

CRYPTOGRAPHY & NETWORK SECURITY LAB
FACULTY MANUAL
IV Year I Semester
2020-21



Prepared by

Dr.T.Srinivasarao
Begum
Associate Professor

Mrs.SK.Salma

Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING
GUDLAVALLERU ENGINEERING COLLEGE

(An Autonomous Institute with Permanent Affiliation to JNTUK, Kakinada)

Seshadri Rao Knowledge Village, Gudlavalleru – 521356

GUDLAVALLERU ENGINEERING COLLEGE

(An Autonomous Institution with Permanent Affiliation to JNTUK, Kakinada)

Seshadri Rao Knowledge Village, Gudlavalleru – 521356

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

INSTITUTE VISION & MISSION

Institute Vision:

To be a leading institution of engineering education and research, preparing students for

leadership in their fields in a caring and challenging learning environment.

Institute Mission:

- To produce quality engineers by providing state-of-the-art engineering education.
- To attract and retain knowledgeable, creative, motivated and highly skilled individuals whose leadership and contributions uphold the college tenets of education, creativity, research and responsible public service.
- To develop faculty and resources to impart and disseminate knowledge and information to students and also to society that will enhance educational level, which in turn, will contribute to social and economic betterment of society.
- To provide an environment that values and encourages knowledge acquisition and academic freedom, making this a preferred institution for knowledge seekers.
- To provide quality assurance.
- To partner and collaborate with industry, government, and R&D institutes to develop new knowledge and sustainable technologies and serve as an engine for facilitating the nation's economic development.
- To impart personality development skills to students that will help them to succeed and lead.
- To instil in students the attitude, values and vision that will prepare them to lead lives of personal integrity and civic responsibility.
- To promote a campus environment that welcomes and makes students of all races, cultures and civilizations feel at home.
- Putting students face to face with industrial, governmental and societal challenges.

DEPARTMENT VISION & MISSION

VISION

To be a Centre of Excellence in computer science and engineering education and training to meet the challenging needs of the industry and society

MISSION

- To impart quality education through well-designed curriculum in tune with the growing software needs of the industry.
- To be a Centre of Excellence in computer science and engineering education and training to meet the challenging needs of the industry and society.
- To serve our students by inculcating in them problem solving, leadership, teamwork skills and the value of commitment to quality, ethical behavior & respect for others.
- To foster industry-academia relationship for mutual benefit and growth.

PROGRAMME EDUCATIONAL OBJECTIVES(PEOs):-

PEO1: Identify, analyze, formulate and solve Computer Science and Engineering problems both independently and in a team environment by using the appropriate modern tools.

PEO2: Manage software projects with significant technical, legal, ethical, social, environmental and economic considerations.

PEO3: Demonstrate commitment and progress in lifelong learning, professional development, leadership and Communicate effectively with professional clients and the public.

PROGRAM OUTCOMES (POs)

Engineering students will be able to:

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **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.
11. **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.
12. **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

Students will be able to

PSO1: Design, develop, test and maintain reliable software systems and intelligent systems.

PSO2: Design and develop web sites, web apps and mobile apps.

Mapping Of Course Outcomes With Program Outcomes:

CRYPTOGRAPHY & NETWORK SECURITY LAB	1	2	3	4	5	6	7	8	9	10	11	12	PSO 1	PSO 2
CO1:Implement different substitution , transposition technique and format string vulnerabilities of information system	3	3	3					2	2	2	2	2	2	3
CO2:Implement DES, Blowfish Encryption and Decryption algorithm.	3	3	3					2	2	2	2	2	2	3
CO3:Implement AES, RSA Encryption and Decryption algorithm	3	2	2					2	2	2	1	2	2	2
CO4:Demonstrate Diffie-Hellman key exchange algorithm, SHA-1 Algorithm	3	3	3					2	2	2	1		2	2

Index

S. No	Program Name	Mapping Of Co's	Page No.
1	Implement different substitution and transposition techniques of information system	CO1	7
2	Write a program to implement format string vulnerabilities.	CO1	13
3	Write a C program to implement DES Encryption and Decryption algorithm.	CO2	14
4	Write a C program to implement Blowfish algorithm	CO2	16
5	Write a C program to implement AES Encryption and Decryption algorithm	CO3	18
6	Implementation of RSA algorithm Encrypt a text data and decrypt the same.	CO3	20
7	Write a C program to implement Diffie-Hellman key exchange algorithm	CO4	22
8	Calculate the message digest of a text using the SHA-1 algorithm	CO4	24
9	Write a C program to implement any virus application	CO4	26
10	Write a C program to implement PGP works	CO4	27

EXERCISE: 1**AIM:**

Write a C program to implement different substitution and transposition techniques of information system

DESCRIPTION:**CaesarCipher:**

The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

Program

```
import java.util.Scanner;
public class CaesarCipher
{
    public static final String lower = "abcdefghijklmnopqrstuvwxyz";
    public static final String upper = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
    public static String encrypt(String P, int K)
    {
        P = P.toLowerCase();
        String C = "";
        for (int i = 0; i < P.length(); i++)
        {
            int charPos = lower.indexOf(P.charAt(i));
            int keyVal = (K + charPos) % 26;
            char replace = lower.charAt(keyVal);
            C += replace;
        }
        C = C.toUpperCase();
        return C;
    }
    public static String decrypt(String C, int K)
    {
        C = C.toUpperCase();
        String P = "";
        for (int i = 0; i < C.length(); i++)
        {
            int charPos = upper.indexOf(C.charAt(i));
            int keyVal = (charPos - K) % 26;
            if (keyVal < 0)
            {
                keyVal = upper.length() + keyVal;
            }
            char replace = upper.charAt(keyVal);
            P += replace;
        }
        P = P.toLowerCase();
        return P;
    }
    public static void main(String args[])
    {
        Scanner s = new Scanner(System.in);
        System.out.println("Enter the String for Encryption: ");
        String msg = new String();
```

```

    msg = s.next();
    System.out.println("Enter the Shift Key: ");
    int key = s.nextInt();
    System.out.println(encrypt(msg, key));
    System.out.println(decrypt(encrypt(msg, key), key));
    s.close();
}
}

```

INPUT&OUTPUT:-

```

D:\islab>java CaesarCipher1
Enter the String for Encryption:
geetha
Enter the Shift Key:
2
IGGUJC
geetha
D:\islab>

```

HillCipher:

Description:

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once.

Program:

```

import java.util.*;
public class HillCipher
{
    public static final String lower="abcdefghijklmnopqrstuvwxyz";
    public static final String upper="ABCDEFGHIJKLMNOPQRSTUVWXYZ";
    public static void main(String args[])
    {
        Scanner s=new Scanner(System.in);
        System.out.println("Enter the shift key matrix order: ");
        int m=s.nextInt();
        int n=s.nextInt();
        int K[][]=new int[m][n];
        int key[][]=new int[m][n];
        System.out.println("Enter the shift key matrix... ");
        for(int i=0;i<m;i++)
        {
            for(int j=0;j<n;j++)
                K[i][j]=s.nextInt();
        }
        System.out.println("Enter the inverse shift key matrix... ");
        for(int i=0;i<m;i++)
        {
            for(int j=0;j<n;j++)
                key[i][j]=s.nextInt();
        }
        System.out.println("Enter string for encryption: ");
        String msg=new String();
    }
}

```



```

        msg=s.next();
        System.out.println(encrypt(K,m,n,msg));
        System.out.println(decrypt(encrypt(K,m,n,msg),key,m,n));
    }
    public static String encrypt(int K[][],int m,int n, String msg)
    {
        int len=msg.length();
        int o=len/n;
        msg=msg.toLowerCase();
        String str="";
        int P[][]=new int[n][o];
        int C[][]=new int[m][o];
        int charpos=lower.indexOf(msg.charAt(0));
        P[0][0]=charpos;
        for(int i=0,j=0,k=1;k<len;k++)
        {
            charpos=lower.indexOf(msg.charAt(k));
            if(++j<o)
                P[i][j]=charpos;
            else
            {
                i++;
                j=0;
                P[i][j]=charpos;
            }
        }
        for(int i=0;i<m;i++)
        {
            for(int j=0;j<o;j++)
            {
                C[i][j]=0;
                for(int k=0;k<n;k++)
                    C[i][j]=C[i][j]+(K[i][k]*P[k][j]);
            }
        }
        for(int i=0;i<m;i++)
        {
            for(int j=0;j<o;j++)
            {
                int keyval=(C[i][j])%26;
                char replace=lower.charAt(keyval);
                str+=replace;
            }
        }
        str=str.toUpperCase();
        return str;
    }
    public static String decrypt(String msg,int K[][],int m,int n)
    {
        int len=msg.length();
        int o=len/n;
        msg=msg.toUpperCase();
        String str="";
        int C[][]=new int[n][o];

```

```

int P[][]=new int[m][o];
int charpos=upper.indexOf(msg.charAt(0));
C[0][0]=charpos;
for(int i=0,j=0,k=1;k<len;k++)
{
    charpos=upper.indexOf(msg.charAt(k));
    if(++j<o)
        C[i][j]=charpos;
    else
    {
        i++;
        j=0;
        C[i][j]=charpos;
    }
}
for(int i=0;i<m;i++)
{
    for(int j=0;j<o;j++)
    {
        P[i][j]=0;
        for(int k=0;k<n;k++)
            P[i][j]=P[i][j]+(K[i][k]*C[k][j]);
    }
}
for(int i=0;i<m;i++)
{
    for(int j=0;j<o;j++)
    {
        int keyval=(P[i][j])%26;
        char replace=upper.charAt(keyval);
        str+=replace;
    }
}
str=str.toLowerCase();
return str;
}
}

```

INPUT&OUTPUT:-

```

D:\islab>java HillCipher
Enter the shift key matrix order:
2
2
Enter the shift key matrix...
1
2
3
4
Enter the inverse shift key matrix...
5
6
7
8
Enter string for encryption:
jaya
FATA
jafa
D:\islab>

```

RailFence:**Description:**

In the rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached. When the top rail is reached, the message is written downwards again until the whole plaintext is written out.

Program:

```
import java.util.*;
class RailFence
{
    public static void main(String args[])
    {
        Scanner s=new Scanner(System.in);
        System.out.println("Enter plain text: ");
        String P=new String();
        P=s.next();
        System.out.println("Enter depth: ");
        int depth=s.nextInt();
        System.out.println(Encrypt(P,depth));
        System.out.println(Decrypt(Encrypt(P,depth), depth));
    }
    public static String Encrypt(String P,int depth)
    {
        int len=P.length(),k=0;
        int c=len/depth;
        char mat[][]=new char[depth][c];
        String C="";
        for(int i=0;i<c;i++)
        {
            for(int j=0;j<depth;j++)
            {
                if(k!=len)
                    mat[j][i]=P.charAt(k++);
            }
        }
        for(int i=0;i<depth;i++)
        {
            for(int j=0;j<c;j++)
                C+=mat[i][j];
        }
        C=C.toUpperCase();
        return C;
    }
    public static String Decrypt(String C,int depth)
    {
        int len=C.length(),k=0;
        int c=len/depth;
        char mat[][]=new char[depth][c];
        String P="";
        for(int i=0;i<depth;i++)
        {
            for(int j=0;j<c;j++)
                mat[i][j]=C.charAt(k++);
        }
    }
}
```

```

        for(int i=0;i< c;i++)
        {
            for(int j=0;j< depth;j++)
                P+=mat[j][i];
        }
        P=P.toLowerCase();
        return P;
    }
}

```

INPUT&OUTPUT:-

```

Enter plain text:
case
Enter depth:
2
CSAE
case

D:\islab>javac RailFence.java

D:\islab>java RailFence
Enter plain text:
mobile
Enter depth:
3
MIOLBE
mobile

D:\islab>_

```

VIVA QUESTIONS:-

1. Caesar Cipher is an example of
2. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
3. Mono alphabetic ciphers are stronger than Poly alphabetic ciphers because frequency analysis is tougher on the former(True/False)
4. Use Caesar’s Cipher to decipher the following
HQFUBSWHG WHAW

Program 2:**Aim:**

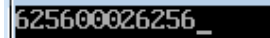
Write a program to implement format string vulnerabilities.

Description:

The Format String exploit occurs when the submitted data of an input string is evaluated as a command by the application. ... The Format Function is an ANSI C conversion function, like printf, fprintf, which converts a primitive variable of the programming language into a human-readable string representation.

Program:

```
#include<stdio.h>
void main()
{
    long a=156246;
    clrscr();
    printf("%p %p %p",a);
    getch();
}
```

OUTPUT:

625600026256_

VIVA QUESTIONS:-

1. sprintf defines Prints into a string checking the length
2. fprintf defines Writes the printf to a file
3. Format string vulnerabilities defines
4. The function printf() is defined as function with variable length of arguments. Therefore, by looking at the number of arguments, everything looks fine.(True/False)

Program 3:

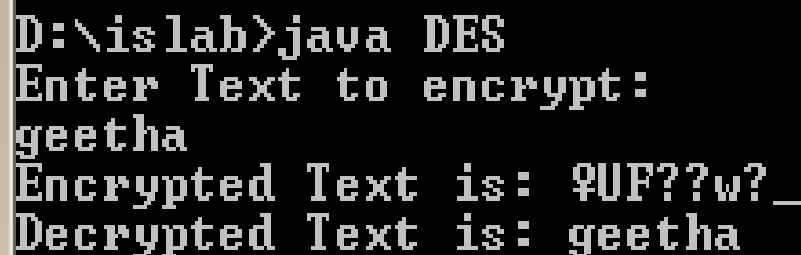
Aim: Implement DES Encryption and Decryption algorithm.

Description:

The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups it into 64-bit blocks.

Program:

```
import javax.crypto.*;
import java.util.*;
public class DES
{
    private static Cipher cipher1 = null;
    public static void main(String[] args) throws Exception
    {
        KeyGenerator kg = KeyGenerator.getInstance("DES");
        kg.init(56);
        SecretKey sk = kg.generateKey();
        cipher1 = Cipher.getInstance("DES");
        Scanner s= new Scanner(System.in);
        System.out.println("Enter Text to encrypt: ");
        String p=s.nextLine();
        byte[] pByte = p.getBytes("UTF8");
        byte[] eByte = encrypt(pByte, sk);
        String c = new String(eByte, "UTF8");
        System.out.println("Encrypted Text is: " +c);
        byte[] dByte = decrypt(eByte, sk);
        String plain = new String(dByte, "UTF8");
        System.out.println("Decrypted Text is: " +plain);
    }
    static byte[] encrypt(byte[] pByte, SecretKey sk) throws Exception
    {
        cipher1.init(Cipher.ENCRYPT_MODE, sk);
        byte[] eByte = cipher1.doFinal(pByte);
        return eByte;
    }
    static byte[] decrypt(byte[] eByte, SecretKey sk) throws Exception
    {
        cipher1.init(Cipher.DECRYPT_MODE, sk);
        byte[] dByte = cipher1.doFinal(eByte);
        return dByte;
    }
}
```

Output:


```
D:\islab>java DES
Enter Text to encrypt:
geetha
Encrypted Text is: 9UF??w?_
Decrypted Text is: geetha
```

VIVA QUESTIONS:-

- 1) What is Cryptography?
- 2) What is the major difference between the Symmetric and Asymmetric Key Algorithm?
- 3) What is the Cryptographic Life Cycle?
- 4) Length of DES key

Program 4:

Aim: Implement the Blowfish algorithm logic.

Description:

Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use.

Program:

```
import javax.crypto.*;
import java.util.*;
public class Blowfish
{
    private static Cipher cipher1 = null;
    public static void main(String[] args) throws Exception
    {
        KeyGenerator kg = KeyGenerator.getInstance("Blowfish");
        kg.init(32);
        SecretKey sk = kg.generateKey();
        cipher1 = Cipher.getInstance("Blowfish");
        Scanner s= new Scanner(System.in);
        System.out.println("Enter Text to encrypt: ");
        String p=s.nextLine();
        byte[] pByte = p.getBytes("UTF8");
        byte[] eByte = encrypt(pByte, sk);
        String c = new String(eByte, "UTF8");
        System.out.println("Encrypted Text is: " +c);
        byte[] dByte = decrypt(eByte, sk);
        String plain = new String(dByte, "UTF8");
        System.out.println("Decrypted Text is: " +plain);
    }
    static byte[] encrypt(byte[] pByte, SecretKey sk) throws Exception
    {
        cipher1.init(Cipher.ENCRYPT_MODE, sk);
        byte[] eByte = cipher1.doFinal(pByte);
        return eByte;
    }
    static byte[] decrypt(byte[] eByte, SecretKey sk) throws Exception
    {
        cipher1.init(Cipher.DECRYPT_MODE, sk);
        byte[] dByte = cipher1.doFinal(eByte);
        return dByte;
    }
}
```


Output:

```
D:\islab>java Blowfish
Enter Text to encrypt:
geetha
Encrypted Text is: r???t??
Decrypted Text is: geetha
```

VIVA QUESTIONS:-

- 1) What is the maximum size of the key in blowfish algorithm?
- 2) Blowfish encrypts blocks of plaintext which have size
- 3) The blowfish algorithm can be implemented on 16 bit processors(True/False)
- 4) The blowfish algorithm's key expansion converts a key of at most 448 bits into several subkey arrays totaling _____ bytes.

Program 5:**Aim:**

Implement AES Encryption and Decryption algorithm.

Description:

It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. ... AES is included in the ISO/IEC 18033-3 standard.

Key sizes: 128, 192 or 256 bits

Block sizes: 128 bits

Certification: AES winner, CRYPTREC, NESSIE, NSA

Rounds: 10, 12 or 14 (depending on key size)

Program:

```
import javax.crypto.*;
import java.util.*;
public class AES
{
    private static Cipher cipher1 = null;
    public static void main(String[] args) throws Exception
    {
        KeyGenerator kg = KeyGenerator.getInstance("AES");
        kg.init(128);
        SecretKey sk = kg.generateKey();
        cipher1 = Cipher.getInstance("AES");
        Scanner s= new Scanner(System.in);
        System.out.println("Enter Text to encrypt: ");
        String p=s.nextLine();
        byte[] pByte = p.getBytes("UTF8");
        byte[] eByte = encrypt(pByte, sk);
        String c = new String(eByte, "UTF8");
        System.out.println("Encrypted Text is: " +c);
        byte[] dByte = decrypt(eByte, sk);
        String plain = new String(dByte, "UTF8");
        System.out.println("Decrypted Text is: " +plain);
    }
    static byte[] encrypt(byte[] pByte, SecretKey sk) throws Exception
    {
        cipher1.init(Cipher.ENCRYPT_MODE, sk);
        byte[] eByte = cipher1.doFinal(pByte);
        return eByte;
    }
    static byte[] decrypt(byte[] eByte, SecretKey sk) throws Exception
    {
        cipher1.init(Cipher.DECRYPT_MODE, sk);
        byte[] dByte = cipher1.doFinal(eByte);
        return dByte;
    }
}
```

Output:

```
D:\islab>java AES
Enter Text to encrypt:
geetha
Encrypted Text is: <???)??K?={?
Decrypted Text is: geetha
```

VIVA QUESTIONS:-

1. Why we use Permutation, Substitution etc. in any AES or DES encryption Algorithms ?
2. AES technique uses the algorithm?
3. AES is an encryption technique of ----- ?
4. AES is found at least ----- times faster than triple DES.

Program6:

Aim:

Using RSA algorithm Encrypt a text data and decrypt the same.

Description:

RSA Algorithm is used to encrypt and decrypt data in modern computer systems and other electronic devices. RSA algorithm is an asymmetric cryptographic algorithm as it creates 2 different keys for the purpose of encryption and decryption. ... RSA makes use of prime numbers (arbitrary large numbers) to function.

Program:

```
import java.util.*;
public class RSA
{
public static void main(String args[])
{
Scanner sc=new Scanner(System.in);
int d=0,e,i;
double c,msg;
System.out.println("Enter the numbered message: ");
int m=sc.nextInt();
System.out.println("Enter two prime numbers: ");
int p=sc.nextInt();
int q=sc.nextInt();
int n=p*q;
int phi=(p-1)*(q-1);
System.out.println("the value of totent function = "+phi);
for(e=2;e<phi;e++)
{
if(gcd(e,phi)==1
                                break;
}
System.out.println("The value of e = "+e);
for(i=1;i<phi;i++)
{
if((e*i)%phi == 1)
{
d=i;
break;
}
}
System.out.println("The value of d = "+d);
c=(Math.pow(m,e))%n;
System.out.println("Encrypted message is: ");
System.out.println(c);
msg=(Math.pow(c,d))%n;
System.out.println("Derypted message is: ");
System.out.println(msg);
}
static int gcd(int a,int b)
{
if(a%b == 0)
return b;
else
```

```
return gcd(b,a%b);  
}  
}
```

Output:

```
D:\islab>java RSA  
Enter the numbered message:  
2  
Enter two prime numbers:  
7 11  
the value of totent function = 60  
The value of e = 7  
The value of d = 43  
Encrypted message is:  
51.0  
Derypted message is:  
12.0
```

VIVA QUESTIONS:-

1. What exactly do you know about RSA?
2. How Is Rsa Used For Authentication In Practice?
3. What Are Rsa Digital Signatures?
4. Is Rsa A De Facto Standard?

EXERCISE: 7**Aim:**

Implement the Diffie-Hellman key exchange algorithm

Description:

The Diffie-Hellman key exchange is a secure method for exchanging cryptographic keys. This method allows two parties which have no prior knowledge of each other to establish a shared, secret key, even over an insecure channel.

Program:

```
import java.io.*;
import java.util.*;
class DiffieHellman
{
    public static void main(String args[])
    {
        Scanner s=new Scanner(System.in);
        System.out.println("Enter modulo(p)");
        int p=s.nextInt();
        System.out.println("Enter primitive root of "+p);
        int g=s.nextInt();
        System.out.println("Choose 1st secret no(Alice)");
        int a=s.nextInt();
        System.out.println("Choose 2nd secret no(BOB)");
        int b=s.nextInt();
        int A = (int)Math.pow(g,a)%p;
        int B = (int)Math.pow(g,b)%p;
        int S_A = (int)Math.pow(B,a)%p;
        int S_B =(int)Math.pow(A,b)%p;
        if(S_A==S_B)
        {
            System.out.println("ALice and Bob can communicate with
each other!!!");
            System.out.println("They share a secret no = "+S_A);
        }
        else
            System.out.println("ALice and Bob cannot communicate with
each other!!!");
    }
}
```

OUTPUT:

```
Enter modulo(p)
17
Enter primitive root of 17
3
Choose 1st secret no(Alice)
12
Choose 2nd secret no(BOB)
14
ALice and Bob can communicate with each other!!!
They share a secret no = 16
```

VIVA QUESTIONS:-

1. Suppose that two parties A and B wish to setup a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is-----
2. What is public key cryptography?
3. What is blind signature scheme?
4. What is Message Authentication Code?

EXERCISE: 8**Aim:**

Calculate the message digest of a text using the SHA-1 algorithm

Description:

SHA-1 or Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. This hash value is known as a message digest. ... To calculate cryptographic hashing value in Java, Message Digest Class is used, under the package java.security.

Program:

```
import java.util.*;
import java.io.IOException;
import sun.misc.*;
public class SHA
{
    private static Random r = new Random((new Date()).getTime());

    public static void main(String args[]) throws Exception
    {
        Scanner s = new Scanner(System.in);
        String st = s.nextLine();
        System.out.println("Encrypted string :" + encrypt(st));
        System.out.println("Decrypted string :" + decrypt(encrypt(st)));
    }
    public static String encrypt(String str)
    {
        BASE64Encoder e = new BASE64Encoder();
        byte[] s = new byte[8];
        r.nextBytes(s);
        return e.encode(s) + e.encode(str.getBytes());
    }
    public static String decrypt(String estr)
    {
        if (estr.length() > 12)
        {
            String c = estr.substring(12);
            BASE64Decoder d = new BASE64Decoder();
            try
            {
                return new String(d.decodeBuffer(c));
            }
            catch (IOException e) { }
        }
        return null;
    }
}
```



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.648]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Zainab>h:

H:\>cd H:\CNS\JavaPrograms

H:\CNS\JavaPrograms>javac SHA1.java

H:\CNS\JavaPrograms>java SHA1
Message digest object info:
  Algorithm=SHA1
  Provider=SUN version 11
  ToString=SHA1 Message Digest from SUN, <initialized>

SHA1("")=DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

SHA1("abc")=A9993E364706816ABA3E25717850C26C9CD0D89D

SHA1("abcdefghijklmnopqrstuvwxyz")=32D10C7B8CF96570CA04CE37F2A19D84240D3A89

H:\CNS\JavaPrograms>
```

Viva Questions:

1. SHA-1 produces a hash value of
2. What is the number of round computation steps in the SHA-256 algorithm?
3. In SHA-512, the message is divided into blocks of size ___ bits for the hash computation.
4. What is the maximum length of the message (in bits) that can be taken by SHA-512?

EXERCISE: 9**Aim:**

Implement any virus application

Description:

A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. The virus requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator.

Program:

```
:x  
Start sample.bat  
Start notepad  
Start wordpad  
Start paint  
goto x
```

OUTPUT:

Today's computer systems are under constant attack from computer viruses. Viruses often disrupt a system's operations and can destroy stored data. With the increased use of the Internet, viruses can spread quickly to systems on a worldwide scale. In order to prevent the infection of computer systems, users employ anti-virus software.

VIVA QUESTIONS:

1. What is a computer virus?
2. How are computer viruses spread?
3. How do I remove a virus infection?
4. What level of support does ITS provide in the removal of viruses?

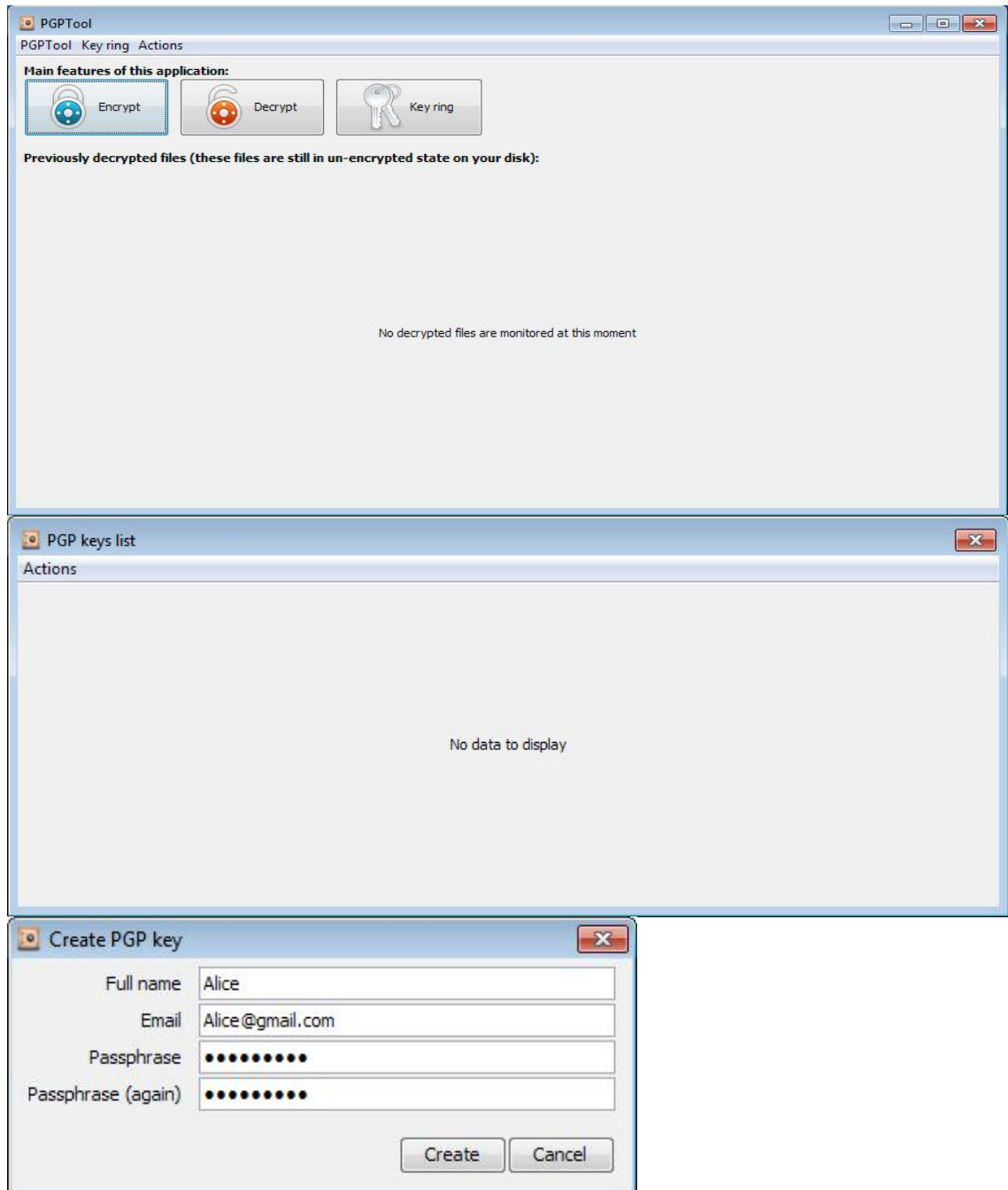
EXERCISE: 10**Aim:**

Examine how PGP works.

Description:

First download the tool-pgptool.github.io

After that perform encryption and decryption.

Program:

Create PGP key

Full name: Bob

Email: bob@gmail.com

Passphrase: ●●●●●●

Passphrase (again): ●●●●●●

Buttons: Create, Cancel

PGP keys list

Actions

User	Key ID	Key Algorithm	Key type	Created on	Expires at
Alice <Alice@gmail.com>	C3AAA3DDC20A06D5	SHA 1withDSA 1024bit	Key Pair	2017-09-25	

PGP keys list

Actions

User	Key ID	Key Algorithm	Key type	Created on	Expires at
Alice <Alice@gmail.com>	C3AAA3DDC20A06D5	SHA 1withDSA 1024bit	Key Pair	2017-09-25	
Bob <Bob@gmail.com>	1C70ECC455FC0581	SHA 1withDSA 1024bit	Key Pair	2017-09-25	

PGPTool

PGPTool Key ring Action

Main features of this app

Encrypt

Previously decrypted files

Select file to encrypt

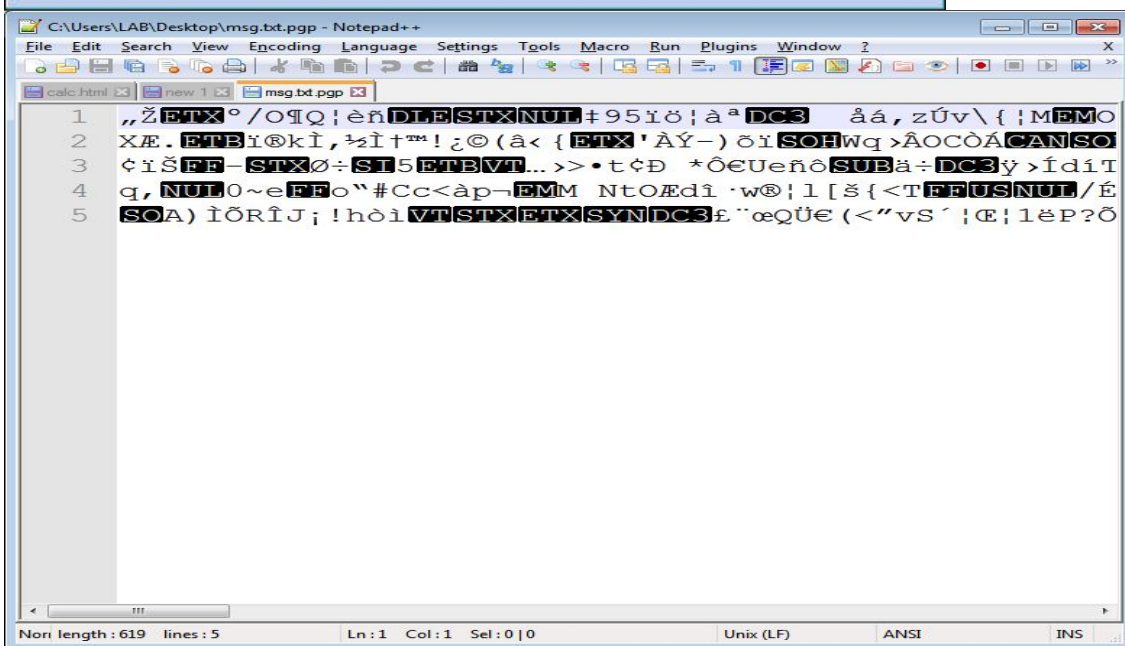
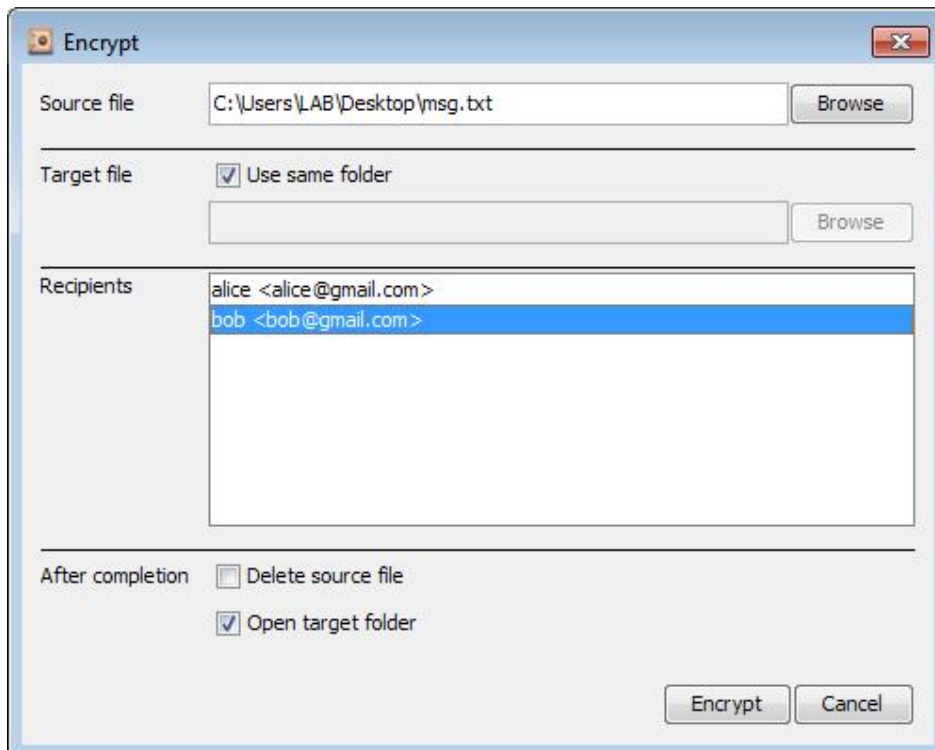
Look in: Desktop

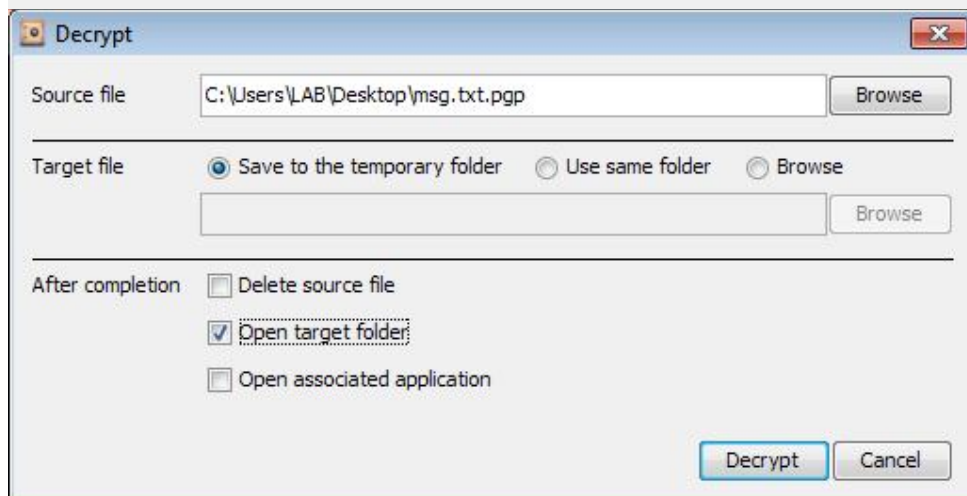
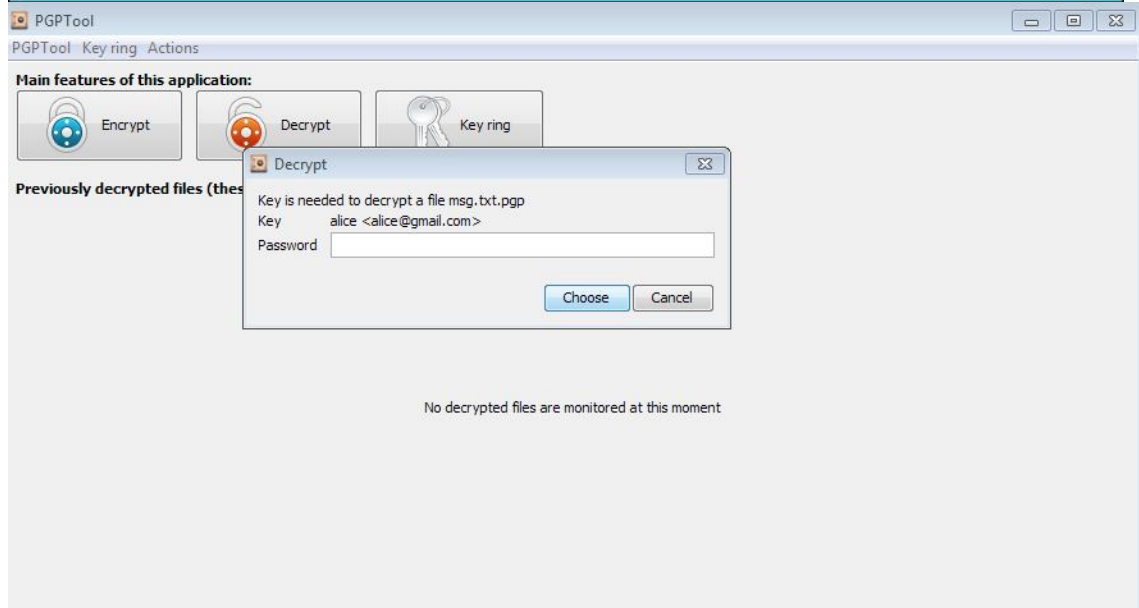
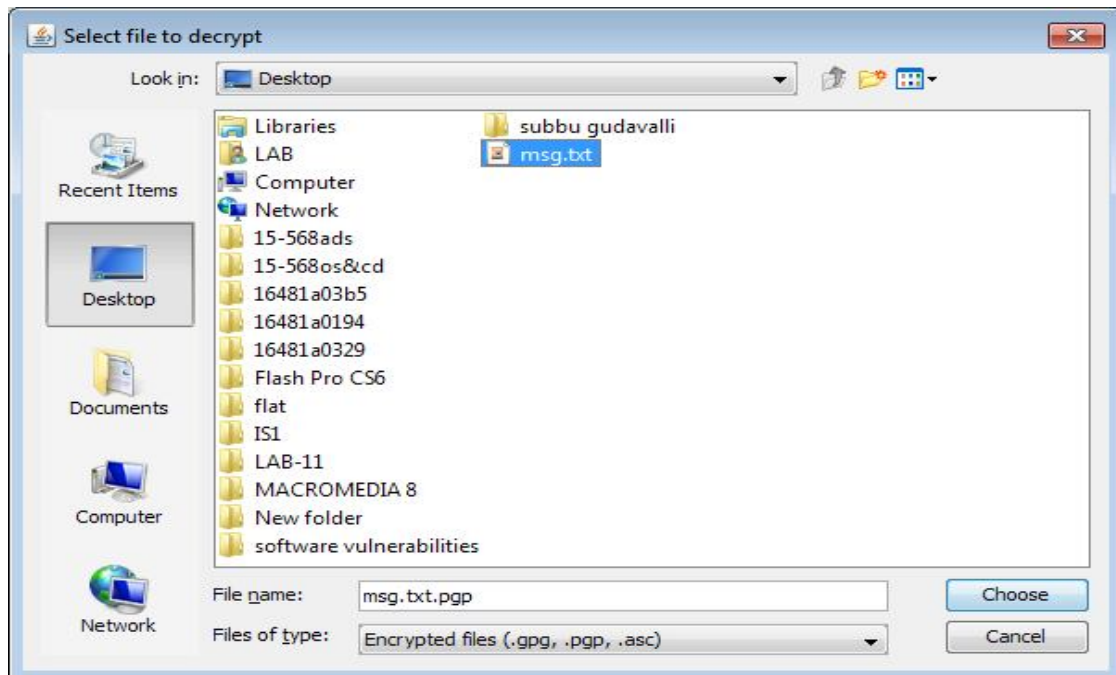
- 14-5D0(1)
- 14-5D0
- 16-329 PPT
- 15481a05d3
- 169481A03A2
- DSUC_Week_3_Lab
- Flash_Professional_8
- HARSHA
- images
- include
- Learning ActionScript 3.0 - Rich Shupe, Zevan Rosser
- MMAD-SAMPLE-LAB-MANUAL
- msg
- New Microsoft Office Word Document (2)
- New Microsoft Office Word Document

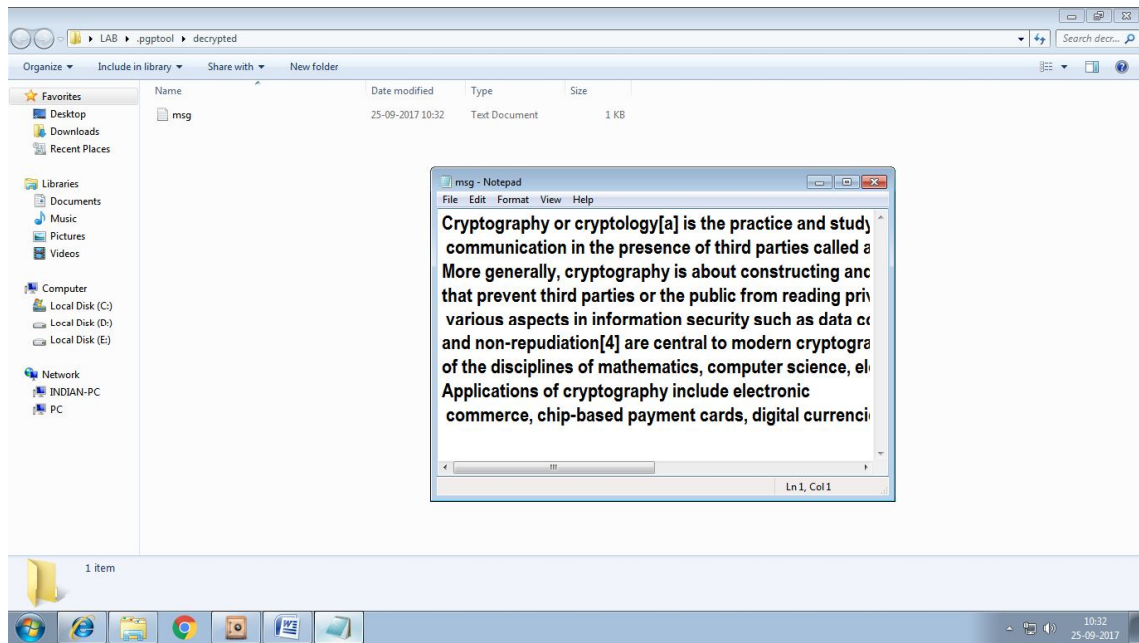
File name: msg.txt

Files of type: All files (except already encrypted)

Buttons: Choose, Cancel







VIVA QUESTIONS:

1. What Is PGP Public Key Block?
2. How Do I Verify A PGP Signature?
3. How To Store Kleopatra PGP Keys On USB Drive?
4. Why Do People Share Their PGP Keys And How To Use It?