19CSE311	COMPUTER SECURITY	L-T-P-C: 3-0-0-3

Course Objectives

- This course provides basic knowledge and skills in the fundamental theories and practices of cyber security.
- It provides an overview of the field of security and assurance emphasizing the need to protect information being transmitted electronically.

Course Outcomes

CO1: Understand the fundamental concepts of computer security and apply to different components of computing systems.
CO2: Understand basic cryptographic techniques.
CO3: Understand how malicious attacks, threats, security and protocol vulnerabilities impact a system's Infrastructure.
CO4: Demonstrate knowledge in terms of relevance and potential of computer security for a given application.

CO-PO Mapping

PO/PSO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	1	1										3	2
CO2	3	3	3	1	2								3	2
CO3	3	3	3	2		2		3					3	2
CO4	3	3	1	2	3	2		2					3	2

Syllabus

Unit 1
Basics of Computer Security: Overview – Definition of terms – Security goals – Shortcomings – Attack and defense – Malicious code – Worms – Intruders – Error detection and correction Encryption and Cryptography: Ciphers and codes – Public key algorithms – Key distribution – Digital signatures.

Unit 2

Security Services: Authentication and Key Exchange Protocols - Access control matrix – User authentication – Directory authentication service – Diffie-Hellman key exchange – Kerberos.

Unit 3
System security and Security models: Disaster recovery - Protection policies. E-mail Security: Pretty good privacy - Database Security: Integrity constraints - Multi-phase commit protocols - Networks Security: Threats in networks - DS authentication -Web and Electronic Commerce: Secure socket layer - Client-side certificates - Trusted Systems : Memory protection.

Text Book(s)
Stallings William, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson/Prentice- Hall, 2018.

Reference(s)

Forouzan B A, Cryptography and Network Security, Special Indian Edition, Tata McGraw Hill, 2007.
Padmanabhan TR, Shyamala C K, and Harini N, Cryptography and Security, First Edition, Wiley India Publications, 2011.

Evaluation Pattern:

Assessment	Internal	External
Periodical 1 (P1)	15	
Periodical 2 (P2)	15	
*Continuous Assessment (CA)	20	
End Semester		50

*CA – Can be Quizzes, Assignment, Projects, and Reports.