CS010 803: Security in Computing

Module 1 (12 hours)

Introduction: Security basics – Aspects of network security – Attacks Different types –Security

attacks -Security services and mechanisms.

Cryptography: Basic Encryption & Decryption – Classical encryption techniques – symmetric

encryption, substitution ciphers – Caesar cipher – Monoalphabetic Cipher, Playfair Cipher,

Polyalphabetic cipher - Vigenère – Cipher, Transposition ciphers - Rail Fence cipher, Row

Transposition Ciphers.

Module 2 (12 hours)

Modern Block Ciphers - Fiestel Networks , DES Algorithm – Avalanche Effect.

Introduction to Number Theory - Prime Factorisation, Fermat's Theorem, Euler's Theorem,

Primitive Roots, Discrete Logarithms.

Public key Cryptography:- Principles of Public key Cryptography Systems, RSA algorithmsKey Management – Diffie-Hellman Key Exchange, Elliptic curve cryptography.

Module 3 (12 hours)

Message Authentication-Requirements- Authentication functions- Message authentication

codes-Hash functions- Secure Hash Algorithm, MD5, Digital signatures- protocols- Digital

signature standards, Digital Certificates.

Application Level Authentications- Kerberos, X.509 Authentication Service, X.509

certificates.

Module 4 (12 hours)

Network Security: Electronic Mail Security, Pretty Good Privacy, S/MIME, IP Security

Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload.

Web Security: Web Security considerations- Secure Socket Layer -Transport layer SecuritySecure electronic transaction. Firewalls-Packet filters- Application Level Gateway- Circuit

Level Gateway.

Module 5 (12 hours)

Operating System Security: Memory and Address Protection, Control of Access to General

Objects, File Protection Mechanisms, Models of Security – Bell-La Padula Confidentiality

Model and Biba Integrity Model.

System Security: Intruders, Intrusion Detection, Password Management, Viruses and Related

Threats, Virus Countermeasure.

Reference Books

1. William Stallings, “Cryptography and Network Security – Principles and Practices”, Pearson Education, Fourth Edition, 2006.
2. Charles P. Pfleeger, “Security in Computing”, Pearson Education, Third Edition, 2005.
3. Behrouz A. Forouzan, Dedeep Mukhopadhyay “Cryptography & Network Security”, Second Edition,Tata McGraw Hill, New Delhi, 2010.
4. Andrew S. Tanenbaum, “Modern Operating Systems”, Pearson Education, Second Edition,
5. 2002.
6. Atul Kahate, “Cryptography and Network Security”, Second Edition, Tata McGraw Hill

7. Wenbo Mao, " Modern Cryptography- Theory & Practice", Pearson Education, 2006.
8. Bruce Schneier, "Applied Cryptography", John Wiley and Sons Inc, 2001.