Security Lab			
Course Code	**19IS704**	**CIE Marks**	**50**
Teaching Hours/Week (L:T:P:S)	**0:0:2:0**	**SEE Marks**	**50**
Total Hours	**2 Hours / week**	**Credits**	**1**

Course Learning Objectives:

This Course will enable students to

- Develop code for classical Encryption Techniques to solve the problems.
- Build cryptosystems by applying symmetric and public key encryption algorithms.
- Construct code for authentication algorithms.
- Develop a signature scheme using Digital signature standard.
- Demonstrate the network security system using open source tools

Course Content

Week – 1

1. Perform encryption, decryption using the Caesar cipher substitution techniques

Week – 2

2.	Perform encryption, decryption using the Monoalphabetic cipher substitution techniques

Week – 3

3.	Perform encryption, decryption using the Playfair cipher substitution techniques

Week – 4

4.	Perform encryption, decryption using the Hill Cipher substitution techniques

Week – 5

5.	Perform encryption, decryption using the Vigenere cipher (Polyalphabetic) substitution techniques

Week – 6

6.	Write a program to demonstrate the working of Feistel Cipher algorithm

Week – 7

7.	Implement RSA Algorithm to encrypt a certain Plain text and verify the received ciphertext.

Week – 8

8.	Implement Diffie-Hellman Algorithm to establish a shared secret between two parties that can be used for secret communication to exchange data over a public network.

Week – 9

9.	Implement encryption/decryption using Elliptic curve cryptographic function

Week – 10

10.	Implement key generation technique used in Data Encryption Standard (DES)

Week 11, 12, 13 and 14 students will be working on mini project on the following topics:

1. Implement SSL with HTTP to secure the web applications.
2. Configure and Manage the network traffic using firewall rules to meet the system and user requirements for the incoming and outgoing traffic.
3. Demonstration of internet packet analysis using Wireshark.
4. Perform wireless audit on an access point or a router and decrypt WEP and WPA
5. Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)
6. Setup a honey pot and monitor the honeypot on network (KF Sensor)
7. Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w)

Course Outcomes:

At the end of the course the student will be able to

Sl. No.	Course Outcomes (CO)	Bloom's Taxonomy Level (BTL)
CO 1	An Ability to develop code for classical Encryption Techniques to solve the problems.	L2
CO 2	An Ability to Build cryptosystems by applying symmetric and public key encryption algorithms	L3
CO 3	An Ability to Construct code for authentication algorithms.	L3
CO 4	An Ability to Develop knowledge of securing web applications	L2
CO 5	An Ability to Demonstrate the network security system using open source tools	L3

Mapping of POs & Cos :

POs COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO 1	3	3	3											
CO 2	3	3	3											
CO 3		3	3											
CO 4			2	3										
CO 5		3		2	3									

(L/1 = Low 30%-49%, M/2 = Medium 50%-69%, H/3 = High >70%)

Table: Mapping of COs to PIs, POs and BTL			
Course Outcomes (COs)	**Program Outcomes (POs) Addressed**	**Performance Indicators (PI)**	**Bloom's Taxonomy Level (BTL)**
CO1	1, 2, 3	1.1.1, 1.3.1, 1.4.1, 2.1.3, 2.2.4, 2.3.1, 2.4.1, 2.4.3, 2.4.4, 3.2.2, 3.3.1	L2
CO2	1, 2, 3	1.1.1, 1.3.1, 1.4.1, 2.1.3, 2.2.4, 2.3.1, 2.4.1, 2.4.3, 2.4.4, 3.1.1, 3.2.1, 3.2.2, 3.4.3	L3
CO3	2, 3	2.1.3, 2.2.4, 2.3.1, 2.4.1, 2.4.3, 2.4.4, 3.1.1, 3.2.1, 3.2.2, 3.4.3	L3
CO4	3,4	2.1.3, 2.2.4, 2.3.1, 2.4.1, 2.4.3, 2.4.4, 3.2.2, 3.3.1, 4.1.1	L2
CO5	2,4,5	2.1.3, 2.2.4, 2.3.1, 2.4.1, 2.4.3, 2.4.4, 4.1.1,5.1.1	L3

TEXTBOOK:

1. William Stallings: Cryptography and Network Security, Pearson 7th Edition, 2017.

REFERENCE BOOK:

1. V K Pachghare: Cryptography and Information Security, PHE, 2013.