**Practical VII**

**Roll No: 07 Date: 18/11/22**

**Aim: Program to implement HMAC for signing messages.**

**CODE**

package prac3;

import javax.crypto.Mac;

import javax.crypto.spec.SecretKeySpec;

import java.security.InvalidKeyException;

import java.security.NoSuchAlgorithmException;

import static java.nio.charset.StandardCharsets.UTF\_8;

import java.util.Scanner;

\* @author Shubham Khedaskar

public class practical7 {

String generateHmac256(String message, byte[] key) throws InvalidKeyException, NoSuchAlgorithmException {

byte[] bytes = hmac("HmacSHA256", key, message.getBytes());

return bytesToHex(bytes);

}

byte[] hmac(String algorithm, byte[] key, byte[] message) throws NoSuchAlgorithmException, InvalidKeyException {

Mac mac = Mac.getInstance(algorithm);

mac.init(new SecretKeySpec(key, algorithm));

return mac.doFinal(message);

}

String bytesToHex(byte[] bytes) {

final char[] hexArray = "0123456789abcdef".toCharArray();

char[] hexChars = new char[bytes.length \* 2];

for (int j = 0, v; j < bytes.length; j++) {

v = bytes[j] & 0xFF;

hexChars[j \* 2] = hexArray[v >>> 4];

hexChars[j \* 2 + 1] = hexArray[v & 0x0F];

}

return new String(hexChars);

}

public static void main(String[] args) throws NoSuchAlgorithmException, InvalidKeyException {

// String valueToDigest = "The quick brown fox jumps over the lazy dog";

Scanner sc= new Scanner(System.in);

System.out.print("Enter String: ");

String valueToDigest= sc.nextLine();

final String ValueText = valueToDigest;

Scanner kc = new Scanner(System.in);

System.out.print("Enter Secret Key: ");

String keyO= kc.nextLine();

byte[] key = keyO.getBytes();

practical7 hm = new practical7();

String messageDigest = hm.generateHmac256(ValueText, key);

System.out.println(messageDigest);

}}

**OUTPUT**

run:

Enter String: hi my name is Shubham and hi again

Enter Secret Key: secret

b831742b4500937856ea8244380dc7f007e8f48f5b24289058d51f718db36de7

BUILD SUCCESSFUL (total time: 13 seconds)