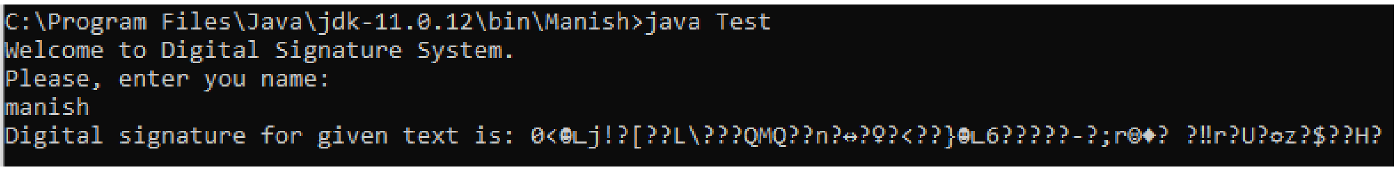
Java Security

Signature Creation

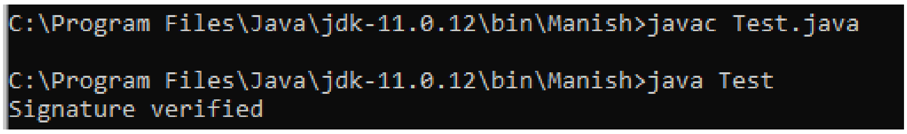
```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.Signature;
import java.util.Scanner;

public class Test
{
        public static void main(String args[]) throws Exception
        {
                //Accepting text from user
                Scanner sc = new Scanner(System.in);
                System.out.println("Welcome to Digital Signature System. \nPlease, enter you name:");
                String text = sc.nextLine();

                //Creating KeyPair generator object
                KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DSA");

                //Initializing the key pair generator
                keyPairGen.initialize(2048);

                //Generate the pair of keys
                KeyPair pair = keyPairGen.generateKeyPair();

                //Getting the private key from the key pair
                PrivateKey privKey = pair.getPrivate();

                //Creating a Signature object
                Signature s1 = Signature.getInstance("SHA256withDSA");

                //Initialize the signature
                s1.initSign(privKey);
                byte[] bytes = text.getBytes();

                //Adding data to the signature
                s1.update(bytes);

                //Calculating the signature
                byte[] signature = s1.sign();

                //Printing the signature
                System.out.println("Digital signature for given text is: "+new String(signature, "UTF8"));
  }
}
```



```
C:\Program Files\Java\jdk-11.0.12\bin\Manish>java Test
Welcome to Digital Signature System.
Please, enter you name:
manish
Digital signature for given text is: 0<☻└j!?[??L\???QMQ??n?↔?♀?<??}☻└6?????-?;r☺♦? ?‼r?U?☼z?$??H?
```

Signature Verification

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.Signature;

import java.util.Scanner;

public class Test
{
        public static void main(String args[]) throws Exception
        {
                //Creating KeyPair generator object
                KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DSA");

                //Initializing the key pair generator
                keyPairGen.initialize(2048);

                //Generate the pair of keys
                KeyPair pair = keyPairGen.generateKeyPair();

                 //Getting the privatekey from the key pair
                PrivateKey privKey = pair.getPrivate();

                //Creating a Signature object
                Signature sign = Signature.getInstance("SHA256withDSA");

                //Initializing the signature
                sign.initSign(privKey);
                byte[] bytes = "Manish Mathuria".getBytes();

                //Adding data to the signature
                sign.update(bytes);

                //Calculating the signature
                byte[] signature = sign.sign();

                //Initializing the signature
                sign.initVerify(pair.getPublic());
                sign.update(bytes);

                //Verifying the signature
                boolean bool = sign.verify(signature);

                if(bool)
                {
                        System.out.println("Signature verified");
                }
                else
                {
                        System.out.println("Signature failed");
                }
        }
}
```



```
C:\Program Files\Java\jdk-11.0.12\bin\Manish>javac Test.java

C:\Program Files\Java\jdk-11.0.12\bin\Manish>java Test
Signature verified
```