PIS 104: CRYPTOGRAPHY

L	T	P	Cr
3	0	2	4.0

Course Objectives: This course provides an introduction to the core cryptographic techniques and the different security services they provide, together with an overview of the key management principles and techniques. It also gives an insight into the design and working of different cryptographic methods.

Introduction: History and Overview of Cryptography, Historical Ciphers and Their Cryptanalysis, Definition of Perfect Secrecy, Shanon's Theorem, Basic Principles of Modern Cryptography

Private Key Cryptography: Private Key Encryption, Computational Approach to Cryptography, Pseudo Randomness, Constructing Secure Encryption Schemes, Chosen Plaintext Attacks, CPA Secure Encryption Schemes, Chosen Cipher Text Attacks, Security Against CCA, Limitations of Private Key Cryptography

Message Integrity: Definition and Applications, Message Authentication Codes, Constructing Secure Message Authentication Codes, Collision Resistant Hashing, Collision Resistant Hashing Functions

Block Ciphers: Feistel Networks, Data Encryption Standard (DES): Design and Security, Advanced Encryption Standard: Design and Security, One Way Functions, Construction of Pseudorandom Generators, Construction of Pseudorandom Functions, Construction of Pseudorandom Permutations

Public Key Cryptography: Basic Group Theory, Primes, Factoring, Cyclic Groups, Discrete Logarithms, Cryptography Using Arithmetic Modulo Primes, Arithmetic Modulo Composites, RSA Public Key Encryption, Security Against Active Attacks, Attacks on RSA, El Gamal Encryption Schemes, Recent Public Key Encryption Schemes

Digital Signatures: Definitions and Applications, Lamport and Merkle Schemes. Overview of Signatures Based on Discrete-Log Certificates and Trust Management. , SSL/TLS and Ipsec, Privacy Mechanisms

Advanced Topics: ECC, DNA Cryptography, Quantum Cryptography, Digital Watermarking and Steganography etc

Recommended Books

1. Introduction to modern cryptography by J. Katz and Y. Lindell, Chapman and Hall/CRC, 2nd Edition,2014
2. Handbook of applied cryptography by A. Menezes, P. Vanoorschot, S. Vanstone, CRC Press, 1st Edition, 1996
3. Cryptography and network security: principles and practice, William Stalling, Prentice Hall, 6th Edition,2013