II YEAR – III SEMESTER
COURSE CODE: 7MCE3C1

CORE COURSE-X–CRYPTOGRAPHY AND NETWORK SECURITY

Unit I

Overview: Computer Security Concepts – 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 – Rotor Machines – Stenography.

Unit II

Block Ciphers and the Data Encryption Standard: Block Cipher Principle – The data encryption Standard – The strength of DES – Differential and Linear Cryptanalysis – Block Cipher Design Principles – Advanced Encryption Standard: Finite Field Arithmetic – AES structure – AES transformation function – AES key expansion – AES implementation.

Unit III

Public-key Cryptography and RSA: Principles of Public-Key Cryptosystems – The RSA algorithm – Other Public key Cryptosystems: Diffie-Hellman Key exchange – ElGamal Cryptographic system – Elliptic curve Arithmetic – Elliptic Curve Cryptography – Pseudorandom Number Generation Based on an Asymmetric cipher.

Unit IV

Message Authentication Codes: Message Authentication Requirements – Message Authentication Functions – Requirements for Message Authentication Codes – Security of MACs – MACs Based Hash Functions – MACs Based Ciphers – Authenticated encryption – Digital Signatures: Digital Signatures – ElGamal Digital Signature Scheme – Schnorr Digital Signature Scheme – Digital signature Standard.

Unit V

Transport Level Security: Web Security Considerations – Secure Socket Layer and Transport Layer security – Transport Layer Security – Electronic Mail Security: Pretty Good privacy – S/MIME – Domain Keys Identified mail – IP security: IP security Overview – IP Security Policy – Encapsulating Security Payload.

Text Book:

1. William Stallings, “Cryptography and Network Security Principles and Practice”, Pearson, 5th Edition.

Book for Reference:

1. William Stallings - “Data Communication” - Pearson

♣♣♣♣♣♣♣♣♣♣