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.getPrivat
e());
        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.getDecod
er().decode(dss.sign), keyPair.getPublic()));
    }
}
```

OUTPUT:

Example 1:

```
C:\Users\WELCOME\Desktop\CNS lab\ex9DSS>javac DSS.java

C:\Users\WELCOME\Desktop\CNS lab\ex9DSS>java DSS

DIGITAL SIGNATURE STANDARD
**************************

Generation of digital signature
-------------------------------

Enter the message: Hello World

Digital Signature is (in Base-64 format):

QRIVCoAY4cw7nsWM2KOuEP91fWuRoDT2ldMtf1Iko3GZFryZthUA0EcMkHaE/mWLr2ddkSUZICQKg+Vi6YNFx
1Hei8Y1x54Xt6tw+KHKNzks0XPldU0t8dRx8kEJeoN8ZbjaZyVbP3/ene1m00cjSP3fiI4LZxVdzUjQ/oK7Ir
jlNPRWE7GnRXq/UlNvlkGdKFoC3E/ApdSh0Xosn83vFRBlSMWboiI9GYVCLsppdvdyyDBXWtyOc6eqrH7krIp
jzlcEhWtwtIxCD+AGcRBZh/+nvyouqCCh7ypUsEu1QuwKem1LiD4bDotcdxB+b0mCFeFUTpieg3Dzo6BvGWfz
Lw==

Verification of digital signature
---------------------------------

Enter the message: Hello World

Enter the signature (in Base-64 format): QRIVCoAY4cw7nsWM2KOuEP91fWuRoDT2ldMtf1Iko3GZ
FryZthUA0EcMkHaE/mWLr2ddkSUZICQKg+Vi6YNFx1Hei8Y1x54Xt6tw+KHKNzks0XPldU0t8dRx8kEJeoN8Z
bjaZyVbP3/ene1m00cjSP3fiI4LZxVdzUjQ/oK7IrjlNPRWE7GnRXq/UlNvlkGdKFoC3E/ApdSh0Xosn83vFR
BlSMWboiI9GYVCLsppdvdyyDBXWtyOc6eqrH7krIpjzlcEhWtwtIxCD+AGcRBZh/+nvyouqCCh7ypUsEu1Quw
Kem1LiD4bDotcdxB+b0mCFeFUTpieg3Dzo6BvGWfzLw==

The given digital signature is verified to be true

C:\Users\WELCOME\Desktop\CNS lab\ex9DSS>
```

Example 2: (Modified message)

```
C:\Users\WELCOME\Desktop\CNS lab\ex9DSS>java DSS

DIGITAL SIGNATURE STANDARD
**************************

Generation of digital signature
-------------------------------

Enter the message: The sun rises in the east

Digital Signature is (in Base-64 format):

dBlYdrBBvMkUN4miZXX/ak6gENKOvNlItlY9MftE8sr3TvkiZjZbV1GSe9+qaeK/N1cZ5pp7SG4LtuWqDKASJ
Ns6AdHF37wnJECwmtUYxdWILNoZ3n19FN0yUBsdFV+quA38PwKg8zVW+AZkFPsD9fpqY7c/jVHsBww9gDiVY8
tHaOIoLCerkPiZQOjSycnLyshT4lESmOdHPjYNje67XqAxdTcdO/dK7vyhRdxErwiL3S/m5WKlW6iOiqtRt3l
6nmT+NLXB8cZ1D2UvFyPeoHcmUXc2kwdrtg/EeVIODw9DCcZqFvZPV1hNi6kSKx7kpx8V31ceuIEkHwFTpR6n
1A==

Verification of digital signature
---------------------------------

Enter the message: The sun rises in the west

Enter the signature (in Base-64 format): dBlYdrBBvMkUN4miZXX/ak6gENKOvNlItlY9MftE8sr3
TvkiZjZbV1GSe9+qaeK/N1cZ5pp7SG4LtuWqDKASJNs6AdHF37wnJECwmtUYxdWILNoZ3n19FN0yUBsdFV+qu
A38PwKg8zVW+AZkFPsD9fpqY7c/jVHsBww9gDiVY8tHaOIoLCerkPiZQOjSycnLyshT4lESmOdHPjYNje67Xq
AxdTcdO/dK7vyhRdxErwiL3S/m5WKlW6iOiqtRt3l6nmT+NLXB8cZ1D2UvFyPeoHcmUXc2kwdrtg/EeVIODw9
DCcZqFvZPV1hNi6kSKx7kpx8V31ceuIEkHwFTpR6n1A==

The given digital signature is verified to be false

C:\Users\WELCOME\Desktop\CNS lab\ex9DSS>
```

Example 3: (Modified signature)

```
C:\Users\WELCOME\Desktop\CNS lab\ex9DSS>java DSS

DIGITAL SIGNATURE STANDARD
**************************

Generation of digital signature
-------------------------------

Enter the message: Good Morning!

Digital Signature is (in Base-64 format):

E3/Pf1g5VG+UACLwns9C7rbCDi/qEdHHthD6P+UY7WIlHQheAc9Trmg4hT7MjsMWs7qTWMcF+sScJ2y7bAhtR
DskEjp8wi1RiAQaYv8m51qn8jDJ0XtSKqAdRGHojXp2F2BGLHD6G0QbI7SOmAe42Pj7bkSmlwF1YheuHOdFEK
uoDyF2A6fQLThDpQn1GHYSmPsUv/6infOnivIuSX/SmFJfixbQAqDj8sSPC8VA71SmwteaNOoFe/lyBibSFp/
7j6fJgssYiwXbs1f/EK6h1P1JnMhFluZ/ZpQkkM1qygzftQwZ72iLNCXMC8UenzmXTE7hfI8YKOS7YVpc4llJ
uw==

Verification of digital signature
---------------------------------

Enter the message: Good Morning!

Enter the signature (in Base-64 format): E3/Pf1g5VG+UACLwns9C7rbCDi/qEdHHthD6P+UY7WIl
HQheAc9Trmg4hT7MjsMWs7qTWMcF+sScJ2y7bAhtRDskEjp8wi1RiAQaYv8m51qn8jDJ0XtSKqAdRGHojXp2F
2BGLHD6G0QbI7SOmAe42Pj7bkSmlwF1YheuHOdFEKuoDyF2A6fQLThDpQn1GHYSmPsUv/6infOnivIuSX/SmF
JfixbQAqDj8sSPC8VA71SmwteaNOoFe/lyBibSFp/7j6fJgssYiwXbs1f/EK6h1P1JnMhFluZ/ZpQkkM1qygz
ftQwZ72iLNCXMC8UenzmXTE7hfI8YKOS7YVpc4lEEEE==

The given digital signature is verified to be false

C:\Users\WELCOME\Desktop\CNS lab\ex9DSS>
```