CYBER SECURITY LABORATORY

II Semester: CSE

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
BCSC24	Core	0	0	4	2	30	70	100
Contact Classes: Nil	Total Tutorials: Nil	Total Practical Classes: 36				Total Classes: 36		

I. COURSE OVERVIEW:

This course covers advanced techniques for writing exploits and patching vulnerabilities, taught through an intense, hands-on security laboratory. It deals about the cyber attackers, their tactics, social engineering, and high-profile case studies. This course covers a variety of topics including reverse engineering, exploitation, binary analysis, and web.

II. COURSE OBJECTIVES:

The students will try to learn:

1 How to implement the cryptographic algorithms.
2 How to identify, analyze, and remediate computer security breaches.
3 The key cyber security vendors in the marketplace.
4 The importance of digital signatures algorithms

III. COURSE OUTCOMES:

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

CO 1	**Implement** encryption and decryption techniques for providing security solutions.	Apply
CO 2	**Analyze** the impact of public key cryptosystems for secure exchange of information.	Understand
CO 3	**Experiment** a signature scheme using Digital signature standard.	Apply
CO 4	**Use** of hashing and authentication for implementing data integrity.	Apply
CO 5	**Use** firewall mechanism for restricting user activities over network.	Apply

IV. SYLLABUS

Week-1: CIPHER ALGORITHM

Implementation of symmetric cipher algorithm (AES and RC4)

Week-2: RANDOM NUMBER GENERATION

Random number generation using a subset of digits and alphabets.

Week-3: RSA ALGORITHM

Implementation of RSA based signature system

Week-4: RANDOM NUMBER GENERATION

Implementation of Subset sum of numbers

Week-5: WEB TRANSACTIONS

Implementation of a trusted secure web transaction.

Week-6: HASH ALGORITHM

Authenticating the given signature using MD5 hash algorithm.

Week-7: DIFFIE-HELLMAN ALGORITHM

Implementation of Diffie-Hellman algorithm

Week-8: CRYPTOSYSTEM
Implementation EIGAMAL cryptosystem.

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

Week-10: CRYPTOSYSTEM
Implementation of Rabin Cryptosystem.

Week-11: KERBEROS
Implementation of Kerberos cryptosystem

Week-12: FIREWALL IMPLEMENTATION
Firewall implementation and testing.

V. REFERENCE BOOKS

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Principles of Information Security, Whitman, Thomson.

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/