4/4 B.Tech - FIRST SEMESTER

IT7T6E CRYPTOGRAPHY AND NETWORK SECURITY Credits:3

Lecture: 3 Periods/week Internal assessment: 30 marks

Practice/Interaction: 1Period/week Semester end examination: 70 marks

Objectives:

- To discuss the tradeoffs inherent in security.
- To explain the issues in creating security policy for a large organization.
- To defend the need for protection and security, and the role of ethical considerations.
- To discuss the fundamental ideas of public-key cryptography and simple extensions of cryptographic protocols.

Outcomes:

Students will be able to

- Get idea on security aspects and classical encryption techniques.
- Apply encryption and decryption techniques.
- Understand the key exchange and key generation mechanisms.
- Understand the hash functions and authentication mechanisms.
- Understand the concepts of email and network security.

Prerequisites:

Discrete Mathematics, Data Communication and Computer Networks.

Syllabus:

UNIT-I

INTRODUCTION: The OSI security architecture, security attacks, security services, security mechanisms, a model for network security.

CLASSICAL ENCRYPTION TECHNIQUES: Symmetric cipher model, Substitution techniques, Transposition techniques, stream and block cipher, steganography.

UNIT-II

BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD: Block cipher principles, Data Encryption Standard: Strength of DES, Avalanche effect, AES Algorithm, Modern symmetric key ciphers

UNIT-III

NUMBER THEORY: Fermats and Euler's theorems, Chinese remainder theorem, RSA algorithm, Diffie-hellman key exchange, Introduction to elliptic curve cryptography, Elliptic curves-Real numbers, GF(P),GF(2^n).

UNIT-IV

AUTHENTICATION APPLICATIONS: Message Integrity, Message Authentication, HMAC, SHA-512,Digital Signature Schemes, X.509 Directory Service, Symmetric Key Management and Distribution, Kerberos, Symmetric key Agreement.

UNIT-V

ELECTRONIC MAIL SECURITY

Network Security: E-mail, PGP, S/SIME.

System Security: Worms, Viruses, Intrusion Detection System.

Text Books:

1. Cryptography and Network Security, 2nd Edition, Behrouz A. Forouzan, Debdeep Mukhopadhyay
2. Cryptography and Network Security, William Stallings, 4th Edition, Pearson Education.

Reference Books:

1. Cryptography & Network Security, Behrouz A. Forouzen, TMH.
2. NETWORK SECURITY, Kaufman, Perlman, Speciner, 2nd Edition, PHI/Eastern Economy Edition
3. Introduction to Cryptography with Coding Theory, Trappe&Washington,2nd Edition,Pearson.

e-Learning Resources:

1. http://nptel.ac.in/courses/106105031/
2. http://searchsecurity.techtarget.com/Understanding-encryption-and-cryptography-basics
3. http://freevideolectures.com/Course/3027/Cryptography-and-Network-Security