CRYPTOGRAPHYAND NETWORK SECURITY LAB

LAB HANDOUT
(R2032056)

III/IV B.Tech, Semester-II
Academic Year: 2024-25

DEPARTMENT OF INFORMATION TECHNOLOGY

Prepared by:

Smt G. KRISHNAVENI
Sri N.PRASAD

SIR C R REDDY COLLEGE OF ENGINEERING

Eluru-534007 ELURU Dist, Andhra Pradesh, India

(**Approved by AICTE, New Delhi & Accredited by NBA)**

&
Affiliated to JNTUK, Kakinada from 2017-18 Admitted Batch)

Telephone No: 08812-230840, 230565, Fax: 08812-224193

Website: www.sircrrengg.ac.in

SIR C.R.REDDY COLLEGE OF ENGINEERING
ELURU-534007, ELURU DIST, A P., INDIA
(Approved by AICTE, New Delhi, & Accredited by NBA)
Phone no: 08812-230840, 2300656 Fax: 08812-224193
Visit us at http://www.sircrrengg.ac.in
DEPARTMENT OF INFORMAION TECHNOLOGY

VISION OF THE DEPARTMENT

To be a premier Department in the region in the field of Information Technology through academic excellence and research that enable graduates to meet the challenges of industry and society

MISSION OF THE DEPARTMENT

- To Provide dynamic teaching-learning environment to make the students industry ready and advancement in career;
- To inculcate professional and leadership quality for better employability and entrepreneurship;
- To make high quality professional with moral and ethical values suitable for industry and society

PO [1]:Engineering Knowledge: Ability to apply basic and contemporary science, technology and engineering skill to identifying software/hardware problems in the industry and academia and be able to develop practical solution to them.

PO [2]: Problem analysis: Ability to analyze identifies, formulate, and solve computer software and hardware related engineering problems.

PO [3]: Design/development of solutions: Ability to design, implement and evaluate a computer – based system, process, component or program to meet desired needs.

PO [4]: Conduct investigations of complex problems: Ability to apply design and development principles in the construction of software systems of varying complexity.

PO [5]: Modern tool usage: Ability to use techniques, skills, and modern software development tools necessary for computing practice.

PO [6]: The engineer and society: Ability to analyze the local and global impact of computing on individuals, organizations and society.

PO [7]: Environment and sustainability: Ability to the broad education necessary to understand the impact of computer engineering solutions in a global, economic, environmental, and social context.

PO [8]: Ethics: Ability for understand of professional, ethical, legal, security and social issues and responsibilities.

PO [9]: Individual and team work: Ability to function effectively as individual and as member with others as part of a team, including those with different specialties with in computer science and computer engineering to accomplish a common goal.

PO [10]: Communication: Be effective communicators and to function well in multi – disciplinary teams the graduates should be able to communicate effectively as software professional with users, peers and higher management.

PO [11]: Project management and finance: Ability to work with good engineering and managerial skills under proper financial constraints.

PO [12]: Life-long learning: Ability to recognize the need for and to engage in life - long learning.

PROGRAMSPECIFICOUTCOMES(PSOs)

PSO1: Conceptual Skills: Apply core information technology of systems, architecture, information management, programming, networking for development of current technical concepts.

PSO2: Technical Skills: Design and develop software by adapting emerging technologies for the need of IT industry.

Programmable Educational Objectives (PEOs)

The Program Educational Objectives of B.Tech (IT) program are as follows:

PEO1: To produce graduates with strong foundation of domain knowledge in the field of Computer Science & Engineering.

PEO2: To produce graduates who can successfully pursue graduate studies and research in Computer Science& Engineering.

PEO3: To produce graduates who can practice their profession and communicate effectively either individually or in groups to meet dynamic needs of the industry.

PEO4: To imbibe in graduates a desire for lifelong learning moulded with professional and ethical values suitable to society.

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, 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 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.

Course Objective, Course Outcomes and CO-PO Correlation with Justification

Course Title:	**CRYPTOGRAPHY AND NETWORK SECURITY LAB**
Year/Semester:	**3/4 IT II Semester**
Class/Section	**Sections A & B**
A.Y	**2024-25**
Name of the Staff:	**Sri N.PRASAD , Smt G.KRISHNAVENI**

SYLLABUS:

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 Blow Fish algorithm logic

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

7. Using Java Cryptography, encrypt the text "Hello world" using Blow Fish. 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.

REFERENCES:

1. Cryptography and Network Security, 3rd Edition Behrouz A Forouzan, Deb deep Mukhopadhyay, McGraw Hill,2015
2. Cryptography and Network Security,4th Edition, William Stallings, (6e) Pearson,2006
3. Everyday Cryptography, 1st Edition, Keith M.Martin, Oxford,2016
4. Network Security and Cryptography, 1st Edition, Bernard Meneges, Cengage Learning,2018

PREREQUISITES:

1. C Programming
2. Concepts of JAVA

COURSE OBJECTIVES

This course will help students to achieve the following objectives:

- To learn basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
- To understand and implement encryption and decryption using Ceaser Cipher, Substitution Cipher, Hill Cipher.

COURSE OUTCOMES

At the end of the course students should be able to:

CO1	**Understand** the various cryptographic techniques like symmetric key, asymmetric key and hash functions
CO2	**Applying** the various cryptographic techniques like symmetric key, asymmetric key and hash functions.
CO3	**Analyze** the various cryptographic techniques like symmetric key and asymmetric key algorithms.
CO4	**Analyze** the various hash functions and digital signatures.

CO-PO/PSO MAPPING

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	-	-	-	-	-	-	-	1	-	-	2	2	-
CO2	2	-	-	-	-	-	-	-	1	-	-	2	2	-
CO3	2	2	-	-	-	-	-	-	1	-	-	2	2	-
CO4	2	2	-	-	-	-	-	-	1	-	-	2	2	-
Avg	2	2	-	-	-	-	-	-	1	-	-	2	2	-

CO-PO MAPPING JUSTIFICATION

CO1	**PO1**	**2**	To understand knowledge of engineering to evaluate the java concepts and methods at moderate level.
	PO9	**1**	Individual /team work is needed to evaluate the java concepts
	PO12	**2**	The rapid change in technology, there is a need for lifelong learning of java concepts to cope up with present trends.
CO2	**PO1**	**2**	To apply knowledge of engineering to evaluate the java concepts at moderate level.
	PO9	**1**	Individual /team work is needed to evaluate the java concepts
	PO12	**2**	The rapid change in technology,there is a need for lifelong learning of java concepts to cope up with present trends.
CO3	**PO1**	**2**	To apply knowledge of engineering to evaluate the java concepts at moderate level.
	PO2	**2**	Problem analysis is needed for analyzing various algorithms.
	PO9	**1**	Individual /team work is needed to evaluate the java concepts
	PO12	**2**	The rapid change in technology, there is a need for lifelong learning of java concepts to cope up with present trends.
CO4	**PO1**	**2**	To apply knowledge of engineering to analyze the java concepts at moderate level.
	PO2	**2**	To analyze the solutions for given problem by using java concepts like threads, event handling and cryptographic functions etc.
	PO9	**1**	Individual /team work is needed to evaluate the java concepts
	PO12	**2**	The rapid change in technology, there is a need for lifelong learning of java concepts to cope up with present trends.

CO-PSO MAPPING JUSTIFICATION

CO1	PSO1	2	To **understand** cryptography techniques ,Core concept skills and programming are required to practice XOR and AND operation.
CO2	PSO1	2	To **implement** cryptography techniques Core concept skills and programming are required
CO3	PSO1	2	**To analyze** cryptography techniques Core concept skills and programming are required
CO4	PSO1	2	To **analyze** cryptography techniques Core concept skills and programming are required

TOPICS BEYOND SYLLABUS:

- Mono-alphabetic Cipher
- One-time pad and perfect secrecy
- digital signatures
- MD5 Algorithm

	Section A	**Section B**
COURSEHANDLER	Sri N.PRASAD	Smt G.KRISHNAVENI
SIGNATURES		
COURSE COORDINATOR	Smt G.KRISHNAVENI	
HOD IT	Dr.K.SATYANARAYANA	

Signature of the Staff Member