

faizanPrac5.java

```
1  package practical5;
2  import java.security.KeyPairGenerator;
3  import java.io.*;
4  import java.security.*;
5  public class Practical5 {
6      public static void main(String[] args) {
7          // TODO code application logic here
8          if(args.length == 1){
9              System.out.println("usage : name of the file to sign ");
10         }
11         else try{
12             KeyPairGenerator keyGen = KeyPairGenerator.getInstance("DSA", "SUN");
13             SecureRandom random = SecureRandom.getInstance("SHA1PRNG", "SUN");
14             keyGen.initialize(1024, random);
15             KeyPair pair = keyGen.generateKeyPair();
16             PrivateKey priv = pair.getPrivate();
17             PublicKey pub = pair.getPublic();
18             Signature dsa = Signature.getInstance("SHA1withDSA", "SUN");
19             dsa.initSign(priv);
20
21             FileInputStream fis = new FileInputStream("D:\\TYCS\\502_INS\\Practical-5\\Pract-
5\\Practical5\\src\\practical5\\Digital.txt");
22             BufferedInputStream bufin = new BufferedInputStream(fis);
23             byte[] buffer = new byte[1024];
24             int len;
25             while(bufin.available() != 0){
26                 len = bufin.read(buffer);
27                 dsa.update(buffer, 0, len);
28             };
29             bufin.close();
30
31             byte[] realSig = dsa.sign();
32             FileOutputStream sigfos = new FileOutputStream("D:\\TYCS\\502_INS\\Practical-
5\\Pract-5\\Practical5\\src\\practical5\\Digi.txt");
33             sigfos.write(realSig);
34             sigfos.close();
35
36             byte[] key = pub.getEncoded();
37             FileOutputStream keyfos = new FileOutputStream("D:\\TYCS\\502_INS\\Practical-
5\\Pract-5\\Practical5\\src\\practical5\\Digi.txt");
38             keyfos.write(key);
39             keyfos.close();
40
41         }
42         catch(Exception e)
43         {
44             System.err.println("Caught exception"+e.toString());
45         }
46     };
47 }
48
```