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

CRYPTOGRAPHY & NETWORK SECURITY
LAB MANUAL

III YEAR CSE (CS) – Semester I

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

ACADEMIC YEAR 2022-23

SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY

(An Autonomous Institution under UGC, New Delhi)
Recognized under 2(f) and 12(B) of UGC Act 1956
NBA Accredited, Approved by AICTE and Permanently affiliated to JNTUH
Sheriguda (V), Ibrahimpatnam, R.R.Dist, Hyderabad - 501 510

DEPARTMENT OF

COMPUTER SCIENCE AND ENGINEERING(CYBER SECURITY)

LAB MANUAL

Branch: CSE(CS)
Subject: Cryptography & Network Security
Academic Year: 2022-23
Core/Elective/H&S: Core

Class: B.Tech- III Year-I sem
Code:R20CSE41L1
Regulation: R20
Credits: 1

Prepared By
Name: E. Mounika Reddy,
E.Rajendra

Verified By
Head of the Department:

DEPARTMENT OF CS

LAB MANUAL- INDEX

Sri Indu College of Engineering & Technology

Sheriguda (V), R.R.Dist

INSTITUTION VISION

To evolve into a center of excellence in Science and Technology through creative and innovative practices in teaching & learning, towards promotion of academic achievement & research excellence to produce globally accepted, competitive and world class professionals, who are psychologically strong and emotionally balanced, imbibed with social consciousness and ethical values.

INSTITUTION MISSION

To provide high quality academic programs, training activities, research facilities and opportunities supported by continuous industry-institute interaction aimed at promoting employability, entrepreneurship, leadership and research aptitude among students and contribute to the economic and technological development of the region, state and Nation.

PRINCIPAL

Sri Indu College of Engineering & Technology

Sheriguda (V), R.R.Dist

Department Of Computer Science And Engineering(CS)

DEPARTMENT VISION

To empower the students to be technologically adopt, innovative, self-motivated and responsible global citizens possessing human values and contribute significantly towards high quality with ever changing world.

DEPARTMENT MISSION

DM$_1$To offer high quality education in the computing fields by providing an environment where the knowledge is gained and applied to participate in research, for both students and Faculty.

DM$_2$To develop the problem solving skills in the students to be ready to deal with cutting edge Technologies of the industry

DM$_3$To make the students and faculty excel in their professional fields by inculcating the Communication Of skills, leadership skills, team building skills with the organization various co-curricular programmers

DM$_4$To provide the students with theoretical and applied knowledge, and adopt an education Approach that promotes lifelong learning and ethical growth.

HOD

Sri Indu College of Engineering & Technology

Sheriguda (V), R.R.Dist

Department of Computer Science &Engineering(CS)

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

PROGRAM OUTCOMES (POs)

PO	Description
PO 1	**Engineering Knowledge:** To be able to apply knowledge of computing, mathematics, Science and Engineering appropriate to the discipline
PO 2	**Problem Analysis:** To be able identify, formulate & analyze a problem, and ascertain and define the computing requirements appropriate to its solution.
PO 3	**Design & Development Solutions:** To be able to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs.
PO 4	**Investigation of complex problems:** To be able to identify and analyze user needs and consider them in the selection, creation, evaluation and administration of Computer-based systems for providing valid solutions to complex problems.
PO 5	**Modern Tool Usage:** To possess skills for creating and in using contemporarytechniques, skills, and tools necessary for computing practice.
PO 6	**Engineering & Society:** To apply conceptual knowledge relevant to professional engineering practices in societal, health, safety, legal and cultural issues and their consequences
PO 7	**Environment & Sustainability:** To be able to analyze the local and global impact of computing on individuals, organizations, and society and work towards sustainable development.
PO 8	**Ethics:** To understand contemporary professional, ethical, legal, security and social issues and responsibilities.
PO 9	**Individual & Team work:** To Be able to function effectively as an individual and on teams to accomplish a common goal.
PO 10	**Communication:** To communicate precisely and effectively both in oral and written form with a range of audiences.
PO 11	**Project management & finance:** To apply engineering and management principles for managing and leading economically feasible projects in multi-disciplinary environments with an effective project plan.
PO 12	**Life Long Learning:** To recognize the need for and an ability to engage in independent & lifelong learning for continuing professional development.

PROGRAM SPECIFIC OUTCOMES (PSOs)

Program Specific Outcomes	
PSO 1	To develop software projects using standard practices and suitable programming environment.
PSO 2	To identify, formulate and solve the real life problems faced in the society, industry and other areas by applying the skills of the programming languages, networks and databases learned.
PSO 3	To apply computer science knowledge in exploring and adopting latest technologies in various inter-disciplinary research activities.

Sri Indu College of Engineering & Technology

Sheriguda (V), R.R.Dist

Department of Computer Science &Engineering(CS)

COs and POs & PSOs Mapping

SUB Name: Cryptography & Network Security Lab

SUB CODE: R20CSE41L1

Course out comes (COs):

C41L1.1	Explain security concepts, Ethics in Network Security. Identify and classify various Attacks and explain the same.
C41L1.2	Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to various attacks.
C41L1.3	Explain the role of third-party agents in the provision of authenticationservices.
C41L1.4	Comprehend and apply authentication, email security, web security servicesand mechanisms.
C41L1.5	Distinguish and explain different protocol like SSL, TLS Vis-à-vis theirapplications
C41L1.6	Discuss the effectiveness of passwords in access control.Explain firewall principles.

`

Faculty

Sri Indu College of Engineering & Technology

Sheriguda (V), R.R.Dist

Department of Computer Science &Engineering(CS)

COs and POs & PSOs Mapping

SUB Name: Cryptography & Network Security Lab

SUB CODE: R20CSE41L1

CO	PO 1	PO2	PO3	PO4	PO 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO1 2	PSO1	PSO2	PSO3
C41L1.1	3	2	-	-	-	-	-	-	-	-	-	-	3	3	3
C41L1.2	3	3	3	-	-	-	-	-	-	-	-	-	3	3	3
C41L1.3	2	3	3	3	-	-	-	-	-	-	-	-	3	3	3
C41L1.4	2	3	2	2	-	-	-	-	-	-	-	-	3	3	3
C41L1.5	2	3	3	2	-	-	-	-	-	-	-	-	3	3	3
C41L1.6	2	2	3	3	-	-	-	-	-	-	-	-	3	3	3
	2.33	**2.67**	**2.8**	**2.5**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	3	3	3

High (3) **Medium (2)** **Low (1)**

1. DIMENSIONS OF THE LAB

Area of the lab in Sqmts	:	66 Sqm
2. CAPACITY OF THE LAB	:	60 Students
3. EQUIPMENTS		
Computer Systems (Clients)	:	60
CPU	:	60
Monitors	:	60
Key Board	:	60
Mouse	:	60
4. SYSTEM CONFIGURATION	**:**	Intel ®Core™ I3 Speed: 3.10 GHz, 2GB RAM Hard Disk: 500 GB HCL LED Monitor Size-18.5
5. SOFTWARE	**:**	**Turbo C, java, Windows OS, Open Office**

6. AMBIENCE

Printers	:	00
Projector	:	01
Computer Tables	:	60
Student Chairs	:	60
Charts	:	
Photo Frames	:	03
Switch/Hub	:	01
White Boards	:	01
A/C s	:	02
Power Backup	:	

Academic Calendar

Recognized under 2(f) and 12(B) of UGC Act 1956
NBA & NAAC Accredited, Approved by AICTE and Permanently affiliated to JNTUH
Sheriguda (V), Ibrahimpatnam, R.R.Dist, Hyderabad - 501 510

BR-20

Lr.No.SICET/AUTO/DAE/III B.Tech Academic Calendar/307/2022 **Dt: 03.08.2022**

Dr.G. SURESH,
Principal,

To,
All the HODs.

III B.TECH I SEM & II SEM ACADEMIC CALENDAR
ACADEMIC YEAR : 2022-23

Sir,

Sub: SICET (Autonomous) - Academic & Evaluation - Academic Calendar for **B.Tech – 3rd Year** - For the academic year **2022-23** – Reg.

***

The approved Academic Calendar for **B.Tech – 3rd Year (I & II Sem)** for the academic year **2022-23** is given below:

Academic Calendar for B.Tech – 3rd Year Students (2020 - 21 Batch), BR-20 Regulation.

I - Semester

Commencement of class work	**25.08.2022 (Thursday)**	
Instruction / Class Work. (Including CRT and Dussehra Holidays).	25.08.2022	28.12.2022 – 18 Weeks
Dussehra Holidays.	03.10.2022	06.10.2022 - 4 Days
I Mid Examinations for III B.Tech I Sem Students.	27.10.2022	29.10.2022 - 3 Days
II Mid Examinations for III B.Tech I Sem Students.	29.12.2022	31.12.2022 - 3 Days
Preparation Holidays & Practical Lab Examinations.	02.01.2023	07.01.2023 - 1 Week
Remedial Mid Test (RMT).	09.01.2023	11.01.2023 - 3 Days
III B.Tech I Semester End Examination.	16.01.2023	28.01.2023 - 2 Weeks
Commencement of class work of III B.Tech II Semester - 30.01.2023 (Monday)		

II - Semester

Commencement of class work	**30.01.2023 (Monday)**	
I Spell of Instructions.	30.01.2023	20.05.2023 - 16 Weeks
I Mid Examinations for III B.Tech II Sem Students.	27.03.2023	29.03.2023 - 3 Days
II Mid Examinations for III B.Tech II Sem Students.	23.05.2023	25.05.2023 - 3 Days
Preparation Holidays & Practical Lab Examinations.	26.05.2023	31.05.2023 - 1 Week
Remedial Mid Test (RMT).	01.06.2023	03.06.2023 - 3 Days
III B.Tech II Semester End Examination.	05.06.2023	17.06.2023 - 2 Weeks

ACE **CE** **DIRECTOR** **PRINCIPAL**

Copy to DAE;
Copy to all the Heads of the Depts.

CONTROLLER OF EXAMINATIONS
Sri Indu College of Engineering & Technology
(An Autonomous Institution under JNTUH)
Sheriguda (V), Ibrahimpatnam, R.R.Dist.-501510

DIRECTOR
(Academic Audit)
Sri Indu College of Engineering & Technology
Sheriguda, IBP, R.R. Dist-501510.

Sri Indu College of Engineering & Technology
(An Autonomous Institution under JNTUH)
Sheriguda (V), Ibrahimpatnam, R.R.Dist.-501510

Cryptography & Network Security

LAB MANUAL

SYLLABUS

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

B.Tech. - III Year – I Semester

L	T	P	C
0	0	2	1

(R18CSE41L1) Cryptography & Network Security Lab

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 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. 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" using Blowfish. 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.

TIME TABLE

SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY

Sheriguda (V), R.R.Dist.

(An Autonomous Institution under UGC)

DEPARTMENT OF CSE (CYBER SECURITY)

ROOM NO: M103 **AY: 2022-23**

Class: III CS (I SEM) **TIME - TABLE**

w.e.f: 25.08.2022

Time	9:40 – 10:30	10:30 – 11:20	11:20 –12:10	12:10—1:00	1:00 To 1:30	1:30 – 2:20	2:20 – 3:10	3:10 – 4:00
Days	1	2	3	4		5	6	7
Monday	DBMS	CNS	EH	DAA	L	CC	AI	EH
Tuesday	CC	CNS	LIB	EH	U	DBMS	DAA	AI
Wednesday	EH	<----------AI LAB---------->			N	CC	CNS	AI
Thursday	DBMS	CC	DAA	TECH.SESSION	C	<----------DBMS LAB---------->		
Friday	CNS	DAA	DBMS	TUTORIAL	H	<----------CNS LAB---------->		
Saturday	DAA	AI	CNS	DBMS		CC	EH	COUNS

SUBJECT CODE	SUBJECT NAME	FACULTY NAME
R20CSE3203	DESIGN AND ANALYSIS OF ALGORITHMS	Mr.Sathyamurthy
R20CSE4101	CRYPTOGRAPHY AND NETWORK SECURITY	Mrs. D.Suma
R20CSE3122	ARTIFICIAL INTELLIGENCE	Mrs.M.Swathi Reddy
R20CSE2203	DATABASE MANAGEMENT SYSTEMS	Ms.D.Mounika
R20CSE4143	**Professional Elective-I**- CLOUD COMPUTING	Ms.K.Anusha
R20CSC3102	**Professional Elective-II**-ETHICAL HACKING	Mrs.G.Uma maheswari
R20CSE41L1	CRYPTOGRAPHY AND NETWORK SECURITY LAB	Mrs.E.Mounika / Mr.E.Rajendra
R20CSM31L1	ARTIFICIAL INTELLIGENCE LAB	Mrs.M.Swathi Reddy /Mrs.K.Shwetha
R20CSE22L2	DATABASE MANAGEMENT SYSTEMS LAB	Mrs.D.Mounika / Mrs.V.Swathi
LIB	LIBRARY	Mrs.E.Mounika
TUTORIAL	TUTORIAL	Ms.D.Mounika / Mr.Sathyamurthy / Mrs. D.Suma
COUNS	COUNSELLING	Mrs.K.Shwetha/ Mrs.V.Swathi / Mrs.E.Mounika
TECH.SESSION	TECHNICAL SESSION	Student Coordinator/ Mrs.K.Shwetha

CLASS INCHARGE: Mrs. K. SHWETHA REDDY

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 the synopsis / program / experiment details.

3. Student should enter into the laboratory with:

a. Laboratory observation notes with all the details (Problem statement, Aim, 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 note book, and get certified by the concerned faculty.

6. All the students should be polite and cooperative with the laboratory staff, must maintain the discipline 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 lab after completing the task (experiment) in all aspects. He/she must ensure the system / seat is kept properly.

HOD **PRINCIPAL**

LAB Schedule

S.No	Name Of The Experiment	No. of sessions required
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 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	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 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	Using Java Cryptography, encrypt the text "Hello world" using Blowfish. 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. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).	
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.	

Lab Manual

EXPERIMENT-1

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

VIVA QUESTIONS:

1. What is AND Operation?
2. What is XOR Operation?
3. What Is String?
4. What is Cryptography?
5. What is Network Security?

EXPERIMENT-2

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

VIVA QUESTIONS:

1. What is a goal of Cryptography?
2. Advantages and Disadvantages of Cryptography and Network Security?
3. Just how important field of Cryptography?
4. What is plaintext?
5. What is cipher text?

EXPERIMENT-3

AIM: Write a Java program to perform encryption and decryption using the following 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(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 (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
```

VIVA QUESTIONS:

1. What is the Ceaser Cipher in Java?
2. How Encryption and Decryption is done in Ceaser Cipher?
3. What is the use of Ceaser Cipher?
4. How do you decrypt a Ceaser Cipher?
5. Where is key for the Ceaser Cipher?
6. How is Ceaser Cipher calculated?

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 d = "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
```

VIVA QUESTIONS:

1. What is the function of Substitution Cipher?
2. How many keys are in a Substitution Cipher?
3. What are the examples for the Substitution Cipher?
4. Which Substitution Cipher is best?

C) Hill Cipher

PROGRAM:

```
package Java;
public class Hill_Cipher {

	public static int[][] keymat = new int[][] { { 1, 2, 1 }, { 2, 3, 2 },{ 2, 2, 1 } };
	public static int[][] invkeymat = new int[][] { { -1, 0, 1 }, { 2, -1, 0 }, { -2, 2, -1 } };
	public static String key = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
	private static String encode(char a, char b, char c)
	{
		String ret = "";
		int x, y, z;
		int posa = (int) a - 65;
		int posb = (int) b - 65;
		int posc = (int) c - 65;
		x = posa * keymat[0][0] + posb * keymat[1][0] + posc * keymat[2][0];
		y = posa * keymat[0][1] + posb * keymat[1][1] + posc * keymat[2][1];
		z = posa * keymat[0][2] + posb * keymat[1][2] + posc * keymat[2][2];
		a = key.charAt(x % 26);
		b = key.charAt(y % 26);
		c = key.charAt(z % 26);
		ret = "" + a + b + c;
		return ret;
	}
	private static String decode(char a, char b, char c)
	{
		String ret = "";
		int x, y, z;
		int posa = (int) a - 65;
		int posb = (int) b - 65;
		int posc = (int) c - 65;
		x = posa * invkeymat[0][0] + posb * invkeymat[1][0] + posc * invkeymat[2][0];
```

```
        y = posa * invkeymat[0][1] + posb * invkeymat[1][1] + posc * invkeymat[2][1];
        z = posa * invkeymat[0][2] + posb * invkeymat[1][2] + posc * invkeymat[2][2];
        a = key.charAt((x % 26 < 0) ? (26 + x % 26) : (x % 26));
        b = key.charAt((y % 26 < 0) ? (26 + y % 26) : (y % 26));
        c = key.charAt((z % 26 < 0) ? (26 + z % 26) : (z % 26));
        ret = "" + a + b + c;
        return ret;
}
public static void main(String[] args) throws java.lang.Exception
{
        String msg;
        String enc = "";
        String dec = "";
        int n;
        msg = ("SecurityLaboratory");
        System.out.println("simulation of Hill Cipher\n-------------------------");
        System.out.println("Input message : " + msg);
        msg = msg.toUpperCase();
        msg = msg.replaceAll("\\s", "");
        n = msg.length() % 3;
        if (n != 0)
        {
                for (int i = 1; i <= (3 - n); i++)
                {
                        msg += 'X';
                }
        }
        System.out.println("padded message : " + msg);
        char[] pdchars = msg.toCharArray();
        for (int i = 0; i < msg.length(); i += 3) {
                enc += encode(pdchars[i], pdchars[i + 1], pdchars[i + 2]);
}
```

```
                System.out.println("encoded message : " + enc);
                char[] dechars = enc.toCharArray();
                for (int i = 0; i < enc.length(); i += 3)
                {
                        dec += decode(dechars[i], dechars[i + 1], dechars[i + 2]);
                }
                System.out.println("decoded message : " + dec);
        }
}
```

Output:

```
simulation of Hill Cipher
-------------------------
Input message : SecurityLaboratory
padded message : SECURITYLABORATORY
encoded message : EACSDKLCAEFQDUKSXU
decoded message : SECURITYLABORATORY
```

VIVA QUESTIONS:

1. What is the Hill Cipher used for?
2. What is the decrypted Algorithm of Hill Cipher?
3. How do you implement Hill Cipher in Java?
4. When was the Hill Cipher used?

EXPERIMENT-4

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

PROGRAM:

```
package Java;
import java.io.*;
import java.security.*;
import java.security.spec.*;
import javax.crypto.*;
import javax.crypto.spec.IvParameterSpec;
public class DesProgram
{
        private static Cipher encrypt;
        private static Cipher decrypt;
        private static final byte[] initialization_vector = { 22, 33, 11, 44, 55, 99, 66, 77 };
        public static void main(String[] args)
        {
        String textFile = "E:\\Demo.txt";
       String encryptedData = "E:\\encrypteddata.txt";
       String decryptedData = "E:\\decrypteddata.txt";
    try
{
        SecretKey scrtkey = KeyGenerator.getInstance("DES").generateKey();
        AlgorithmParameterSpec aps = new IvParameterSpec(initialization_vector);
        encrypt = Cipher.getInstance("DES/CBC/PKCS5Padding");
        encrypt.init(Cipher.ENCRYPT_MODE, scrtkey, aps);
        decrypt = Cipher.getInstance("DES/CBC/PKCS5Padding");
        decrypt.init(Cipher.DECRYPT_MODE, scrtkey, aps);
        encryption(new FileInputStream(textFile), new FileOutputStream(encryptedData));
        decryption(new FileInputStream(encryptedData), new FileOutputStream(decryptedData));
                System.out.println("The encrypted and decrypted files have been created
    successfully.");
                }
```

```
            catch (NoSuchAlgorithmException | NoSuchPaddingException | InvalidKeyException |
        InvalidAlgorithmParameterException | IOException e)
            {
                e.printStackTrace();
            }
        }
        private static void encryption(InputStream input, OutputStream output) throws IOException
        {
            output = new CipherOutputStream(output, encrypt);
            writeBytes(input, output);
        }
        private static void decryption(InputStream input, OutputStream output) throws IOException
        {
            input = new CipherInputStream(input, decrypt);
            writeBytes(input, output);
        }
        private static void writeBytes(InputStream input, OutputStream output) throws IOException
        {
            byte[] writeBuffer = new byte[512];
            int readBytes = 0;
            while ((readBytes = input.read(writeBuffer)) >= 0)
            {
                output.write(writeBuffer, 0, readBytes);
            }
            output.close();
            input.close();
        }
    }
```

OUTPUT:

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

VIVA QUESTIONS:

1. What is DES Algorithm used for?
2. What type of Algorithm is DES?
3. Where is DES Algorithm used?
4. What is DES principle?

EXPERIMENT-5

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

PROGRAM:

```
package BlowfishAlgorithm;
import java.util.Scanner;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
public class BlowfishAlgorithm {
	public static void main(String[] args) throws Exception {
		KeyGenerator keyGenerator = KeyGenerator.getInstance("blowfish");
		SecretKey secretKey = keyGenerator.generateKey();
		Cipher cipher = Cipher.getInstance("blowfish");
		cipher.init(Cipher.ENCRYPT_MODE, secretKey);
		Scanner sc = new Scanner(System.in);
		System.out.print("Enter the words want you to Encrypt : ");
		String inputText = sc.nextLine();
		byte[] encrypt = cipher.doFinal(inputText.getBytes());
		cipher.init(Cipher.DECRYPT_MODE, secretKey);
		byte[] decrypt = cipher.doFinal(encrypt);
		System.out.println("Words After Encryption : " + new String(encrypt));
		System.out.println("Words After Decryption : " + new String(decrypt));
		}
}
```

Output:

Enter the words want you to Encrypt: Hello World!

Words after Encryption: êŽ;´_ƒ89Ô_(®Ú_Ê_

Words after Decryption: Hello World!

VIVA QUESTIONS:

1. What is Blowfish Algorithm used for?
2. What type of algorithm is Blowfish?
3. What is the minimum size of key in Blowfish Algorithm?
4. What is block size of Blowfish?

EXPERIMENT-6

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

PROGRAM:

```
package Java;
import javax.crypto.*;
import javax.crypto.spec.*;
class Rijndael
{
	private 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 = "SRI INDU COLLEGE";
		KeyGenerator kgen = KeyGenerator.getInstance("AES");
		kgen.init(128);
		SecretKey skey = kgen.generateKey();
		byte[] raw = skey.getEncoded();
		SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");
		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 in Hexadecimal: "+ asHex(original));
            System.out.println("Original String: " + originalString);
        }
}
```

OUTPUT:

Input your message: Hello KGRCET

Encrypted text: 3000&&(*&*4r4)

Decrypted text: Hello KGRTCET

VIVA QUESTIONS:

1. How does Rijndael Algorithm work?
2. What is difference between AES and Rijndael?
3. What is Rijndael better known as?
4. What are some characteristics of Rijndael?

EXPERIMENT-7

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.crypto.SecretKey;
import javax.swing.JOptionPane;

/**
 * This program demonstrates how to encrypt/decrypt input
 * using the Blowfish Cipher with the Java Cryptograhpy.
 *
 */
public class BlowfishCipher {

  public static void main(String[] args) throws Exception {

    // create a key generator based upon the Blowfish cipher
    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 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(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(),
                        "encrypted text: " + new String(encrypted) + "\n" +
                        "decrypted text: " + new String(decrypted));

    // end example
    System.exit(0);
  }
}
```

OUTPUT:

Input your message: Hello world

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

Decrypted text: Hello world

VIVA QUESTIONS:

1. What is RC4 logic in java?
2. How do you use Blowfish encryption in java?
3. How many sub keys are in Blowfish Algorithm?
4. What is the key in RC4?

EXPERIMENT-8

AIM: Write a Java program to implement RSA Algorithm.

PROGRAM:

```
package Java;
//Java Program to Implement the RSA Algorithm
import java.math.*;

class RSA {
	public static void main(String args[])
	{
		int p, q, n, z, d = 0, e, i;

		// The number to be encrypted and decrypted
		int msg = 12;
		double c;
		BigInteger msgback;

		// 1st prime number p
		p = 3;

		// 2nd prime number q
		q = 11;
		n = p * q;
		z = (p - 1) * (q - 1);
		System.out.println("the value of z = " + z);

		for (e = 2; e < z; e++) {

			// e is for public key exponent
			if (gcd(e, z) == 1) {
				break;
			}
```

```
            }
            System.out.println("the value of e = " + e);
            for (i = 0; i <= 9; i++) {
                int x = 1 + (i * z);

                // d is for private key exponent
                if (x % e == 0) {
                    d = x / e;
                    break;
                }
            }
            System.out.println("the value of d = " + d);
            c = (Math.pow(msg, e)) % n;
            System.out.println("Encrypted message is : " + c);

            // converting int value of n to BigInteger
            BigInteger N = BigInteger.valueOf(n);

            // converting float value of c to BigInteger
            BigInteger C = BigDecimal.valueOf(c).toBigInteger();
            msgback = (C.pow(d)).mod(N);
            System.out.println("Decrypted message is : "
                                        + msgback);
        }

        static int gcd(int e, int z)
        {
            if (e == 0)
                return z;
            else
                return gcd(z % e, e);
        }
}
```

OUTPUT:

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

VIVA QUESTIONS:

1. What is RSA algorithm in java?
2. How is RSA algorithm implemented?
3. What is RSA algorithms explain with example?
4. How do you do RSA encryption in java?

EXPERIMENT-9

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
```

VIVA QUESTIONS:

1. What is Diffie-Hellman Key Exchanged used for?
2. What is the principle behind Diffie-Hellman Key Exchanged?
3. What are the features of Diffie-Hellman Key Exchanged?
4. What are the steps in Diffie-Hellman Key Exchanged Algorithm?

EXPERIMENT-10

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

PROGRAM:

```
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

public class GFG {
    public static String encryptThisString(String input)
    {
        try {
            // getInstance() method is called with algorithm SHA-1
            MessageDigest md = MessageDigest.getInstance("SHA-1");

            // digest() method is called
            // to calculate message digest of the input string
            // returned as array of byte
            byte[] messageDigest = md.digest(input.getBytes());

            // Convert byte array into signum representation
            BigInteger no = new BigInteger(1, messageDigest);

            // Convert message digest into hex value
            String hashtext = no.toString(16);

            // Add preceding 0s to make it 32 bit
            while (hashtext.length() < 32) {
                hashtext = "0" + hashtext;
            }

            // return the HashText
            return hashtext;
```

```
        }
        // For specifying wrong message digest algorithms
        catch (NoSuchAlgorithmException e) {
            throw new RuntimeException(e);
        }
    }
    // Driver code
    public static void main(String args[]) throws
                                NoSuchAlgorithmException
    {
        System.out.println("HashCode Generated by SHA-1 for: ");
        String s1 = "sri indu";
        System.out.println("\n" + s1 + " : " + encryptThisString(s1));
        String s2 = "hello world";
        System.out.println("\n" + s2 + " : " + encryptThisString(s2));
    }
}
```

OUTPUT:

Hash Code Generated by SHA-1 for:

sri indu : 7063ac6f682b31d895d12650a8d9a5f4b0f83c2e

hello world : 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed

VIVA QUESTIONS:

1. How Is Message Digest Calculated?
2. What Is SHA Algorithm Used For?
3. How Does SHA-1 Algorithm Work?
4. What Is SHA Digest?

EXPERIMENT-11

AIM: Calculate the message digest of a text using the MD5 algorithm in JAVA.

PROGRAM:

```
import java.math.BigInteger;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

// Java program to calculate MD5 hash value

public class MD5 {

    public static String getMd5(String input)

    {

        try {

            // Static getInstance method is called with hashing MD5

            MessageDigest md = MessageDigest.getInstance("MD5");

            // digest() method is called to calculate message digest

            // of an input digest() return array of byte

            byte[] messageDigest = md.digest(input.getBytes());

            // Convert byte array into signum representation

            BigInteger no = new BigInteger(1, messageDigest);

            // Convert message digest into hex value

            String hashtext = no.toString(16);

            while (hashtext.length() < 32) {

                hashtext = "0" + hashtext;

            }

            return hashtext;
```

```
        }
        // For specifying wrong message digest algorithms
        catch (NoSuchAlgorithmException e) {
            throw new RuntimeException(e);
        }
    }
    // Driver code
    public static void main(String args[]) throws NoSuchAlgorithmException
    {
        String s = "HELLO WORLD";
        System.out.println("Your HashCode Generated by MD5 is: " + getMd5(s));
    }
}
```

OUTPUT:

Your Hash Code Generated by MD5 is: 361fadf1c712e812d198c4cab5712a79

VIVA QUESTIONS:

1. How is Message Digest calculated?
2. What is MD5 Algorithm in java?
3. How does MD5 Message Digest Algorithm work explain?
4. What is MD5 Algorithm used for?

Viva Questions

1. Define Cryptography and its benefits?
2. What are the few major applications of cryptography in the modern world?
3. What is decryption? What is its need?
4. What do you mean by Secret Key Cryptography and Public Key Cryptography? How they are different from one another?
5. What type of information can be secured with Cryptography?
6. What exactly do you know about RSA?
7. What is the Digital Signature Algorithm?
8. Differentiate symmetric and asymmetric encryption?
9. What is the Caesar cipher?
10. What is plaintext?
11. What is cipher text?
12. What are the mathematical algorithms used in symmetric cryptography?
13. What are the mathematical algorithms used in asymmetric cryptography?
14. What is the difference between a private key and a public key?
15. What is a block cipher?
16. What is Transposition Ciphers?
17. What is the International Data Encryption Algorithm (IDEA)?
18. How is a Key Distribution Center (KDC) used?
19. What are the specific components of the Public Key Infrastructure (PKI)?
20. List down some Hashing Algorithms