**Practical 5**

**Theory:**

**1 page full theory on Digital Signature**

**Code:**

package com.mycompany.tycs.rehmah;

import java.io.\*;

import java.security.\*;

public class Prac5 {

public static void main(String args[]){

if(args.length==1){

System.out.println("Usage: nameOfFileToSign");

}

else try{

KeyPairGenerator keyGen=KeyPairGenerator.getInstance("DSA","SUN");

SecureRandom random=SecureRandom.getInstance("SHA1PRNG","SUN");

keyGen.initialize(1024, random);

KeyPair pair=keyGen.generateKeyPair();

PrivateKey priv=pair.getPrivate();

PublicKey pub=pair.getPublic();

Signature dsa=Signature.getInstance("SHA1withDSA","SUN");

dsa.initSign(priv);

FileInputStream fis=new FileInputStream("D:\\Digital Signature Demo\\digital.txt");

BufferedInputStream bis=new BufferedInputStream(fis);

byte[] buffer=new byte[1024];

int len;

while(bis.available()!=0){

len=bis.read(buffer);

dsa.update(buffer,0,len);

}

bis.close();

byte[] realSig=dsa.sign();

FileOutputStream fos=new FileOutputStream("D:\\Digital Signature Demo\\signature.txt");

fos.write(realSig);

fos.close();

byte[] key=pub.getEncoded();

FileOutputStream keyfos=new FileOutputStream("D:\\Digital Signature Demo\\publickey.txt");

keyfos.write(key);

keyfos.close();

}catch(Exception e){

System.out.println("Caught Exception:"+e.toString());

}

}

}