7th Semester

Information Security

Credit=4+2

Unit-I

Introduction to Concept of Security, Need for Security, Security Approaches (Security Models, Security Management Practices), Principles of Security, Types of Attacks (Theoretical Concepts, Practical Side of Attacks, Packet Sniffing, Packet Spoofing), Introduction to Cryptology, Cryptanalysis, Steganography

Unit-II

Introduction to Cryptographic Techniques, Plain Text, Cipher Text, Substitution Techniques, Transposition Techniques, Encryption, Decryption, Symmetric Key Cryptography (Overview of DES), Key Range, Key Size, Possible Types of Attacks, Stream & Block Ciphers

Unit-III

Public and Private Key Encryption Schemes, RSA Algorithm, Digital Signatures, Overview of Knapsack Algorithm, Public Key Infrastructure (PKI), Digital Certificates, Private Key Management, Diffie-Hellman Key Exchange Algorithm, PKIX Model. Authentication Protocols, Authentication Requirements,. Authentication Functions, Message Authentication Codes, Cryptographic Hash, Message Digest Algorithms, MD5.

Unit-IV

Internet Security Protocols, Secure Socket Layer(SSL), Secure Hyper Text Transfer Protocol (Shttp), Time Stamping Protocol (TSP), Secure Electronic Transaction (SET), Electronic Money, Email Security, Wireless Application Protocol (WAP) Security. Network Security, Kerberos, X.509 Directory Authentication Service, Electronic Mail Security, PGP , Overview of IP Security, IP Security Architecture, Authenticatior Header, Encapsulation Security Payload.

References:

1. William Stallings, Cryptography and Network Security: Principles and Practices, 7th Edition, PHI

2. Atul Kahate, Cryptography and Network Security, 4th Edition, TMH,.

3. Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, 4th Edition, CENGAGE Learning.