22AIE314	COMPUTER SECURITY	L-T-P-C: 2- 0- 3- 3

Course Objective

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

Course Outcomes

After completing this course, the students will be able to

CO1: Implement cryptographic techniques in secure application development

CO2: Apply methods for authentication, access control, intrusion detection and prevention

CO3: Apply fundamental security principles to analyze threat situations

CO4: Design mechanisms to provide security in a network

CO-PO Mapping

PO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	2	-	2	2	1	1	1	-	-	-	1	1	-
CO2	3	3	2	3	3	3	2	1	2	1	-	-	-	1	2
CO3	3	3	3	3	3	3	2	3	3	3	-	-	-	2	3
CO4	3	3	1	2	3	2	1	1	1	1	-	-	-	-	-

Syllabus

Unit 1

Basics of Computer Security: Overview – Definition of terms – Security goals – Shortcomings – Attack and defence – 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.

Textbooks/References

William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 4th edition

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

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	Weightage (%)
Assignments (Minimum 2)	Internal	30
Quizzes (Minimum 2)	Internal	20
Mid-Term Examination	Internal	20
Term Project/ End Semester Examination	External	30