Practical 8

Name:Satishkumar Rajan Nadar

Aim Hmac

package inspractical8;

import java.security.InvalidKeyException;

import java.security.NoSuchAlgorithmException;

import java.util.Formatter;

import javax.crypto.Mac;

import javax.crypto.spec.SecretKeySpec;

public class INSPractical8 {

private static final String HMAC\_SHA1\_ALGORITHM = "HmacSHA1";

private static String toHexString(byte[] bytes){

Formatter formatter = new Formatter();

for (byte b: bytes){

formatter.format("%02x", b);

}

return formatter.toString();

}

public static String calculateRFC2104HMAC(String data, String key) throws NoSuchAlgorithmException, InvalidKeyException {

SecretKeySpec signingkey = new SecretKeySpec(key.getBytes(),HMAC\_SHA1\_ALGORITHM);

Mac mac =Mac.getInstance(HMAC\_SHA1\_ALGORITHM);

mac.init(signingkey);

return toHexString(mac.doFinal(data.getBytes()));

}

public static void main(String[] args) throws Exception {

String hmac = calculateRFC2104HMAC("data","key");

System.out.println(hmac);

assert hmac.equals("104152c5bfdca07bc633eebd46199f0255c9f49d");

}

}

