COURSE NAME: **Introduction to Cyber Security**

(A Program/Specialization Elective for CSE students) **L-T-P-C: 2-1-0-3**

1. OUTLINE:

This course is an introductory course on the fundamental concepts of cyber security. The course covers the basic concepts of cyber security such as attacks, threats and security principles. The course also covers the concepts of cryptography and access control and introduces students to the fundamentals of network and software security. The course also covers basic incident response strategies to handle cyber security incidents.

2. OBJECTIVES:

The objective of this course is to introduce students to the basic concepts of cyber security. The course aims to introduce the concept of cyber security and provide an overview of the tools and technologies used in cyber security.

3. PRE-REQUISITES:

Basics of Operating Systems and Computer Networks.

4. COURSE OUTLINE (TOPICS):

The following list of topics is tentative.
Based on available time slots, some topics may be dropped or added or reordered.

Module 1: Overview **[2 Weeks = 6 Hours]**

Cyber security Concepts, Threats, Attacks, and Assets, Security Functional Requirements, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Security Strategy

Module 2: Security Layers **[2 Weeks = 6 Hours]**

Human factors in cyber security, Perimeter Security, Network Security, EndPoint Security, Application Security

Module 3: Data Security and Access Control **[2 Weeks = 6 Hours]**

Cryptography - symmetric and asymmetric encryption, basics of hashing, common use cases, Access Control - Authentication, Authorization

Module 4: Network Security **[2 Weeks = 6 Hours]**

Network Organization - Firewalls, Proxies, DMZ, Internet security protocols and standards, Intrusion detection and prevention

Module 5: Operating System Security **[2 Weeks = 6 Hours]**
Program Security: non-malicious program errors, viruses, controls against program threats; Protection in Operating Systems: protected objects, methods of protection, access control, authentication;

Module 6: Incident Response **[2 Weeks = 6 Hours]**
Incident Prioritization, Incident Handling, Disaster Recovery, Incident Response and Handling Process, Incident Management

5. TENTATIVE WEEKLY PLAN

Module	Week	Topics Scheduled to be Covered
1	1	Cyber security Concepts, Threats, Attacks, and Assets, Security Functional Requirements
	2	Fundamental Security Design Principles, Attack Surfaces and Attack Trees, Security Strategy
2	3	Human factors in cyber security, Perimeter Security, Network Security
	4	EndPoint Security, Application Security
3	5	Cryptography - symmetric and asymmetric encryption, basics of hashing, common use cases
	6	Access Control - Authentication, Authorization
4	7	Network Organization - Firewalls, Proxies, DMZ
	8	Internet security protocols and standards, Intrusion detection and prevention
5	9	Program Security: non-malicious program errors, viruses, controls against program threats;
	10	Protection in Operating Systems: protected objects, methods of protection, access control, authentication
6	11	Incident Prioritization, Incident Handling, Disaster Recovery
	12	Incident Response and Handling Process, Incident Management

6. BOOKS:

Text Books:

1. William Stallings and Lawrie Brown, Computer Security Principles and Practice, Pearson, 2014

Reference Books:

1. Matt Bishop, Introduction to Computer Security, Addison-Wesley, 2004

2. Ross Anderson, Security Engineering, Wiley, 2008
3. Douglas Robert Stinson and Maura Paterson. Cryptography Theory And Practice, CRC Press, 2018
4. William Stallings, Cryptography and Network Security: Principle and Practice, Pearson, 2013

7. EVALUATION:

Course grades will be based on the following tentative weightage pattern.

a) Examinations: 50%
Mid Semester Exam: 20%
End Semester Exam: 30%

b) Assignments: 25%

c) Class Participation (Surprise Quizzes): 10%

d) Scheduled Quizzes: 15%

8. COURSE OUTCOMES

At the end of the course, students should have the ability:

CO1: Ability to understand the basic concepts and layers of cyber security

CO2: Ability to understand the different tools and mechanisms used in cyber security including access control and cryptography

CO3: Ability to identify the appropriate security mechanisms/tools to handle different cyber security requirements

CO4: Ability to apply the suitable incident response strategy to handle cyber security incidents

9. ETHICS:

Please note down the following activities leading to a fair academic honesty:

a) All class work is to be done independently.

b) It is best to try to solve problems on your own, since problem solving is an important component of the course, and exam problems are often based on the outcome of the assignment problems.

c) You are allowed to discuss class material, assignment problems, and general solution strategies with your classmates. But, when it comes to formulating or writing solutions you must work alone.

d) You may use free and publicly available sources, such as books, journal and conference publications, and web pages, as research material for your answers. (You will not lose marks for using external sources.)

e) You may not use any paid service and you must clearly and explicitly cite all outside sources and materials that you made use of.

f) The use of uncited external sources as portraying someone else's work as your own is a violation of the University's policies on academic dishonesty.

g) Such Instances will be dealt with harshly and typically result in a failing course grade.