S

Sri Indu
College of Engineering & Technology
UGC Autonomous Institution
Recognized under 2(f) & 12(B) of UGC Act 1956,
NAAC, Approved by AICTE &
Permanently Affiliated to JNTUH

Estd.2001

NAAC
NATIONAL ASSESSMENT AND ACCREDITATION COUNCIL

INFORMATION SECURITY LAB
(R22INF4126)

LAB MANUAL

IV Year I Semester

DEPARTMENT OF INFORMATION TECHNOLOGY

SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY
B. TECH –INFORMATION TECHNOLOGY

INSTITUTION VISION

To be a premier Institution in Engineering & Technology and Management with competency, values and social consciousness.

INSTITUTION MISSION

IM1 Provide high quality academic programs, training activities and research facilities.

IM2 Promote Continuous Industry-Institute Interaction for Employability, Entrepreneurship, Leadership and Research aptitude among stakeholders.

IM3 Contribute to the Economical and technological development of the region, state and nation.

DEPARTMENT VISION

To be a recognized knowledge centre in the field of Information Technology with self - motivated, employable engineers to society.

DEPARTMENT MISSION

The Department has following Missions:

DM1 To offer high quality student centric education in Information Technology.

DM2 To provide a conducive environment towards innovation and skills.

DM3 To involve in activities that provide social and professional solutions.

DM4 To impart training on emerging technologies namely cloud computing and IOT with involvement of stake holders.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

PEO1: **Higher Studies:** Graduates with an ability to apply knowledge of Basic sciences and programming skills in their career and higher education.

PEO2: **Lifelong Learning:** Graduates with an ability to adopt new technologies for ever changing IT industry needs through Self-Study, Critical thinking and Problem solving skills.

PEO3: **Professional skills:** Graduates will be ready to work in projects related to complex problems involving multi-disciplinary projects with effective analytical skills.

PEO4: **Engineering Citizenship:** Graduates with an ability to communicate well and exhibitsocial, technical and ethical responsibility in process or product.

PROGRAM OUTCOMES (POs) & PROGRAM SPECIFIC OUTCOMES (PSOs)

PO	Description
PO 1	**Engineering Knowledge:** Apply knowledge of mathematics, natural science, computing, engineering fundamentals and an engineering specialization as specified in WK1 to WK4 respectively to develop to the solution of complex engineering problems.
PO 2	**Problem Analysis:** Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusions with consideration for sustainable development. (WK1 to WK4)
PO 3	**Design/Development of Solutions:** Design creative solutions for complex engineering problems and design/develop systems/components/processes to meet identified needs with consideration for the public health and safety, whole-life cost, net zero carbon, culture, society and environment as required. (WK5)
PO 4	**Conduct Investigations of Complex Problems:** Conduct investigations of complex engineering problems using research-based knowledge including design of experiments, modelling, analysis & interpretation of data to provide valid conclusions. (WK8).
PO 5	**Engineering Tool Usage:** Create, select and apply appropriate techniques, resources and modern engineering & IT tools, including prediction and modelling recognizing their limitations to solve complex engineering problems. (WK2 and WK6)
PO 6	**The Engineer and The World:** Analyze and evaluate societal and environmental aspects while solving complex engineering problems for its impact on sustainability with reference to economy, health, safety, legal framework, culture and environment. (WK1, WK5, and WK7).
PO 7	**Ethics:** Apply ethical principles and commit to professional ethics, human values, diversity and inclusion; adhere to national & international laws. (WK9)
PO 8	**Individual and Collaborative Team work:** Function effectively as an individual, and as a member or leader in diverse/multi-disciplinary teams.
PO 10	**Project Management and Finance:** Apply knowledge and understanding of engineering management principles and economic decision-making and apply these to one's own work, as a member and leader in a team, and to manage projects and in multidisciplinary environments.
PO 11	**Life-Long Learning:** Recognize the need for, and have the preparation and ability for i) independent and life-long learning ii) adaptability to new and emerging technologies and iii) critical thinking in the broadest context of technological change. (WK8)
Program Specific Outcomes	
PSO 1	**Software Development:** To apply the knowledge of Software Engineering, Data Communication, Web Technology and Operating Systems for building IOT and Cloud Computing applications.
PSO 2	**Industrial Skills Ability:** Design, develop and test software systems for world-wide network of computers toprovide solutions to real world problems.
PSO 3	**Project implementation:** Analyze and recommend the appropriate IT Infrastructure required for the implementationof a project.

GENERAL LABORATORY INSTRUCTIONS

1. Students are advised to come to the laboratory at least 5 minutes before (to the starting time),those who come after 5 minutes will not be allowed into the lab.
2. Plan your task properly much before to the commencement, come prepared to the lab with thesynopsis / program / experiment details.
3. Student should enter into the laboratory with:
    a) Laboratory observation notes with all the details (Problem statement, Aim, Algorithm,Procedure, Program, Expected Output, etc.,) filled in for the lab session.
    b) Laboratory Record updated up to the last session experiments and other utensils (if any)needed in the lab.
    c) Proper Dress code and Identity card.
4. Sign in the laboratory login register, write the TIME-IN, and occupy the computer system allotted to you by the faculty.
5. Execute your task in the laboratory, and record the results / output in the lab observation notebook, and get certified by the concerned faculty.
6. All the students should be polite and cooperative with the laboratory staff, must maintain thediscipline and decency in the laboratory.
7. Computer labs are established with sophisticated and high end branded systems, which should be utilized properly.
8. Students / Faculty must keep their mobile phones in SWITCHED OFF mode during the lab sessions. Misuse of the equipment, misbehaviors with the staff and systems etc., will attract severe punishment.
9. Students must take the permission of the faculty in case of any urgency to go out ; if anybody found loitering outside the lab / class without permission during working hours will be treated seriously and punished appropriately.
10. Students should LOG OFF/ SHUT DOWN the computer system before he/she leaves the labafter completing the task (experiment) in all aspects. He/she must ensure the system / seat is kept properly.

Head of the Department **Principal**

DEPARTMENT OF INFORMATION TECHNOLOGY

COURSE NAME: INFORMATION SECURITY LAB

Course Name	Course outcomes
C41L1.1	Explain security concepts, Ethics in Network Security. Identify and classify various Attacks and explain the same(L2-Understand
C41L1.2	Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to various attacks. (L5-Evaluate)
C41L1.3	Explain the role of third-party agents in the provision of authentication services. (L2-Understand)
C41L1.4	Comprehend and apply authentication, email security, web security services and mechanisms. (L3- Apply)
C41L1.5	Distinguish and explain different protocol like SSL, TLS and their applications. (L6-Create)
C41L1.6	Discuss the effectiveness of passwords in access control. Explain Firewall principles. (L4-Analyze)

COURSE ARTICULATION MATRIX

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
C41L1.1	2	2	-	-	-	-	-	-	-	-	-	-	3	3	3
C41L1.2	2	2	3	-	-	-	-	-	-	-	-	-	3	3	3
C41L1.3	2	2	3	3	-	-	-	-	-	-	-	-	3	3	3
C41L1.4	2	2	2	2	-	-	-	-	-	-	-	-	3	3	3
C41L1.5	2	2	3	2	-	-	-	-	-	-	-	-	3	3	3
C41L1.6	2	2	3	3	-	-	-	-	-	-	-	-	3	3	3
C41L1	2	2	2.8	2.5	-	-	-	-	-	-	-	-	3	3	3

SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY
(An Autonomous Institution under UGC, New Delhi)

B.Tech. - IV Year – I Semester

L	T	P	C
0	0	2	1

(R22INF4126) INFORMATION SECURITY LAB

List of Experiments:

1. Write a C program that contains a string (char pointer) with a value 'Hello world'. The programshould XOR each character in this string with 0 and displays the result.
2. Write a C program that contains a string (char pointer) with a value 'Hello world'. The programshould AND or and XOR each character in this string with 127 and display the result.
3. Write a Java program to perform encryption and decryption using the following algorithms
   a. Ceaser cipher b. Substitution cipher c. Hill Cipher
4. Write a C/JAVA program to implement the DES algorithm logic.
5. Write a C/JAVA program to implement the Blowfish algorithm logic.
6. Write a C/JAVA program to implement the Rijndael algorithm logic.
7. Write the RC4 logic in Java Using Java cryptography; encrypt the text "Hello world" usingBlowfish. Create your own key using Java key tool.
8. Write a Java program to implement RSA algorithm.
9. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript.
10. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.
11. Calculate the message digest of a text using the MD5 algorithm in JAVA.

Course outcomes:

At the end of the course student will be able to

- To summarize master information security governance, and related legal and regulatory issues(Understanding)
- .To be familiar with how threats to an organization are discovered, analyzed, (Remembering)
- To be familiar with network security threats and countermeasures(Remembering)
- To be familiar with network security designs using available secure solutions (such as PGP,SSL, IPSec, etc).(Creating)
- To be familiar with advanced security issues and technologies (such as DoS attack detection and containment, and anonymous communication(Evaluating)
- compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.(Analyzing)

List of Experiments

S.No	Name Of The Experiment	No. of Class required	CO
1.	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 displays the result.	**3**	**CO1**
2.	Write a C program that contains a string (char pointer) with a value 'Hello world'. The program should AND or and XOR each character in this string with 127 and display the result.	**3**	**CO1**
3.	Write a Java program to perform encryption and decryption using the following algorithms a. Ceaser cipher b. Substitution cipher c. Hill Cipher	**3**	**CO1**
4.	Write a C/JAVA program to implement the DES algorithm logic.	**3**	**CO3**
5.	Write a C/JAVA program to implement the Blowfish algorithm logic.	**3**	**C03**
6.	Write a C/JAVA program to implement the Rijndael algorithm logic	**3**	**C03**
7	Write the RC4 logic in Java Using Java cryptography; encrypt the text "Hello world" using Blowfish. Create your own key using Java key tool.	**3**	**C03**
8	Write a Java program to implement RSA algorithm.	**3**	**C03**
9	Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript.	**3**	**C03**
10	Calculate the message digest of a text using the SHA-1 algorithm in JAVA.	**3**	**C04**
11	Calculate the message digest of a text using the MD5 algorithm in JAVA.	**3**	**C04**

LAB INCHARGE **HOD**

CONTENT BEYOND THE SYLLABUS

S.No	Name Of The Experiment	No. of Class required	CO
12	Implement different substitution and transposition techniques of information system	3	CO1
13	Write a program to implement format string vulnerabilities.	3	CO1
14	Write a C program to implement any virus application	3	C04

EXPERIMENT NO-1

NAME OF THE EXPERIMENT: 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 displays the result.

PROGRAM:

```
#include<stdlib.h>  main()
{
char str[]="Hello World";
char str1[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:

Hello World

Hello World

EXPERIMENT NO-2

NAME OF THE EXPERIMENT: XOR a string with a 127

AIM: Write a C program that contains a string (char pointer) with a value \Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.

PROGRAM:

```
#include<stdio.h>
#include<stdlib.h>
void main()
{
    char str[]="Hello World";
    char str1[11];
    char str2[11]=str[];
    int i,len;
    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:

Hello World

Hello World

Hello World

EXPERIMENT NO-3

NAME OF THE EXPERIMENT: Encryption & Decryption using Cipher Algorithms

AIM: Write a Java program to perform encryption and decryption using thefollowing algorithms:

a) Ceaser Cipher
b) Substitution Cipher
c) Hill Cipher

PROGRAM:

a) Ceaser Cipher

```
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(newInputStreamReader(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 (int i = 0; i < str.length(); i++)
            {int c = str.charAt(i);
            if (Character.isUpperCase(c))
                {c = c + (key % 26);
                if (c > 'Z') {
                    c = c - 26;
                }
            } else if (Character.isLowerCase(c))
                {c = c + (key % 26);
                if (c > 'z') {
                    c = c - 26;
                }
            }
            encrypted += (char) c;
        }
        return encrypted;
    }

    public static String decrypt(String str, int key) {
        String decrypted = "";
        for (int i = 0; i < str.length(); i++) {
            int c = str.charAt(i);

            if (Character.isUpperCase(c))
                {c = c - (key % 26);
                if (c < 'A') {
                    c = c + 26;
                }
            } else if (Character.isLowerCase(c))
                {c = c - (key % 26);
```

```
if (c < 'a') {  c = c + 26;
                }
                    }
                decrypted += (char) c;
                }
                return decrypted;
        }
```

Output:

Enter any String: hello

Enter the Key: 4

Encrypted String is: lipps

Decrypted String is: hello

b) Substitution Cipher

PROGRAM:

```
import java.io.*;
import
java.util.*;
public class SubstitutionCipher {
        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 String a =
                "abcdefghijklmnopqrstuvwxyz";String b =
                "zyxwvutsrqponmlkjihgfedcba";
                String a =
                "abcdefghijklmnopqrstuvwxyz";
                System.out.print("Enter any string: ");
                String str = br.readLine();
                String decrypt =
                "";char c;
                for (int i = 0; i < str.length(); i++)
                        {c = str.charAt(i);
                        int j = a.indexOf(c);
                        decrypt = decrypt + b.charAt(j);
                }
                System.out.println("The encrypted data is: " + decrypt);
        }
}
```

Output:

```
Enter any string: hello
The encrypted data is: svool
```

c) Hill cipher

PROGRAM:

```
class HillCipher  {
    public static void main(String args[]) throws Exception {
        String plainText, cipherText;
        int block;
        Scanner scn = new Scanner(System.in);
        System.out.println("Enter plain-text:");
        plainText = scn.nextLine();
        System.out.println("Enter block size of
        matrix:");block = scn.nextInt();
        Hill hill = new  Hill(block);
        plainText = plainText.replaceAll(" ",
        "");cipherText =
        hill.encrypt(plainText);
        System.out.println("Encrypted Text is:\n" + cipherText);
        String decryptedText = hill.Decrypt(cipherText);
        System.out.println("Decrypted Text is:\n" +
        decryptedText);
    }
}
```

Output:

```
Enter a 3 letter string: hai
Encrypted string is :fdx
Inverse Matrix is :
0.083333336  0.41666666  -0.33333334
-0.41666666   -0.083333336   0.6666667
0.5833333   -0.083333336   -0.33333334
Decrypted string is: hai
```

EXPERIMENT NO-4

NAME OF THE EXPERIMENT: Java program for DES algorithm logic

AIM: Write a Java program to implement the DES algorithm logic.

PROGRAM:

```
import java.util.*;
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.security.spec.KeySpec;
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESedeKeySpec;
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"; privateKeySpecmyKeySpec;
privateSecretKeyFactorymySecretKeyFactory;
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 heremyEncryptionKey = 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);
      BASE64Encoder base64encoder = new BASE64Encoder();
encryptedString = base64encoder.encode(encryptedText); }
catch (Exception e) {
e.printStackTrace(); }
returnencryptedString; }
public String decrypt(String encryptedString)
    { String decryptedText=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(); }
returndecryptedText; }
private static String bytes2String(byte[] bytes){ StringBufferstringBuffer = new StringBuffer();
for (int i = 0; i <bytes.length;
```

```
i++) { stringBuffer.append((char) bytes[i]); }
returnstringBuffer.toString(); }
public static void main(String args []) throws Exception
{ System.out.print("Enter the string:
");DES myEncryptor= new
DES();
String stringToEncrypt = br.readLine();
String encrypted = myEncryptor.encrypt(stringToEncrypt);
 Stringdecrypted=myEncryptor.decrypt(encrypted);
System.out.println("\nString To Encrypt: " +stringToEncrypt);
System.out.println("\nEncrypted Value : " +encrypted);
System.out.println("\nDecrypted Value : " +decrypted);
System.out.println("");
  }
}
```

OUTPUT:

```
Enter the string: Welcome
String To Encrypt: Welcome
Encrypted Value : BPQMwc0wKvg=
Decrypted Value : Welcome
```

EXPERIMENT NO-5

NAME OF THE EXPERIMENT: Program to implement BlowFish algorithm logic

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

PROGRAM:

```
import javax.swing.*;
import
java.security.SecureRandom;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import
javax.crypto.spec.SecretKeySpec;
import java.util.Random;
public class BlowFish {
        byte[] skey = new
        byte[1000];String
        skeyString;
        static byte[] raw;
        String inputMessage, encryptedData, decryptedMessage;
        public void Blowfish() {
                try {
                        generateSymmetricKey();
         encryptedData);
encry inputMessage = JOptionPane.showInputDialog(null, "Enter messageto
pt");
         byte[] ibyte = inputMessage.getBytes();byte[]
         ebyte = encrypt(raw, ibyte);
         String encryptedData = new String(ebyte);
         System.out.println("Encrypted message " + encryptedData);
         JOptionPane.showMessageDialog(null, "Encrypted Data " + "\n" +
```

```
                byte[] dbyte = decrypt(raw, ebyte);
                String decryptedMessage = new String(dbyte);
                System.out.println("Decrypted message " + decryptedMessage);

                JOptionPane.showMessageDialog(null, "Decrypted Data " + "\n" +
decryptedMessage);
            } catch (Exception e) {
                System.out.println(e);
            }

        }

        void generateSymmetricKey() {
            try {
                Random r = new
                Random();int num =
                r.nextInt(10000);
                String knum =
                String.valueOf(num);byte[]
                knumb = knum.getBytes(); skey =
                getRawKey(knumb); skeyString =
                new String(skey);
                System.out.println("Blowfish Symmetric key = " + skeyString);
            } catch (Exception e) {
                System.out.println(e);
            }
        }

        private static byte[] getRawKey(byte[] seed) throws Exception {
            KeyGenerator kgen = KeyGenerator.getInstance("Blowfish");
            SecureRandom sr = SecureRandom.getInstance("SHA1PRNG");
            sr.setSeed(seed);
```

```
            kgen.init(128, sr); // 128, 256 and 448 bits may not be available
            SecretKey skey = kgen.generateKey();
            raw = skey.getEncoded();
            return raw;
        }
        private static byte[] encrypt(byte[] raw, byte[] clear) throws Exception {
            SecretKeySpec skeySpec = new SecretKeySpec(raw,
            "Blowfish");Cipher cipher = Cipher.getInstance("Blowfish");
            cipher.init(Cipher.ENCRYPT_MODE, skeySpec);
            byte[] encrypted =
            cipher.doFinal(clear);return encrypted;
        }

        private static byte[] decrypt(byte[] raw, byte[] encrypted) throws Exception
            {SecretKeySpec skeySpec = new SecretKeySpec(raw, "Blowfish");
            Cipher cipher = Cipher.getInstance("Blowfish");
            cipher.init(Cipher.DECRYPT_MODE, skeySpec);
            byte[] decrypted =
            cipher.doFinal(encrypted);return decrypted;
        }

        public static void main(String args[])
            {BlowFish bf = new
            BlowFish(); bf.Blowfish();
        }
}
```

OUTPUT:

Blowfish Symmetric key = ?ó? ^EW??&?L??b]

Encrypted message ¶J. "¼?Y

Decrypted message hello

EXPERIMENT NO-6

NAME OF THE EXPERIMENT: 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.*;
import
javax.crypto.spec.*;
import java.io.*;
public class AES {
public static String asHex (byte buf[]) {
StringBuffer strbuf = new StringBuffer(buf.length
*2); int i;
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)); }
return strbuf.toString(); }
public static void main(String[] args) throws Exception
{ String message="AES still rocks!!";
// Get the KeyGenerator
KeyGenerator kgen = KeyGenerator.getInstance("AES");
kgen.init(128); // 192 and 256 bits may not be available
// Generate the secret key specs.
SecretKey skey = kgen.generateKey();
byte[] raw = skey.getEncoded();
SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");
// Instantiate the cipher
Cipher cipher = Cipher.getInstance("AES");
cipher.init(Cipher.ENCRYPT_MODE, skeySpec);
```

```
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 =
cipher.doFinal(encrypted); String originalString
= new String(original);
System.out.println("Original string: " + originalString + " " + asHex(original));
}
```

EXPERIMENT NO:7

NAME OF THE EXPERIMENT:Encrypt a string using BlowFish algorithm

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

PROGRAM:

```
import javax.crypto.Cipher;
import
javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import
javax.swing.JOptionPane;

public class  BlowFishCipher1  {
        public  static  void  main(String[]  args)  throws  Exception  {
                // create a key generator based upon the Blowfish cipher
                // KeyGeneratorkeygenerator = KeyGenerator.getInstance("Blowfish");
                // create a key
                // create a cipher based upon Blowfish
                Cipher cipher = Cipher.getInstance("Blowfish");
                // initialise cipher to 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(in
putText.getBytes(
));
        // re-
        initialise the
        cipher to be
        in decrypt
        mode
        //
        cipher.init(C
        ipher.DECR
        YPT_MOD
        E,
        secretkey);
        // decrypt
        message
        byte[]
        decrypted =
        cipher.doFin
        al(encrypted)
        ;
        // and
        display the
        results
        JOptionPan
        e.showMess
        ageDialog(J
        OptionPane.
        getRootFram
        e(),"\nEncryt
        ed
```

```
text: " + new String(encrypted) + "\n" + "\nDecrypted text: " + new String(decrypted));
                System.exit(0);
        }
}
```

OUTPUT:

Input your message: Hello world

Encrypted text: 3ooo&&(*&*4r4

Decrypted text: Hello world

EXPERIMENT NO:8

NAME OF THE EXPERIMENT: JAVA PROGRAM TO IMPLEMENT RSA ALGORITHM

AIM: Write a Java program to implement RSA Algorithm.

PROGRAM:

```
import java.io.BufferedReader;
import
java.io.InputStreamReader;
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
```

```
fiofn){int y, intGCD;
BigInteger e;
BigInteger gcd;
Random x = new Random();
do {
y = x.nextInt(fiofn.intValue()-
1);String z =
Integer.toString(y);
e = new BigInteger(z);
gcd =  fiofn.gcd(e);
intGCD =
gcd.intValue();
}
while(y <= 2 || intGCD !=
1);return e;
}
}
```

OUTPUT:

```
Enter a Prime number: 5
Enter another prime number:
Encryption keys are: 13, 35
Decryption keys are: 13, 35
```

EXPERIMENT NO:9

NAME OF THE EXPERIMENT: TO IMPLEMENT DIFFEI-HELLMAN KEY EXCHANGE USING JAVASCRIPT

Diffie-Hellman

AIM: 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 other party (bob).

PROGRAM:

```
import java.math.BigInteger;
import
java.security.KeyFactory;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import    java.security.SecureRandom;
import javax.crypto.spec.DHParameterSpec;
import
javax.crypto.spec.DHPublicKeySpec; public
class DiffeHellman {
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;
// 512 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");
DHPublicKeySpec kspec =
(DHPublicKeySpec)
kfactory.getKeySpec(kp.getPublic(),DHPublicKeySpec.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 DHParameterSpec(p, g);
kpg.initialize(param);
KeyPair kp = kpg.generateKeyPair();
KeyFactory kfactory = KeyFactory.getInstance("DiffieHellman");
DHPublicKeySpec kspec =
(DHPublicKeySpec)
kfactory.getKeySpec(kp.getPublic(),DHPublicKeySpec.class);
System.out.println("\nPublic key is : " +kspec);
}
}
```

OUTPUT:

Public key is: javax.crypto.spec.DHPublicKeySpec@5afd29

Public key is: javax.crypto.spec.DHPublicKeySpec@9971ad

EXPERIMENT NO:10

NAME OF THE EXPERIMENT: 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]); } return buf.toString(); }
}
```

OUTPUT:

```
Message digest object info:
Algorithm = SHA1
Provider = SUN version 1.6

ToString = SHA1 Message Digest from SUN, <initialized> SHA1("") =
DA39A3EE5E6B4B0D3255BFEF95601890AFD80709 SHA1("abc")
=
A9993E364706816ABA3E25717850C26C9CD0D89D
SHA1("abcdefghijklmnopqrstuvwxyz")=32D10C7B8CF96570CA04CE37F2A19D8424
0D3A89
```

EXPERIMENT NO:11

NAME OF THE EXPERIMENT: MESSAGE DIGEST ALGORITHM5 (MD5)

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

PROGRAM:

```
import java.security.*;
public class MD5 {
public static void main(String[] a) {
// TODO code application logic here
try {
MessageDigest md = MessageDigest.getInstance("MD5");
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("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.digest();
```

```
System.out.println();
System.out.println("MD5(\"" +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]); } return buf.toString();
 }
 }
```

OUTPUT:

```
Message digest object info:Algorithm = MD5Provider
= SUN version 1.6
ToString = MD5 Message Digest from SUN, <initialized>
MD5("") =D41D8CD98F00B204E9800998ECF8427E
MD5("abc") =
900150983CD24FB0D6963F7D28E17F72 MD5("abcdefghijklmnopqrstuvwxyz") =
C3FCD3D76192E4007DFB496CCA67E13B
```

ADDITIONAL EXPERIMENTS

EXPERIMENT NO:12

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

DESCRIPTION:

CeaserCipher:

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:-

EXPERIMENT NO:13

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 void main()
{
long a=156246;
clrscr();
printf("%p %p %p",a);
getch();
}
```

OUTPUT:

625600026256

EXPERIMENT NO:14

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.

MODEL PAPER FOR LAB INTERNAL-1

SET-1

1.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 displays the result.

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

Using **Ceaser Cipher**

SET-2

1.Write a C program that contains a string (char pointer) with a value \Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.

2.Write a Java program to perform encryption and decryption using the following algorithms using **Substitution Cipher.**

SET-3

1. Write a C program that contains a string (char pointer) with a value \Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.

2.Write a Java program to perform encryption and decryption using the following algorithms using **Hill cipher**.

SET-4

1.Write a C program that contains a string (char pointer) with a value \Hello World'.

The program should XOReach character in this string with 0 and displays the result.

2.Write a Java program to implement RSA Algorithm.

SET-5

1.Write a Java program to perform encryption and decryption using the following algorithms using **Hill cipher**.

2**.** To Implement Diffei-Hellman Key Exchange Using Javascript

MODEL PAPER FOR LAB INTERNAL-2

SET-1

1. Using Java Cryptography, encrypt the text "Hello world" using BlowFish. Create your own key using Java key tool.
2. Calculate the message digest of a text using the MD5 algorithm in JAVA

SET-2

1. Write a Java program to implement RSA Algorithm.
2. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.

SET-3

1. 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 other party (bob).
2. Using Java Cryptography, encrypt the text "Hello world" using BlowFish. Create your own key using Java key tool.

SET-4

1. Write a Java program to implement RSA Algorithm.
2. Calculate the message digest of a text using the MD5 algorithm in JAVA

SET-5

1. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.
2. 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 other party (bob).

Viva Questions

1. What Is C.I.A?

The C.I.A. triangle was the standard based on confidentiality, integrity, and availability. The C.I.A. triangle has expanded into a list of critical characteristics of information.

2. Define Network Security ?

Network security - is the protection of networking components,connections,and contents.

3. What Are The Critical Characteristics Of Information?

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity

- Utility Possession

4.What is cryptography?

Cryptography aids to secure information from third parties who are called adversaries. It allows only the sender and the recipient to access the data securely.

5. What is a firewall? Mention its uses.

A firewall is a network security device/system, which blocks malicious traffic such as hackers, worms, malware, and viruses.

Uses:

It monitors the incoming and outgoing network traffic. It permits or allows only data packets that agree to the set of security rules.

It acts as a barrier between the internal network and the incoming traffic from external sources like the Internet.

6. Mention the difference between symmetric and asymmetric encryption.

Differentiator	Symmetric Encryption	Asymmetric Encryption
Encryption Key	Only one key to encrypt and decrypt a message	Two different keys (public and private keys) to encrypt and decrypt the message
Speed of Execution	Encryption is faster and simple	Encryption is slower and complicated
Algorithms	RC4, AES, DES, and 3DES	RSA, Diffie-Hellman, and ECC
Usage	For the transmission of large chunks of data	For smaller transmission to establish a secure connection prior to the actual data transfer

7. What is SSL encryption?

Secure Socket Layer is a security protocol that is used for the purpose of encryption. It ensures privacy, data integrity, and authentication in the network like online transactions.

8. Mention the steps to set up a firewall.

Following are the steps you have to follow to set up a firewall:

1. **Username/password:** Alter the default password of a firewall device.
2. **Remote Administration**: Always disable the Remote Administration feature.
3. **Port Forward**: For the web server, FTP, and other applications to work properly, configure appropriate ports.
4. **DHCP Server:** Disable the DHCP server when you install a firewall to avoid conflicts.
5. **Logging**: Enable logs to view the firewall troubleshoots and to view logs.
6. **Policies:** Configure strong security policies with the firewall.

9. What is the CIA triad?

It is a security model to ensure IT security. CIA stands for confidentiality, integrity, and availability.

- **Confidentiality:** To protect sensitive information from unauthorized access.
- **Integrity:** To protect data from deletion or modification by an unintended person.
- **Availability:** To confirm the availability of the data whenever needed.

10. What exactly is SNMP?

SNMP is an abbreviation for Simple Network Management Protocol. This protocol provides a foundation for gathering data that will allow us to control, monitor, and modify electronic properties on a network.

11. What are the different kinds of sniffing attacks?

There are two types of sniffing attacks:

Passive sniffing: When a set of devices or computers are connected to a hub, passive sniffing can be performed. Every host on the network can see traffic through a hub. Therefore, the attacker allows the sniffer to listen to all traffic to the same broadcast domain devices.

Active sniffing: Active sniffing attacks occur when a device is connected to a switch. In this attack, the attacker intentionally sends malicious traffic onto the network to overload and trick the memory table into diverting traffic to them. This attack can be carried out using MAC flooding, ARP poisoning, and MAC duplicating.

12. What are salted hashes?

Salt is a piece of random data. When an adequately secured password system gets a new password, it generates a hash value of that password and a random salt value and stores the combined value in its database. This aids in the defense against dictionary and known hash attacks.

13. What can be done to avoid identity theft?

Below are some of the tips to prevent identity theft:

- Use a strong and unique password
- Avoid sharing sensitive information online, particularly on social media
- Buy from well-known and reliable websites
- Install specialized malware and spyware removal software
- Always keep your system and antivirus up to date

14.What do you mean by data leakage?

Purposeful or unintentional data transmission from within the organization to an unapproved outside location is known as data leakage. Data leakage can be divided into three types based on how it occurs.

- **Accidental breach:** An entity unintentionally sends data to an unauthorized person due to an error or mistake.
- **Intentional breach:** Data is purposefully sent by the authorized party to the unauthorized party.
- **System hack:** Data leakage is caused via hacking methods.

15. What do you understand by regulatory compliance?

Regulatory compliance refers to the adherence of individuals, organizations, or businesses to the laws, regulations, guidelines, and standards set forth by regulatory bodies or authorities governing their specific industry or jurisdiction. It involves following the rules and requirements designed to ensure ethical behavior, safety, security, data privacy, and transparency within a particular field.