Cryptography & Network Security
CS801D
Contracts: 3L
Credits- 3

Total: - 38 Lectures

Module1: Attacks on Computers & Computer Security (5L)
Introduction, Need for Security, Security approaches, Principles of Security, Types of attack.

Module2: Cryptography: Concepts & Techniques (7L)
Introduction, Plaintext & Cipher text, Substitution Techniques, Transposition Techniques, Encryption & Decryption, Symmetric & Asymmetric key Cryptography, Key Range & Key Size

Module3: Symmetric Key Algorithm (8L)
Introduction, Algorithm types & Modes, Overview of Symmetric Key Cryptography, DES(Data Encryption Standard) algorithm, IDEA(International Data Encryption Algorithm) algorithm, RC5(Rivest Cipher 5) algorithm.

Module4: Asymmetric Key Algorithm, Digital Signature and RSA (5L)
Introduction, Overview of Asymmetric key Cryptography, RSA algorithm, Symmetric & Asymmetric key Cryptography together, Digital Signature, Basic concepts of Message Digest and Hash Function (Algorithms on Message Digest and Hash function not required).

Module5: Internet Security Protocols, User Authentication (6L)
Basic Concepts, SSL protocol, Authentication Basics, Password, Authentication Token, Certificate based Authentication, Biometric Authentication.

Module6 : Electronic Mail Security (4L)
Basics of mail security, Pretty Good Privacy, S/MIME.

Module7: Firewall (3L)
Introduction, Types of firewall, Firewall Configurations, DMZ Network

Text :
1. “Cryptography and Network Security”, William Stallings, 2nd Edition, Pearson Education Asia
2. “Network Security private communication in a public world”, C. Kaufman, R. Perlman and M. Speciner, Pearson
3. Cryptography & Network Security: Atul Kahate, TMH.

Reference :
1. “Network Security Essentials: Applications and Standards” by William Stallings, Pearson
2. “Designing Network Security”, Merike Kaeo, 2nd Edition, Pearson Books
3. “Building Internet Firewalls”, Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2nd Edition, Oreilly
4. “Practical Unix & Internet Security”, Simson Garfinkel, Gene Spafford, Alan Schwartz, 3rd Edition, Oreilly
Module6 : Electronic Mail Security (4L)