

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING



CNS WORKSHOP LABORATORY MANUAL

Subject Code : **KG21CS624**

Regulation : **KG21**

Academic Year : **2023-2024**

III B. TECH II SEMESTER

COMPUTER SCIENCE AND ENGINEERING – DATA SCIENCE

KG REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

Affiliated to 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- DATA SCIENCE

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	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.
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

S.NO.	TOPIC	PAGE NUMBER
1	Write a C program that contains a string (char pointer) with a value 'HelloWorld'. The program should XOR each character in this string with 0 and display the result.	1
2	Write a C program that contains a string (char pointer) with a value 'HelloWorld'. The program should AND or XOR each character in this string with 127 and display the result.	2
3	Write a Java program to perform encryption and decryption using the following algorithms: <ul style="list-style-type: none"> a) Ceaser Cipher b) Substitution Cipher c) Hill Cipher 	3-9
4	Write a Java program to implement the DES algorithm logic.	10-12
5	Write a C/JAVA program to implement the Blowfish algorithm logic.	13-14
6	Write a C/JAVA program to implement the Rijndael algorithm logic.	15
7	Using Java Cryptography, encrypt the text "Helloworld" using Blowfish. Create your own key using Java keytool.	17-18
8	Write a Java program to implement RSA Algorithm.	19
9	Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as the other party (Bob).	21-22
10	Calculate the message digest of a text using the SHA-1 algorithm in JAVA.	23-24
11	Calculate the message digest of a text using the SHA-1 algorithm in JAVA.	25-26

1. XOR a string with a Zero

AIM: Write a C program that contains a string (char pointer) with a value

\Hello

World'. The program should XOR each character in this string with 0 and display the result.

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: Write a C program that contains a string (char pointer) with a value

\\Hello

World'. The program should AND or XOR each character in this string with 127 and display the result.

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: Write a Java program to perform encryption and decryption using the following algorithms:

- a) CeaserCipher
- b) SubstitutionCipher
- c) HillCipher

PROGRAM:

d) CeaserCipher

```
import java.io.BufferedReader; import java.io.IOException;
import java.io.InputStreamReader; import java.util.Scanner;

public class CeaserCipher {

    static Scanner sc = new Scanner(System.in);
    static BufferedReader br = new BufferedReader(new InputStreamReader(System.in));

    public static void main(String[] args) throws IOException {
        // TODO code application logic here

        System.out.print("Enter any String:"); String str = br.readLine();
        System.out.print(" \nEnter the Key:"); int key = sc.nextInt();

        String encrypted = encrypt(str, key);
        System.out.println("\nEncrypted String is: " + encrypted);

        String decrypted = decrypt(encrypted, key);
        System.out.println("\nDecrypted String is: " + decrypted);
        System.out.println("\n");
    }

    public static String encrypt(String str, int key)
```

```
{ 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)

HillCipher

rPROGRAM:

```
import java.io.*;
import
java.util.*;import java.io.*;public class
HillCipher{
    static float[][] decrypt=new float[3][1];static float[][]
    a=new float[3][3];static float[][] b = new
    float[3][3]; static float[][] mes = new
    float[3][1]; static float[][] res=new float[3][1];
    static BufferedReader br = new
    BufferedReader(new InputStreamReader(System.in));static Scanner sc=new Scanner(System.in);public stati
    c void main(String[] args)throws IOException{
        //TODO code application logic here get ke
        ymes();
        for(int i=0;i<3;i++)for(int j=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("\n
        Encrypted string is:"); 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(int j=0;j<1;j
        ++)for(int k=0;k<3;k++){
        decrypt[i][j]=decrypt[i][j]+b[i][k]*res[k][j];}System.out.prin
        t("\n Decrypted string is:");
```

```
        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(Itshouldbeinvertible:");for(inti=0;i<3;i++)
    for(intj=0;j<3;j++)a[i][j]=sc.
    nextFloat();
    System.out.print("\nEnter3letterstring:");Stringmsg=br.read
    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: Write a Java program to implement the DES algorithm logic.

PROGRAM:

```
import java.util.*;
import
java.io.BufferedReader; import java.io.InputStreamRe
ader; import java.security.spec.KeySpec; import javax.c
ypto.Cipher; import javax.crypto.SecretKey;
import
javax.crypto.SecretKeyFactory; import javax.crypto.spec.DESE
deKeySpec; import sun.misc.BASE64Decoder;
import sun.misc.BASE64Encoder; public class DES {
private static final String UNICODE_FORMAT = "UTF8";
public static final String DESEDE_ENCRYPTION_SCHEME = "DESede"; private KeySpec myKeySpec;
private SecretKeyFactory mySecretKeyFactory;
private Cipher cipher; byte[] keyAsBytes;
private String myEncryptionKey; private String myEncryptionScheme; SecretKey key;
    static BufferedReader br = new
    BufferedReader(new InputStreamReader(System.in)); public DES() throws Exception {
        // TODO code application logic here myEncryptionKey
        = "ThisIsSecretEncryptionKey"; myEncryptionScheme = DESEDE_ENCRYPTION_SCHEME; keyAsBytes
        =
myEncryptionKey.getBytes(UNICODE_FORMAT);
myKeySpec = new DESedeKeySpec(keyAsBytes);
mySecretKeyFactory = SecretKeyFactory.getInstance(myEncryptionScheme);
cipher = Cipher.getInstance(myEncryptionScheme);
key = mySecretKeyFactory.generateSecret(myKeySpec);
    }
public String encrypt(String unencryptedString)
    { String encryptedString = null;
    try {
cipher.init(Cipher.ENCRYPT_MODE, key);
byte[] plainText = unencryptedString.getBytes(UNICODE_FORMAT); byte[] encryptedText = cipher.doFinal(plainText);
```

```
        BASE64Encoderbase64encoder=newBASE64Encoder();encryptedString=base64enc
oder.encode(encryptedText);}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;}

privatetaticStringbytes2String(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:
");DESMycryptor=newDES();

StringstringToEncrypt=br.readLine();

String encrypted = myEncryptor.encrypt(stringToEncrypt);String decrypted =
myEncryptor.decrypt(encrypted);System.out.println("\nStringToEncrypt:"+string
ToEncrypt);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. Program to implement Blowfish algorithm logic

AIM: Write a C/JAVA program to implement the Blowfish algorithm logic.

PROGRAM:

```
import java.io.*;
import java.io.FileInputStream; import java.io.FileO
utputStream; import java.security.Key;

import javax.crypto.Cipher;
import javax.crypto.CipherOutputStream; import javax.crypto.KeyGen
erator;
import sun.misc.BASE64Encoder; public
class BlowFish {
public static void main (String [] args) throws Exception {
// TODO code application logic here KeyGenerat
or keyGenerator =
KeyGenerator.getInstance ("Blowfish"); keyGenerator.init (128); Key secretKey =
keyGenerator.generateKey ();
Cipher cipherOut = Cipher.getInstance ("Blowfish/CFB/NoPadding"); cipherOut.init (Ci
pher.E_NCRYPT_MODE, secretKey); BASE64Encoder encoder = new
BASE64Encoder ();
byte iv [] = cipherOut.getIV (); if
(iv != null) {
System.out.println ("Initialization Vector of the Cipher: " + encoder.encode (iv));
}
FileInputStream fin = new FileInputStream ("inputFile.txt"); FileOutputStream fout = new
FileOutputStream ("outputFile.txt"); CipherOutputStream cout = new CipherOutputStream (fout, cipherO
ut); int input = 0;
while ((input = fin.read ()) != -1) { cout.write (input); }

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

OUTPUT:

```
Initialization Vector of the Cipher: dIIMXzW97oQ=ContentsofinputFil
e.txt: Hello World
ContentsofoutputFile.txt: ùJÖ~NâI“
```

6. Program to implement Rijndael algorithm logic

AIM: Write a C/JAVA program to implement the Rijndael algorithm logic.

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();
SecretKeySpeckeySpec=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:HelloKGR CET
Encryptedtext:3000&&(*&*4r4Decrypted
text:Hello KGR CET
```

7. Encrypt a string using Blowfish algorithm

AIM: Using Java Cryptography, encrypt the text "Hello world" using Blowfish. Create your own key using Java key tool.

PROGRAM:

```
import javax.crypto.Cipher; import javax.crypto.KeyGenerator;
import javax.swing.JOptionPane;
public class BlowFishCipher {
    public static void main(String[] args) throws Exception {
        // create a key generator based upon the Blowfish
        KeyGenerator keyGenerator = KeyGenerator.getInstance("Blowfish");
        // create a key
        SecretKey secretKey = keyGenerator.generateKey();
        // create a cipher based upon Blowfish
        Cipher cipher = Cipher.getInstance("Blowfish");
        // initialise cipher with secret key
        cipher.init(Cipher.ENCRYPT_MODE, secretKey);
        // get the text to encrypt
        String inputText = JOptionPane.showInputDialog("Input your message:");
        // encrypt message
        byte[] encrypted = cipher.doFinal(inputText.getBytes());
        // re-initialise the cipher to be in decrypt mode
        cipher.init(Cipher.DECRYPT_MODE, secretKey);
        // decrypt message
        byte[] decrypted = cipher.doFinal(encrypted);
        // and display the results
        JOptionPane.showMessageDialog(JOptionPane.getRootFrame(),
            "\nEncrypted text: " + new String(encrypted) + "\n" +
            "\nDecrypted text: " + new String(decrypted));
        System.exit(0);
    }
}
```

OUTPUT:

```
Input your message: Hello world
Encrypted text: 3000&&(*&*4r4
Decrypted text: Hello world
```

8. RSA Algorithm

AIM: Write a Java program to implement RSA Algorithm.

PROGRAM:

```
import
java.io.BufferedReader;import java.io.InputStreamReade
r;import java.math.*;
import      java.util.Random;import
java.util.Scanner;public class RSA {
static      Scanner      sc      =      new
Scanner(System.in);public static void main(String[] args){
    // TODO code application logic
    here System.out.print("Enter a Prime number:");
    BigInteger p = sc.nextBigInteger(); // Here's one
    primenumber..System.out.print("Enter another prime
    number:"); BigInteger q = sc.nextBigInteger(); // ..and another.
    BigInteger n = p.multiply(q);
    BigInteger n2 = p.subtract(BigInteger.ONE).multiply(q.subtract(BigInteger.ONE)); BigInteger e = generateE(
    n2);
    BigInteger d = e.modInverse(n2); // Here's the multiplicative inverse

    System.out.println("Encryption keys are: "+ e + ", "+ n); System.out.println("Decryption keys are: "+ d + ", "+ n);
}
public static BigInteger generateE(BigInteger f, int n){ int i, int gcd;
    BigInteger e;
    BigInteger gcd;
    Random r = new Random();
do{
```

```
        y=x.nextInt(fiofn.intValue()-
        1);Stringz=Integer.toString(y);
        e=new BigInteger(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. heparties(Alice)andtheJavaScriptapplicationas otherparty (bob).

PROGRAM:

```
import
java.math.BigInteger;import java.se
curity.KeyFactory;import
java.security.KeyPair;
import java.security.KeyPairGenerator;import
 java.security.SecureRandom;
import javax.crypto.spec.DHParameterSpec;import ja
vax.crypto.spec.DHPublicKeySpec;public class
DiffieHellman{
public final static int pValue =
47;public final static int gValue =
71;public final static int XaValue =
9;public final static int XbValue=14;

public static void main(String[] args) throws Exception
    { // TODO code application logic here
        BigInteger p = new
        BigInteger(Integer.toString(pValue)); BigInteger g = new
        BigInteger(Integer.toString(gValue)); BigInteger Xa = new
        BigInteger(Integer.toString(XaValue)); BigInteger Xb = new BigInteger
        (Integer.toString(XbValue)); createKey(); int bitLength = 512; // 5
        12 bits

        SecureRandom rnd = new SecureRandom();
        p = BigInteger.probablePrime(bitLength, rnd
        ); g = BigInteger.probablePrime(bitLength, rnd
        );

        createSpecificKey(p, g);
    }

    public static void createKey() throws Exception {
        KeyPairGenerator kpg = KeyPairGenerator.getInstance("DiffieHellman"); kpg.initialize(512);
        KeyPair kp = kpg.generateKeyPair();
        KeyFactory kfactory =
        KeyFactory.getInstance("DiffieHellman"); DHParameterSpec param = (DHParameterSpec) k
        factory.getKeySpec(kp.getPublic(), DHParameterSpec.class);
        System.out.println("Public key is: " + kspec);
    }

    public static void createSpecificKey(BigInteger p, BigInteger g) throws Exception
    { KeyPairGenerator kpg
    = KeyPairGenerator.getInstance("DiffieHellman"); DHParameterSpec param = new DHPa
    rameterSpec(p, g); kpg.initialize(param);
    KeyPair kp = kpg.generateKeyPair();
    KeyFactory kfactory = KeyFactory.getInstance("DiffieHellman");
    DHParameterSpec param = (DHParameterSpec) kfactory.getKeySpec(kp.getPublic(), DHPubli
    cKeySpec.class);
    System.out.println("\nPublic key is: " + kspec);
    }
}
```

OUTPUT:

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

10. SHA-1

AIM: Calculate the message digest of a text using the SHA-1 algorithm in JAVA.

PROGRAM:

```
import java.security.*;
public class SHA1 {
    public static void main(String[] a) { try {
        MessageDigest md = 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());
        byte[] output = md.digest();
        System.out.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.digest();
        System.out.println();
        System.out.println("SHA1(\"" + input + "\")=" + bytesToHex(output));
        System.out.println("");
    } catch (Exception e) {
        System.out.println("Exception:" + e);
    }
}

public static String bytesToHex(byte[] b) {
    char hexDigit[] = {'0','1','2','3','4','5','6','7','8','9','A','B','C','D','E','F'};
    StringBuffer buf = new StringBuffer();
    for (int j = 0; j < b.length; j++)
        buf.append(hexDigit[(b[j] >> 4) & 0x0f]);
    buf.append(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-1algorithm inJAVA.

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("abcdefghijklmnopqrstuvwxy
z")
=C3FCD3D76192E4007DFB496CCA67E13B
```