MCPE2002 CRYPTOGRAPHIC FOUNDATIONS (3-0-0)

Course Description : The course introduces the underlying the principles and design of cryptosystems. The course covers the basics concepts of cryptography including: traditional ciphers, block ciphers, stream ciphers, public and private key cryptosystems. The course also includes the theory of hash functions, authentication systems, network security protocols and malicious logic.

Course Objectives:

After learning the course the students should be able to:

- Understand the principles and practices of cryptographic techniques.
- Understand information security goals for designing secure systems.
- Apply security algorithms in solving real-life security problems in communicating systems.
- Understand different cryptographic techniques based on asymmetric key encryption.

Module-I

Introduction: What is modern cryptography, Historical ciphers and their cryptanalysis, The heuristic versus the rigorous approach; adversarial models and principles of defining security

Perfectly-Secret Encryption: Definitions, the one-time pad; proven limitations

Private-Key (Symmetric) Encryption: Computational security, Defining secure, encryption, Constructing secure encryption; pseudo randomness, Stronger security notions, Constructing CPA-secure encryption, Modes of operation; CBC vs. CTR, Security of CTR with n − k bit counter for messages to size 2k blocks with proof directly to the LR definition, CCA attacks.

Module-II

Message Authentication Codes: Message integrity, Definition of security, Constructions from pseudorandom functions, CBC-MAC, Authenticated encryption.

Collision-Resistant Hash Functions: Definitions, The Merkle-Damgard transform, HMAC, Birthday attacks, The Random oracle model, Password hashing, Constructions of Pseudorandom Permutations (Block Ciphers) in Practice, Substitution-permutation and Feistel networks, DES and attacks on reduced-round versions, double-DES and triple-DES, AES, Hash functions from block ciphers.

Module-III

Number Theory: Preliminaries and basic group theory, Primes, factoring and RSA, Cryptographic assumptions in cyclic groups, Collision-resistant hash functions from discrete log, Public-Key (Asymmetric) Cryptography: Introduction and motivation, Diffie-Hellman key exchange

Module-IV

Public-Key (Asymmetric) Encryption: The model and definitions, Hybrid encryption and KEM/DEM, El Gamal, RSA: textbook encryption, attacks on textbook RSA, padded RSA; CCA-secure RSA KEM.Digital Signatures: Definition and applications, Hash and sign, RSA signatures: textbook RSA, hashed RSA, security with ROM, Certificates and public-key infrastructures.

Text Book

1. Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, second edition 2014, CRC Press.

Reference Books

1. Cryptography: Theory and Practice by Douglas Stinson, Third edition, CRC Press.
2. Handbook of Applied Cryptography by Alfred Menezes, Paul Oorschot and Scott Vanstone. Available Online.
3. Foundations of Cryptography by Oded Goldreich. Available Online.
4. Cryptography, an Introduction by Nigel Smart. Available Online