INFORMATION SYSTEM SECURITY

Subject Code: CS34212CS	Subject Type: Core
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 2-0-2

Pre-Requisites: Computer Networks, Operating Systems, Programming, Mathematical Foundations (Discrete Mathematics, Number Theory)

Course Objective: At the end of the course, the student will be able to:

CO-1	Understand and analyze classical and modern symmetric cryptographic techniques.
CO-2	Apply number theory and algebraic structures in the design and analysis of cryptographic algorithms.
CO-3	Analyze and implement public-key cryptographic algorithms and key exchange mechanisms.
CO-4	Evaluate advanced cryptographic systems, cryptanalysis techniques, and secure communication protocols.

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	2	2	1	2	1
CO-2	3	3	2	2	2	2
CO-3	3	3	3	2	2	2
CO-4	2	3	3	2	3	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Classical and Symmetric Cryptography

Introduction to cryptography; security goals and services; classical cryptosystems (substitution and transposition ciphers); cryptanalysis techniques (frequency analysis); Playfair cipher; block ciphers; Data Encryption Standard (DES), Triple DES; modes of operation (ECB, CBC, CFB, OFB); stream ciphers; pseudorandom sequence generation; Linear Feedback Shift Register (LFSR) based stream cipher.

Unit-2: Mathematical Foundations of Cryptography

Abstract algebra: groups, rings, and fields; modular arithmetic (addition, multiplication, exponentiation); prime numbers and factorization; group structures ($\mathbb{Z}n^*$, $\mathbb{Z}p^*$); cyclic groups; greatest common divisor (GCD) and Euclidean algorithms; multiplicative inverse; linear congruences; Chinese Remainder Theorem; Fermat's Little Theorem; Euler's theorem; quadratic residues; polynomial arithmetic; Advanced Encryption Standard (AES).

Unit-3: Public-Key Cryptography and Algorithms

Introduction to public-key cryptosystems; discrete logarithm problem (DLP); Diffie-Hellman key exchange; RSA cryptosystem; ElGamal cryptosystem; Rabin cryptosystem; knapsack cryptosystem; elliptic curve cryptography (ECC); primality testing; Legendre and Jacobi symbols; message authentication; digital signatures and authentication protocols.

Unit-4: Advanced Cryptography and Security Protocols

Key management and distribution; key exchange protocols; hash functions and secure hash algorithms (SHA); digital signature standards; cryptanalysis techniques (differential and linear cryptanalysis, memory trade-off attacks); secret sharing schemes (Shamir); identity-based encryption (IBE); attribute-based encryption (ABE); functional encryption; implementation attacks (side-channel attacks); network security protocols: SSL/TLS, PGP; secure communication mechanisms.

Learning Resources:

Text Books:

[1] Katz & Lindell – *Introduction to Modern Cryptography*
[2] Douglas Stinson – *Cryptography: Theory and Practice*
[3] Nigel Smart – *Cryptography: An Introduction*

Reference Books:

[1] Boneh & Shoup – *A Graduate Course in Applied Cryptography*
[2] Menezes, Van Oorschot – *Handbook of Applied Cryptography*