# COURSE CONTENT

| CYBER SECURITY LABORATORY | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **II Semester: CSE** | | | | | | | | |
| **Course Code** | **Category** | **Hours / Week** | | | **Credits** | **Maximum Marks** | | |
| | | **L** | **T** | **P** | **C** | **CIA** | **SEE** | **Total** |
| **BCSE24** | **Core** | 0 | 0 | 4 | 2 | 40 | 60 | 100 |
| **Contact Classes: Nil** | **Tutorial Classes: Nil** | **Practical Classes: 42** | | | | **Total Classes:42** | | |
| **Prerequisites: Computer Networks** | | | | | | | | |

## I. COURSE OVERVIEW:

This course typically aims to equip students with the knowledge and skills necessary to protect information and information systems from various threats. This course covers public key crypto systems, Kerberos, and firewall mechanisms. The students can gain expertise in information security and contribute to the protection of valuable organizational assets

## II. COURSE OBJECTIVES:

The students will try to learn:

I. How to implement the cryptographic algorithms.
II. How to identify, analyze, and remediate computer security breaches.
III. The importance of digital signature algorithms

## III. COURSE OUTCOMES:

After successful completion of the course, students will be able to:

CO1 Implement cryptography techniques and attack detection for providing security solutions.
CO2 Analyze the impact of public key cryptosystems for secure exchange of information and web transactions.
CO3 Experiment with a signature scheme using the Digital signature standard.
CO4 Make Use of hashing and authentication for implementing data integrity and develop Kerberos.
CO5 Design a firewall for restricting user activities over the network.
CO6 Apply random number generation techniques for cryptosystems.

## IV. COURSE CONTENT:

**Week 1: CIPHER ALGORITHM**

Implement the encryption and decryption of symmetric cipher algorithm (AES and RC4)

**Week 2: RANDOM NUMBER GENERATION**

a) Design and implement a Random number generation algorithm using a subset of digits and alphabets.
b) Design and implement a Random number generation algorithm using a Subset-sum of numbers

**Week 3: RSA ALGORITHM**

a) Implement RSA algorithm for encryption and decryption in C
b) In an RSA System, the public key of a given user is e=31, n=3599.
Write a program to find the private key of the User.

**Week 4: HASH ALGORITHMS**
Calculate the message digest of a text using the SHA-1 and MD-5 algorithm

**Week 5: WEB TRANSACTIONS**
Implement a trusted secure web transaction

**Week 6: DIGITAL SIGNATURE ALGORITHM**
Implement the SIGNATURE SCHEME – Digital Signature Standard.

**Week 7: DIFFIE-HELLMAN ALGORITHM**
Implement the Diffie-Hellman Key Exchange algorithm

**Week 8: CRYPTOSYSTEM**
Implement of EIGAMAL cryptosystem.

**Week-9: PUBLIC KEY SYSTEM**
Implement of Goldwasser-Micali probabilistic public key system

**Week 10: CRYPTOSYSTEM**
Implement of Rabin Cryptosystem

**Week 11: KERBEROS**
Implementation of Kerberos cryptosystem

**Week 12: FIREWALL IMPLEMENTATION**
Configure a firewall to block the following for 5 minutes and verify the correctness of this system using the configured parameters:

(a) Two neighborhood IP addresses on your LAN
(b) All ICMP requests
(c) All TCP SYN Packets.

**Week 13**: **WIRESHARK**
Install and analyze the network packets using Wireshark.

**Week 14**: **PROBE ATTACKS**
Write an algorithm to detect probe attacks in network flows.

## V. REFERENCE BOOKS:


1. William Stallings "Network Security Essentials (Applications and Standards)" Pearson Education 6th edition, 2017.
2. Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security", Cengage Learning, 2011.


## VI. WEB REFERENCES:

1. https://www.iiitm.ac.in/index.php/en/information-security-lab
2. https://omscs.gatech.edu/cs-6265-information-security-lab
3. https://www.iitr.ac.in/departments/CSE/pages/Facilities+Information_Security_Lab.html
4. https://isec.unige.ch/