ELECTIVE-2

FOUNDATION OF MODERN CRYPTOGRAPHY AND APPLICATION

Subject Code: CS34221CS	Subject Type: Elective
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 3-0-0

Pre-Requisites: Discrete Mathematics, Probability & Statistics, Computer Networks, Operating System, Data Structures & Algorithms, and Programming

Course Objective: To provide students with a strong foundation in modern cryptographic principles, mathematical techniques, and security mechanisms used in contemporary Cyber Security systems. The course aims to introduce cryptographic algorithms, secure communication protocols, authentication mechanisms, and practical applications of cryptography in protecting digital information, networks, and computing infrastructures.

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

CO-1	Understand the fundamental concepts of modern cryptography, security goals, and mathematical foundations used in cryptographic systems.
CO-2	Analyze and apply symmetric and asymmetric cryptographic algorithms for secure communication and data protection.
CO-3	Understand cryptographic hash functions, digital signatures, key management, and authentication protocols used in modern security architectures.
CO-4	Evaluate the security of communication protocols and identify vulnerabilities, attacks, and cryptographic weaknesses in practical systems.
CO-5	Design and implement secure cryptographic solutions for real-world applications including network security, digital forensics, cloud systems, and cyber security infrastructures.

Course Articulation Matrix:

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

1- Slightly; 2 - Moderately; 3 - Substantially

Syllabus:

Unit-1 Introduction to Modern Cryptography and Mathematical Foundations:

Overview of Information Security and Security Goals, CIA Triad, Fundamentals of Cryptography, Symmetric Key Cryptography, Asymmetric Key Cryptography, Hardness of Computational Problems, One-Way Functions, Trapdoor Functions, Semantic Security (SS), Message Indistinguishability (MI), Equivalence of SS and MI, Hardcore Predicates, Goldwasser-Micali Encryption Scheme, Goldreich-Levin Theorem, Computational Complexity and Security Assumptions, Overview of Public Key Infrastructure (PKI), Introduction to Secure Communication Systems.

Unit-2 Cryptographic Security Models and Attack Frameworks:

Formal Security Definitions, Chosen Plaintext Attacks (IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2), Non-Malleability Attacks (NM-CPA and NM-CCA2), Relationships Among Security Models, Random Oracle Model, Provable Security Techniques, Security Reductions, Cryptographic Hash Functions, Password Security and Authentication Mechanisms, Secure Key Exchange Protocols, Steganography, Cryptographic Attack Taxonomy, Threat Modeling, Cryptanalysis Fundamentals, Security Analysis of Communication Protocols.

Unit-3 Pseudorandomness, Block Cipher Design, and Authentication Mechanisms:

Weak and Strong One-Way Functions, Pseudorandom Generators (PRGs), Blum-Micali-Yao Construction, Construction of Secure PRGs, Relationship Between One-Way Functions and PRGs, Pseudorandom Functions (PRFs), Pseudorandom Permutations (PRPs), Luby-Rackoff Construction, Feistel Networks, Design Principles of Block Ciphers, DES and AES Architecture, Left-or-Right Security (LOR), Message Authentication Codes (MACs), Weak and Strong MAC Definitions, Variable Length MACs, Digital Signatures, Signing and Verification Algorithms, Full Domain Hashing, Secure One-Time Signature Schemes, Secret Sharing Schemes including Shamir's Secret Sharing.

Unit-4 Advanced Cryptographic Protocols and Applications:

Formal Analysis of Cryptographic Protocols, Zero Knowledge Proofs and Interactive Protocols, Secure Multi-Party Computation Basics, Authentication and Authorization Systems, Blockchain and Cryptocurrency Security, Cryptography in Cloud Computing, Network Security Applications, Cryptography for Digital Forensics, Cryptographic Protocols for IoT Devices, AI-Assisted Security Mechanisms, Emerging Trends in Modern Cryptography, Post-Quantum Cryptography, Secure Electronic Transactions, Privacy-Preserving Systems, Cryptographic Applications in Cyber Security and Digital Evidence Protection.

Learning Resources:

Text Books:

1. Introduction to Modern Cryptography — Jonathan Katz and Yehuda Lindell, CRC Press.
2. Introduction to Cryptography: Principles and Applications — Hans Delfs and Helmut Knebl, Springer Verlag.
3. Modern Cryptography: Theory and Practice — Wenbo Mao, Pearson Education.

4. Lecture Notes on Cryptography — Shaffi Goldwasser and Mihir Bellare.
5. Foundations of Cryptography — Oded Goldreich, CRC Press, Part-I and Part-II.

Reference Books:

1. Cryptography and Network Security — William Stallings, Pearson Education.
2. Understanding Cryptography — Christof Paar and Jan Pelzl, Springer.
3. Applied Cryptography — Bruce Schneier, Wiley Publications.
4. Introduction to Mathematical Cryptography — Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman, Springer.
5. Serious Cryptography — Jean-Philippe Aumasson, No Starch Press.