DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

CNS WORKSHOP LABORATORY MANUAL

Subject Code : **CS407PC**
Regulation : R18/JNTUH
Academic Year : 2020-2021

IV B. TECH I SEMESTER

COMPUTER SCIENCE AND ENGINEERING

KG REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

Affiliated o JNTUH, Chilkur,(V), Moinabad(M) R. R Dist, TS-501504

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

VISION AND MISSION OF THE INSTITUTION

VISION

To become self-sustainable institution this is recognized for its new age engineering through innovative teaching and learning culture, inculcating research and entrepreneurial ecosystem, and sustainable social impact in the community.

MISSION

- To offer undergraduate and post-graduate programs that is supported through industry relevant curriculum and innovative teaching and learning processes that would help students succeed in their professional careers.
- To provide necessary support structures for students, this will contribute to their personal and professional growth and enable them to become leaders in their respective fields.
- To provide faculty and students with an ecosystem that fosters research and development through strategic partnerships with government organisations and collaboration with industries.
- To contribute to the development of the region by using our technological expertise to work with nearby communities and support them in their social and economic growth.

VISION AND MISSION OF CSE DEPARTMENT

VISION

To be recognized as a department of excellence by stimulating a learning environment in which students and faculty will thrive and grow to achieve their professional, institutional and societal goals.

MISSION

- To provide high quality technical education to students that will enable life-long learning and build expertise in advanced technologies in Computer Science and Engineering.
- To promote research and development by providing opportunities to solve complex engineering problems in collaboration with industry and government agencies.
- To encourage professional development of students that will inculcate ethical values and leadership skills while working with the community to address societal issues.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

PROGRAM EDUCATIONAL OBJECTIVES (PEOS):

A graduate of the Computer Science and Engineering Program should:

PEO1	**Program Educational Objective1: (PEO1)** The Graduates will provide solutions to difficult and challenging issues in their profession by applying computer science and engineering theory and principles.
PEO2	**Program Educational Objective2 :(PEO2)** **The** Graduates have successful careers in computer science and engineering fields or will be able to successfully pursue advanced degrees.
PEO3	**Program Educational Objective3: (PEO3)** The Graduates will communicate effectively, work collaboratively and exhibit high levels of Professionalism, moral and ethical responsibility.
PEO4	**Program Educational Objective4 :(PEO4)** **The** Graduates will develop the ability to understand and analyse Engineering issues in a broader perspective with ethical responsibility towards sustainable development.

PROGRAM OUTCOMES (POS):

PO1	**Engineeringknowledge**:Applytheknowledgeofmathematics,science,engineering Fundamentals andanengineeringspecializationtothesolutionofcomplexengineeringproblems.
PO2	**Problem analysis**: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3	**Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO4	**Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5	**Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
PO6	**The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO7	**Environment and sustainability**: Understand the impact of the professional engineering Solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
PO8	**Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO9	**Individual and team work**: Function effectively as an individual, and as a member or leader In diverse teams, and in multi-disciplinary settings.
PO10	**Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
PO11	**Project management and finance**: Demonstrate knowledge and understanding of the Engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO12	**Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES(PSOS):

PSO1	**Problem Solving Skills** – Graduate will be able to apply computational techniques and software principles to solve complex engineering problems pertaining to software engineering.
PSO2	**Professional Skills** – Graduate will be able to think critically, communicate effectively, and collaborate in teams through participation in co and extra-curricular activities.
PSO3	**Successful Career** – Graduates will possess a solid foundation in computer science and engineering that will enable them to grow in their profession and pursue lifelong learning through post-graduation and professional development.

INDEX

1. XORastringwithaZero

AIM: Write a C programthatcontainsastring(charpointer)withavalue \Hello World'.TheprogramshouldXOReachcharacterinthisstringwith0anddisplay theresult.

PROGRAM:

```
#include<stdlib.h>main()
{
charstr[]="HelloWorld";charstr1[11];
int
i,len;len=strlen(str);for(i=0;i<len;i++
)
{
str1[i]=str[i]^0;printf("%c",str1[i]);
}
printf("\n");
}
```

Output:

```
HelloWorldHelloWorld
```

2. XORastringwitha127

AIM: WriteaCprogramthatcontainsastring(charpointer)withavalue \Hello World'.TheprogramshouldANDorandXOReachcharacterinthisstringwith127 and displaytheresult.

PROGRAM:

```
#include<stdio.h>
#include<stdlib.h>voidmain()
{
        charstr[]="HelloWorld";charstr1
        [11];
        charstr2[11]=str[];inti,le
        n;
        len=strlen(str);
        for(i=0;i<len;i++)
        {
            str1[i]=str[i]&127;printf(
            "%c",str1[i]);
        }
            printf("\n");
        for(i=0;i<len;i++)
        {
            str3[i]=str2[i]^127;printf("
            %c",str3[i]);
        }
            printf("\n");
}
```

Output:

```
HelloWorld
HelloWorldHelloWorld
```

3. Encryption&DecryptionusingCipherAlgorithms

AIM: WriteaJavaprogramtoperformencryptionanddecryptionusingthefollowingalgorithms:

a) CeaserCipher
b) SubstitutionCipher
c) HillCipher

PROGRAM:

d) CeaserCipher

```
importjava.io.BufferedReader;importjava.io.IO
Exception;
importjava.io.InputStreamReader;import
java.util.Scanner;

publicclassCeaserCipher {

staticScannersc=newScanner(System.in);
        staticBufferedReaderbr=newBufferedReader(newInputStreamReader(System.in));publicstaticvoidmain(St
        ring[]args)throwsIOException{
            //TODOcodeapplicationlogichere

        System.out.print("EnteranyString:");Stringstr=br.
            readLine();
System.out.print(" \nEntertheKey:");intkey=sc.nextInt();
            String encrypted = encrypt(str,
        key);System.out.println("\nEncryptedStringis:"+encrypted);

            Stringdecrypted=decrypt(encrypted,key);System.out.println("\nDecrypte
        dStringis:"
+decrypted);System.out.println("\n");
            }

publicstaticStringencrypt(String str,intkey)
```

```
        { String encrypted =
"";for(inti=0;i<str.length();i++){intc=str.charAt(i);
if(Character.isUpperCase(c)){
                        c=c+(key%26);
                if(c>'Z')
                        c=c-26;
                }
elseif(Character.isLowerCase(c)){
                        c=c+(key%26);
                if(c>'z')
                        c=c-26;
                }
encrypted+=(char)c;
                }
            returnencrypted;
            }
public staticStringdecrypt(String str,int key)
        { String decrypted =
"";for(inti=0;i<str.length();i++){intc=str.charAt(i);
if(Character.isUpperCase(c)){
                        c=c-(key%26);
                if(c<'A')
                        c=c+26;
                }
elseif(Character.isLowerCase(c)){
                        c=c-(key%26);
                 if(c<'a')
                        c=c+26;
                }
```

```
decrypted+=(char)c;
                }
        returndecrypted;
            }
}
```

Output:

```
EnteranyString:HelloWorldEnterthe
Key:5
EncryptedString
is:MjqqtBtwqiDecryptedStringis:Hello
World
```

b) SubstitutionCipher

PROGRAM:

```
import
java.io.*;importjava.
util.*;
publicclassSubstitutionCipher{
staticScannersc=newScanner(System.in);
staticBufferedReaderbr=newBufferedReader(newInputStreamReader(System.in));publicstaticvoidmain(St
ring[]args)throwsIOException{
  //TODOcodeapplicationlogichereStringa="abcdefghij
klmnopqrstuvwxyz";Stringb="zyxwvutsrqponmlkjihgfe
dcba";
System.out.print("Enteranystring:");Stringstr=b
r.readLine();
Stringdecrypt="";charc;
for(inti=0;i<str.length();i++)
{
c=str.charAt(i);intj=a.indexOf(
c);
decrypt=decrypt+b.charAt(j);
}
System.out.println("Theencrypteddatais:"+decrypt);
}
}
```

Output:

```
Enterany string:aceho
Theencrypteddatais:zxvsl
```

a)

HillCiphe

rPROGRAM:

```
 importjava.io.*;
import
java.util.*;importjava.io.*;publicclass
HillCipher{
        staticfloat[][]decrypt=newfloat[3][1];staticfloat[][
        ]a=newfloat[3][3];staticfloat[][] b = new
        float[3][3]; staticfloat[][] mes = new
        float[3][1]; staticfloat[][]res=newfloat[3][1];
static BufferedReader br = new
BufferedReader(newInputStreamReader(System.in));staticScannersc=newScanner(System.in);publicstati
cvoidmain(String[] args)throws IOException{
            //TODOcodeapplicationlogicheregetke
        ymes();
for(inti=0;i<3;i++)for(intj=0;j<1;j++)for(int k=0;k<3;k++)
{res[i][j]=res[i][j]+a[i][k]*mes[k][j]; }System.out.print("
\nEncryptedstringis:"); for(int i=0;i<3;i++)
{System.out.print((char)(res[i][0]%26+97));res[i][0]=res[i][0];

            }
inverse();
        for(int
        i=0;i<3;i++)for(intj=0;j<1;j
        ++)for(intk=0;k<3;k++){
        decrypt[i][j]=decrypt[i][j]+b[i][k]*res[k][j];}System.out.prin
        t("\nDecryptedstringis:");
```

```
        for(int
        i=0;i<3;i++){System.out.print((char)(decrypt[i][0]%26+97)
        );
                }
        System.out.print("\n");
            }
public static void getkeymes() throws IOException
{System.out.println("Enter3x3matrixforkey(Itshouldbeinversible):");for(inti=0;i<3;i++)
        for(intj=0;j<3;j++)a[i][j]=sc.
        nextFloat();
        System.out.print("\nEntera3letterstring:");Stringmsg=br.rea
                dLine();
for(inti=0;i<3;i++)
mes[i][0]=msg.charAt(i)-97;
            }
publicstaticvoidinverse(){floatp,q;
float[][] c =
a;for(inti=0;i<3;i++)for(intj=0;j<3;j
++){
                        //a[i][j]=sc.nextFloat();
if(i==j)b[i][j]=1;
elseb[i][j]=0;
                    }
for(intk=0;k<3;k++){for(inti=0;i<3;i++){
                        p=c[i][k];
              q=c[k][k];for(intj=0;j<3
;j++){if(i!=k){
```

```
c[i][j]=c[i][j]*q-p*c[k][j];
b[i][j]=b[i][j]*q-p*b[k][j];
                                }}}}
for(inti=0;i<3;i++)for(intj=0;j<3;j++){
b[i][j]=b[i][j]/c[i][i]; }
        System.out.println("");
System.out.println("\nInverseMatrixis:");for(inti=0;i<3;i++){
        for(int
        j=0;j<3;j++)System.out.print(b[i][j]+"
        ");
        System.out.print("\n");}
            }}
```

Output:

```
Enter a 3 letter string:
haiEncrypted string is
:fdxInverseMatrix is:
0.0833333360.41666666-0.33333334
-0.41666666-0.0833333360.6666667
0.5833333-0.083333336-0.33333334
Decryptedstringis:hai
```

4. JavaprogramforDESalgorithmlogic

AIM: WriteaJavaprogramtoimplementtheDESalgorithmlogic.

PROGRAM:

```
importjava.util.*;
import
java.io.BufferedReader;importjava.io.InputStreamRe
ader;importjava.security.spec.KeySpec;importjavax.cr
ypto.Cipher;importjavax.crypto.SecretKey;
import
javax.crypto.SecretKeyFactory;importjavax.crypto.spec.DESe
deKeySpec;importsun.misc.BASE64Decoder;
importsun.misc.BASE64Encoder;public classDES{
privatestaticfinalStringUNICODE_FORMAT="UTF8";
publicstaticfinalStringDESEDE_ENCRYPTION_SCHEME="DESede";privateKeySpecmyKeyS
pec;privateSecretKeyFactorymySecretKeyFactory;
privateCiphercipher;byte[]keyAsByt
es;
privateStringmyEncryptionKey;privateStringmyEncrypt
ionScheme;SecretKeykey;
        static BufferedReader br = new
        BufferedReader(newInputStreamReader(System.in));publicDES()throwsException{
            //TODOcodeapplicationlogicheremyEncryptionKey
        ="ThisIsSecretEncryptionKey";myEncryptionScheme=DESEDE_ENCRYPTION_SCHEME;keyAsByte
        s=
myEncryptionKey.getBytes(UNICODE_FORMAT);
myKeySpec=newDESedeKeySpec(keyAsBytes);
        mySecretKeyFactory=SecretKeyFactory.getInstance(myEncryptionScheme);
        cipher=Cipher.getInstance(myEncryptionScheme);
        key=mySecretKeyFactory.generateSecret(myKeySpec);

            }
publicStringencrypt(StringunencryptedString)
                {StringencryptedString=null;
try{
cipher.init(Cipher.ENCRYPT_MODE,key);
        byte[]plainText=unencryptedString.getBytes(UNICODE_FORMAT);byte[]encrypte
        dText= cipher.doFinal(plainText);
```

```
BASE64Encoderbase64encoder=newBASE64Encoder();encryptedString=base64enc
oder.encode(encryptedTe xt);}catch(Exceptione){
        e.printStackTrace();
        }returnencryptedString;}
publicStringdecrypt(StringencryptedString)
                {StringdecryptedText=null;
try{
cipher.init(Cipher.DECRYPT_MODE,key);
                    BASE64Decoder base64decoder = new
        BASE64Decoder();byte[]encryptedText=base64decoder.decodeBuffer(encryptedString)
        ;byte[]plainText=cipher.doFinal(encryptedText);decryptedText=bytes2String(plainText
        );}
catch (Exception e)
{e.printStackTrace();}returndecryptedT
ext;}
privatestaticStringbytes2String(byte[]bytes)
{StringBufferstringBuffer=new
        StringBuffer();for(inti=0;i<bytes.length;
        i++){stringBuffer.append((char)bytes[i]);}returnstringBuffer.toString();}
publicstaticvoidmain(Stringargs[])throwsException
        { System.out.print("Enter the string:
            ");DESmyEncryptor=newDES();
            StringstringToEncrypt=br.readLine();
            String encrypted = myEncryptor.encrypt(stringToEncrypt);String decrypted =
            myEncryptor.decrypt(encrypted);System.out.println("\nStringToEncrypt:"+strin
            gToEncrypt);System.out.println("\nEncryptedValue:"+encrypted);
            System.out.println("\nDecryptedValue:"+decrypted);System.out.println("");
        }
}
```

OUTPUT:

```
Enter the string:
WelcomeStringToEncrypt:Welcom
e
EncryptedValue:BPQMwc0wKvg=DecryptedVa
lue:Welcome
```

5. ProgramtoimplementBlowFishalgorithmlogic

AIM: WriteaC/JAVAprogramtoimplementtheBlowFishalgorithmlogic.

PROGRAM:

```
importjava.io.*;
importjava.io.FileInputStream;importjava.io.FileO
utputStream;importjava.security.Key;
importjavax.crypto.Cipher;
importjavax.crypto.CipherOutputStream;importjavax.crypto.KeyGen
erator;
importsun.misc.BASE64Encoder;public
classBlowFish{
publicstaticvoidmain(String[]args)throwsException{
        //TODOcodeapplicationlogichereKeyGenerat
    orkeyGenerator=
    KeyGenerator.getInstance("Blowfish");keyGenerator.init(128);KeysecretKey=
    keyGenerator.generateKey();
    CiphercipherOut=Cipher.getInstance("Blowfish/CFB/NoPadding");cipherOut.init(Ci
    pher.E NCRYPT_MODE, secretKey); BASE64Encoderencoder=new
    BASE64Encoder();
    byteiv[]=cipherOut.getIV();if
    (iv!=null){
     System.out.println("InitializationVectoroftheCipher:"+encoder.encode(iv)); }
FileInputStream fin = new FileInputStream("inputFile.txt");FileOutputStreamfout = new
FileOutputStream("outputFile.txt");CipherOutputStreamcout=newCipherOutputStream(fout,cipherO
ut);intinput= 0;
while((input=fin.read())!=-1){cout.write(input);}

fin.close();cout.close(); }}
```

OUTPUT:

```
InitializationVectoroftheCipher:dI1MXzW97oQ=ContentsofinputFil
e.txt:Hello World
ContentsofoutputFile.txt:ùJÖ˜NåI“
```

6. ProgramtoimplementRijndaelalgorithmlogic

AIM: WriteaC/JAVAprogramtoimplementtheRijndaelalgorithmlogic.

PROGRAM:

```
import java.security.*;import
javax.crypto.*;importjavax.crypto.s
pec.*;importjava.io.*;
publicclassAES{
publicstaticStringasHex(bytebuf[]){
StringBufferstrbuf=newStringBuffer(buf.length*2);inti;
for(i=0;i<buf.length;i++){if(((int)buf[i
] &0xff)<0x10)strbuf.append("0");
strbuf.append(Long.toString((int)buf[i]&0xff,16));}returnstrbuf.toString
();}
publicstaticvoidmain(String[]args)throwsException
 {Stringmessage="AESstillrocks!!";
 //GettheKeyGenerator
 KeyGeneratorkgen=KeyGenerator.getInstance("AES");kgen.init(128);//
 192and256bitsmaynotbeavailable
 //Generatethesecretkey
 specs.SecretKeyskey=kgen.generateKey();byte
 []raw=skey.getEncoded();
 SecretKeySpecskeySpec=newSecretKeySpec(raw,"AES");
 //Instantiatethecipher
 Cipher cipher =
 Cipher.getInstance("AES");cipher.init(Cipher.ENCRYPT_MODE,sk
 eySpec);
byte[]encrypted=cipher.doFinal((args.length==0?message:
```

```
args[0]).getBytes()); System.out.println("encrypted string: "
+asHex(encrypted));cipher.init(Cipher.DECRYPT_MODE,skeySpec);byte[]original=ciph
er.doFinal(encrypted);

StringoriginalString=newString(original);

System.out.println("Originalstring:"+originalString+""+asHex(original));
}
 }
```

OUTPUT:

```
Inputyourmessage:HelloKGRCET
Encryptedtext:3ooo&&(*&*4r4Decrypted
text:Hello KGRCET
```

7. EncryptastringusingBlowFishalgorithm

AIM: UsingJavaCryptography,encryptthetext“Helloworld”usingBlowFish.Createyourownkeyusing Javaketytool.

PROGRAM:

```
importjavax.crypto.Cipher;importjavax.crypto.KeyG
enerator;import
javax.crypto.SecretKey;importjavax.swing.J
OptionPane;publicclassBlowFishCipher{
publicstaticvoidmain(String[]args)throwsException{
        //create a key generator based upon the Blowfish
    cipherKeyGeneratorkeygenerator=KeyGenerator.getInstance("Blowfish");
        //createakey
        //createa
        cipherbaseduponBlowfishCiphercipher=Cipher.getInstance("B
        lowfish");
        //initialise cipher to with secret
    keycipher.init(Cipher.ENCRYPT_MODE,secretkey);
        //getthetexttoencrypt
        StringinputText=JOptionPane.showInputDialog("Inputyourmessage:");//encryptmessage
byte[]encrypted=cipher.doFinal(inputText.getBytes());
        //re-
    initialisetheciphertobeindecryptmodecipher.init(Cipher.DECRY
    PT_MODE,secretkey);
        //decryptmessage
byte[]decrypted=cipher.doFinal(encrypted);
        //anddisplaytheresults
    JOptionPane.showMessageDialog(JOptionPane.getRootFrame(),
            "\nEncryptedtext:"+newString(encrypted)+"\n"+"\nDecryptedtext:"+newString(
            decrypted));
    System.exit(0);
      }}
```

OUTPUT:

```
Inputyourmessage:HelloworldEncrypted
text:3ooo&&(*&*4r4Decryptedtext:Hell
oworld
```

8. RSA Algorithm

AIM: WriteaJavaprogramtoimplementRSAAlgoithm.

PROGRAM:

```
import
java.io.BufferedReader;importjava.io.InputStreamReade
r;importjava.math.*;
import          java.util.Random;import
java.util.Scanner;publicclassRSA{
static          Scanner          sc          =          new
Scanner(System.in);publicstaticvoidmain(String[]args){
                //      TODO      code      application      logic
        hereSystem.out.print("EnteraPrimenumber:");
        BigInteger p = sc.nextBigInteger(); // Here's one
        primenumber..System.out.print("Enteranotherprime
        number:");BigIntegerq=sc.nextBigInteger();// ..andanother.
        BigIntegern=p.multiply(q);
        BigIntegern2=p.subtract(BigInteger.ONE).multiply(q.subtract(BigInteger.ONE));BigIntegere=generateE(
        n2);
        BigIntegerd=e.modInverse(n2);//Here'sthemultiplicativeinverse
        System.out.println("Encryptionkeys are: "+ e + ", "+ n);System.out.println("Decryptionkeysare:"+d+","+n);
            }
publicstaticBigIntegergenerateE(BigIntegerfiofn){inty,intGCD;
        BigIntegere;
        BigIntegergcd;
            Randomx=newRandom();
do{
```

```
                    y=x.nextInt(fiofn.intValue()-
                    1);Stringz=Integer.toString(y);
          e=newBigInteger(z);gc
d=fiofn.gcd(e);
intGCD=gcd.intValue();
                }
          while(y<=2||intGCD!=1
          );returne;
              }
}
```

OUTPUT:

```
EnteraPrimenumber:5
Enteranotherprime
number:11Encryptionkeys
are:33,55
Decryptionkeysare:17,55
```

9. Diffie-Hellman

AIM: ImplementtheDiffie-HellmanKeyExchangemechanismusingHTMLandJavaScript.Consideritastextchatbetweentwo heparties(Alice)andtheJavaScriptapplicationas otherparty (bob).

PROGRAM:

```
import
java.math.BigInteger;importjava.se
curity.KeyFactory;import
java.security.KeyPair;
importjava.security.KeyPairGenerator;impor
t java.security.SecureRandom;
importjavax.crypto.spec.DHParameterSpec;importja
vax.crypto.spec.DHPublicKeySpec;publicclass
DiffeHellman{
public final static int pValue =
47;public final static int gValue =
71;public final static int XaValue =
9;publicfinalstatic intXbValue=14;
publicstaticvoidmain(String[]args)throwsException
        {//TODOcodeapplicationlogichere
    BigInteg er p = new
    BigInteger(Integer.toString(pValue));BigInteger g = new
    BigInteger(Integer.toString(gValue));BigIntegerXa=new
BigInteger(Integer.toString(XaValue));BigIntegerXb=newBigInte
ger(Integer.toString(XbValue));createKey();intbitLength=512;//5
12bits
    SecureRandomrnd=newSecureRandom();
        p=BigInteger.probablePrime(bitLength,rnd
        );g=BigInteger.probablePrime(bitLength,rn
        d);

createSpecificKey(p,g);
        }
publicstaticvoidcreateKey()throwsException{
    KeyPairGeneratorkpg=KeyPairGenerator.getInstance("DiffieHellman");kpg.initialize(512);
    KeyPairkp=kpg.generateKeyPair();
    KeyFactorykfactory =
    KeyFactory.getInstance("DiffieHellman");DHPublicKeySpeckspec=(DHPublicKeySpec)k
    factory.getKeySpec(kp.getPublic(),DHPublicKeySpec.class);
    System.out.println("Publickeyis:"+kspec);
        }
    public static void createSpecificKey(BigInteger p, BigInteger g) throwsException
    {KeyPairGeneratorkpg
    =KeyPairGenerator.getInstance("DiffieHellman");DHParameterSpecparam=newDHPa
    rameterSpec(p,g);kpg.initialize(param);
    KeyPairkp=kpg.generateKeyPair();
    KeyFactorykfactory=KeyFactory.getInstance("DiffieHellman");
    DHPublicKeySpeckspec=(DHPublicKeySpec)kfactory.getKeySpec(kp.getPublic(),DHPubli
    cKeySpec.class);
    System.out.println("\nPublickeyis:"+kspec);
        }
}
```

OUTPUT:

Publickeyis:javax.crypto.spec.DHPublicKeySpec@5afd29Public
keyis:javax.crypto.spec.DHPublicKeySpec@9971ad

10. SHA-1

AIM: CalculatethemessagedigestofatextusingtheSHA-1algorithminJAVA.

PROGRAM:

```
importjava.security.*;p
ublicclassSHA1{
publicstaticvoidmain(String[]a){try {
        MessageDigestmd=MessageDigest.getInstance("SHA1");System
        .out.println("Message digest object info:
        ");System.out.println("Algorithm="+md.getAlgorithm());System.
        out.println("Provider="+md.getProvider());System.out.println("
        ToString="+md.toString());

         String input =
"";md.update(input.getBytes());by
te[]output=md.digest();System.ou
t.println();
        System.out.println("SHA1(\""+input+"\")="+bytesToHex(output));

input =
"abc";md.update(input.getBytes())
;output =
md.digest();System.out.println();
        System.out.println("SHA1(\""+input+"\")="+bytesToHex(output));

input="abcdefghijklmnopqrstuvwxyz";md.update(input.getBytes());
        output=md.di
        gest();Syste
        m.out.printl
        n();
        System.out.println("SHA1(\""+input+"\")="+bytesToHex(output));System.out.println("");}
catch(Exceptione){
        System.out.println("Exception:"+e);
            }
        }

publicstaticStringbytesToHex(byte[]b){
            charhexDigit[]={'0','1','2','3','4','5','6','7','8','9','A','B','C','D','E','F'};
StringBufferbuf=newStringBuffer();for (int
j=0; j<b.length; j++)
{buf.append(hexDigit[(b[j]>>4)&0x0f]);buf.ap
pend(hexDigit[b[j] & 0x0f]);
```

```
}returnbuf.toString();}
}
```

OUTPUT:

```
Message digest
  object
  info:Algorithm=
  SHA1
  Provider=SUNversion1.6
ToString = SHA1 Message Digest from SUN, <initialized> SHA1("")
=DA39A3EE5E6B4B0D3255BFEF95601890AFD80709SHA1("abc")
=A9993E364706816ABA3E25717850C26C9CD0D89D
SHA1("abcdefghijklmnopqrstuvwxyz")=32D10C7B8CF96570CA04CE37F2A19D84240D
3A89
```

11. MessageDigestAlgorithm5(MD5)

AIM: CalculatethemessagedigestofatextusingtheSHA-1algorithminJAVA.

PROGRAM:

```
importjava.security.*;p
ublic classMD5{
publicstaticvoidmain(String[]a){
        //TODOcodeapplicationlogichere
try{
        MessageDigestmd=MessageDigest.getInstance("MD5");System.
        out.println("Message digest object info:
        ");System.out.println("Algorithm=
        "+md.getAlgorithm());System.out.println("Provider="+md.getPr
        ovider());System.out.println("ToString="+md.toString());
         String input =
"";md.update(input.getBytes());
        byte[]output=md.dig
        est();System.out.pri
        ntln();
        System.out.println("MD5(\""+input+"\")="+bytesToHex(output));
input =
"abc";md.update(input.getBytes())
;output =
md.digest();System.out.println();
        System.out.println("MD5(\""+input+"\")="+bytesToHex(output));
input="abcdefghijklmnopqrstuvwxyz";md.update(input.getBytes());
        output=md.di
        gest();Syste
        m.out.printl
        n();
```

```
        System.out.println("MD5(\""+input+"\")="
+bytesToHex(output));System.out.println("");
                }
        catch(Exceptione){System.out.pri
        ntln("Exception:"+e);}
            }
publicstaticStringbytesToHex(byte[]b){
                charhexDigit[]={'0','1','2','3','4','5','6','7','8','9','A','B','C','D','E','F'};
StringBufferbuf=newStringBuffer();for (int
j=0; j<b.length; j++)
{buf.append(hexDigit[(b[j]>>4)&0x0f]);buf.ap
pend(hexDigit[b[j]&0x0f]);}
                returnbuf.toString();}}
```

OUTPUT:

```
        Messagedigestobject
          info:Algorithm=
          MD5
          Provider=SUNversion1.6
        ToString=MD5MessageDigestfromSUN,<initialized>MD5("")=D41D8CD98F00B204E98
        00998ECF8427EMD5("abc")=
900150983CD24FB0D6963F7D28E17F72MD5("abcdefghijklmnopqrstuvwxyz")
=C3FCD3D76192E4007DFB496CCA67E13B
```