PROFESSIONAL ELECTIVES

Electives in Cyber Security

19CSE331	CRYPTOGRAPHY	L-T-P-C: 3-0-0-3

Pre-Requisite(s): 19MAT115 Discrete Mathematics

Course Objectives

- The course will cover how cryptography (symmetric and asymmetric) work, how security is analyzed theoretically, and how exploits work in practice.
- It will also present Cryptanalysis attacks against the cryptographic techniques, and attack models.

Course Outcomes

CO1: Understand classical cryptography techniques and apply cryptanalysis
CO2: Analyze measures for securing cryptosystem
CO3: Apply and analyze operations on Feistel and non-Feistel structures
CO4: Apply asymmetric encryption techniques for securing messages

CO-PO Mapping

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

Syllabus

Unit 1

Basics of number theory: Integers and operations on integers - Modular arithmetic - Prime Numbers - Primality related properties. Basic conventions and Terminology - Substitution Ciphers -Transposition ciphers - Rotor machines - Cryptanalysis.

Unit 2

Foundations of Modern Cryptography: Perfect Secrecy-Information and Entropy - Source Coding, Channel Coding, and Cryptography - Product cryptosystems. Symmetric Cryptosystems: Substitution Permutation Networks - DES and Enhancements - AES and its Modes.

Unit 3

Asymmetric Key Cryptography: Basic ideas of Asymmetric Key Cryptography - RSA Cryptosystem - Attacks on RSA Discrete Logarithm Problem and related algorithms – El-Gamal Cryptosystem – ECC. Digital Signatures and hash functions properties.

Text Book(s)

Stallings W. Cryptography and network security: principles and practice. Upper Saddle River: Pearson; 2018.
Padmanabhan TR, Shyamala C K, and Harini N. Cryptography and Security, First Edition, Wiley India Publications; 2011.

Reference(s)

Forouzan BA. Cryptography & network security. McGraw-Hill, Inc.; 2007 Feb 28.

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.