CRYPTOGRAPHY & NETWORK SECURITY LAB

Course Code	23CS3652	**Year**	III	**Semester**	II
Course Category	PCC	**Branch**	CSE	**Course Type**	Practical
Credits	1.5	**L-T-P**	0-0-3	**Prerequisites**	C, Java, Computer Networks
Continuous Internal Evaluation	30	**Semester End Evaluation:**	70	**Total Marks:**	100

Course Outcomes		
Upon successful completion of the course, the student will be able to:		
CO1	Apply Security principles for Data & Network	**L3**
CO2	Implement programs as an individual on different IDEs/ online platforms.	**L3**
CO3	Develop an effective report based on various programs implemented	**L3**
CO4	Apply technical knowledge for a given problem and express with an effective oral communication.	**L3**
CO5	Analyze outputs using given constraints/test cases.	**L4**

Syllabus

Exp No.	**CONTENTS**	**Mapped 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.	**CO1,CO2,CO3, CO4, CO5**
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.	**CO1,CO2,CO3, CO4, CO5**
3	Write a Java program to perform encryption and decryption using the following algorithms: a) Ceaser Cipher b) Substitution Cipher c) Hill Cipher	**CO1,CO2,CO3, CO4, CO5**
4	Write a Java program to implement the DES algorithm logic	**CO1,CO2,CO3, CO4, CO5**
5	Write a C/JAVA program to implement the BlowFish algorithm logic.	**CO1,CO2,CO3, CO4, CO5**
6	Write a C/JAVA program to implement the Rijndael algorithm logic.	**CO1,CO2,CO3, CO4, CO5**
7	Using Java Cryptography, encrypt the text "Hello world" using BlowFish. Create your own key using Java key tool.	**CO1,CO2,CO3, CO4, CO5**
8	Write a Java program to implement RSA Algorithm.	**CO1,CO2,CO3, CO4, CO5**

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).	**CO1,CO2,CO3, CO4, CO5**
10	Calculate the message digest of a text using the SHA-1 algorithm in JAVA.	**CO1,CO2,CO3, CO4, CO5**
11	Implementation of Symmetric and Asymmetric Encryption using PGP Tool.	**CO1,CO2,CO3, CO4, CO5**
12	Implementation of Network Scanning using Nmap and Exploitation using Metasploit.	**CO1,CO2,CO3, CO4, CO5**

Learning Resources
Text Books
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 Everyday Cryptography, 1st Edition, Keith M.Martin, Oxford,2016
Reference Books
1. "Network Security and Cryptography, 1st Edition, Bernard Meneges, Cengage Learning,2018
E-Resources & other digital material
1.. Cryptography and Network Security, NPTEL 2. Cryptography, Coursera 3. Cryptography and Hashing Fundamentals, Udemy