**EX.No.9 DIGITAL SIGNATURE STANDARD (DSS)**

**CODE:**

import java.security.KeyPair;

import java.security.KeyPairGenerator;

import java.security.PrivateKey;

import java.security.PublicKey;

import java.security.SecureRandom;

import java.security.Signature;

import java.util.\*;

public class DSS {

String message,sign;

private static final String SIGNING\_ALGORITHM = "SHA256withRSA";

private static final String RSA = "RSA";

public KeyPair Generate\_RSA\_KeyPair() throws Exception

{

KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance(RSA);

keyPairGenerator.initialize(2048);

return keyPairGenerator.generateKeyPair();

}

public byte[] Create\_Digital\_Signature(byte[] msg, PrivateKey prKey) throws Exception

{

Signature signature = Signature.getInstance(SIGNING\_ALGORITHM);

signature.initSign(prKey);

signature.update(msg);

return signature.sign();

}

public boolean Verify\_Digital\_Signature(byte[] msg,byte[] signatureToVerify,PublicKey puKey) throws Exception

{

Signature signature = Signature.getInstance(SIGNING\_ALGORITHM);

signature.initVerify(puKey);

signature.update(msg);

return signature.verify(signatureToVerify);

}

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

{

Scanner sc = new Scanner(System.in);

System.out.println("\nDIGITAL SIGNATURE STANDARD");

System.out.println("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*");

DSS dss = new DSS();

System.out.println("\nGeneration of digital signature");

System.out.println("-------------------------------");

System.out.print("\nEnter the message: ");

dss.message=sc.nextLine();

KeyPair keyPair = dss.Generate\_RSA\_KeyPair();

byte[] signature = dss.Create\_Digital\_Signature(dss.message.getBytes(),keyPair.getPrivate());

System.out.println("\nDigital Signature is (in Base-64 format):\n\n"+ Base64.getEncoder().encodeToString(signature));

System.out.println("\nVerification of digital signature");

System.out.println("---------------------------------");

//sc.next();

System.out.print("\nEnter the message: ");

dss.message=sc.nextLine();

//sc.nextLine();

System.out.print("\nEnter the signature (in Base-64 format): ");

dss.sign=sc.next();

System.out.println("\nThe given digital signature is verified to be "+ dss.Verify\_Digital\_Signature(dss.message.getBytes(),Base64.getDecoder().decode(dss.sign), keyPair.getPublic()));

}

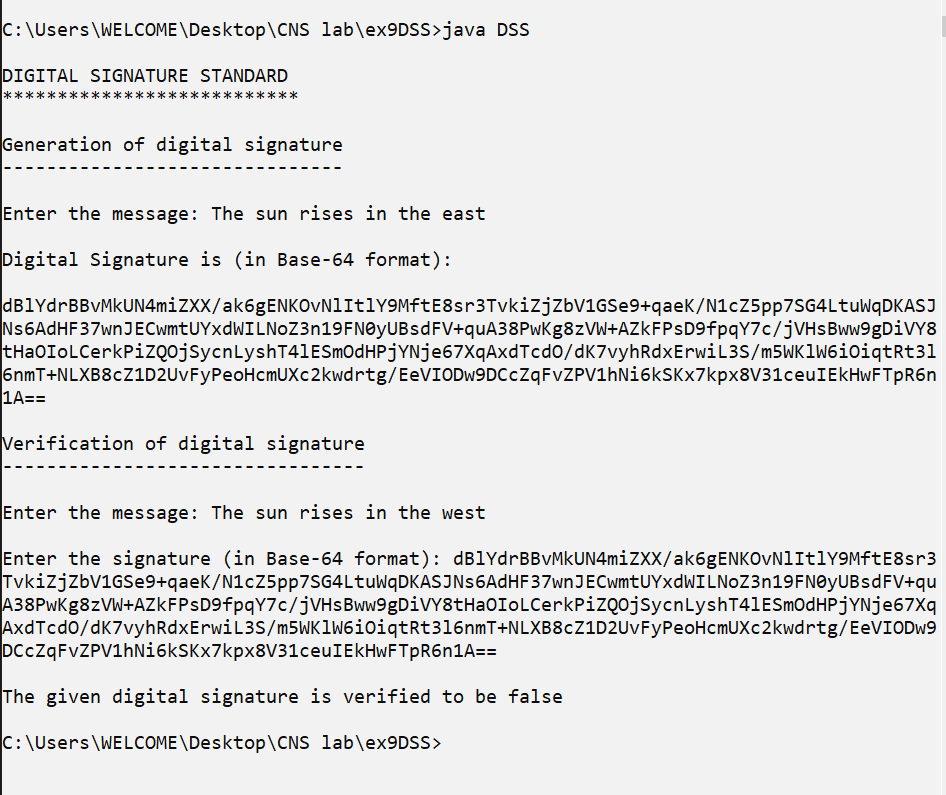
}

**OUTPUT:**

Example 1:



Example 2: (Modified message)



Example 3: (Modified signature)

