5MCACC2: NETWORK INFORMATION SECURITY

Total No. of Hours: 52 **Hours/Week: 04**

Course Objective: To introduce the concept of network security and techniques

Course Outcome: Students will be able to

CO1: Identify and classify computer and security threats and understand the concept of encryption and decryption

CO2: Apply modern algebra and number theory to understanding of cryptographic algorithms and vulnerabilities

CO3: Examine and understand the techniques and algorithms used for message authentication:MAC, Digital Signatures and Hash functions.

CO4: Understand the need for Kerberos authentication and the techniques involved.

CO5: Familiarize with network security designs using available secure solutions such as PGP, SSL, IPSec, etc.

Unit I	**Introduction to Computer Security**: Computer concepts, The OSI Security architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. **Classical Encryption Techniques**: Symmetric Cipher Models, Substitution techniques, Transposition techniques, Steganography. Block Ciphers and Data Encryption Standards: Block Cipher Principles, Data Encryption Standard (DES) Operation, DES Example, The strength of DES. **Advanced Encryption Standard(AES):** AES structure, AES example	12 hrs
Unit II	**Introduction To Number Theory:** Prime Numbers, Fermat's and Euler's theorem. **Public key Cryptography and RSA**: Principles of Public Key Cryptosystems, The RSA Algorithm. **Other Public key cryptosystems**: Diffie Hellman Key Exchange. **Cryptographic Hash Functions**: Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	10 hrs
Unit III	**Message Authentication Codes**: Message Authentication Requirements, Message Authentication Functions, Requirements for Security of MACs **Digital Signature**: Concepts of Digital Signature, Digital Signatures Standard	10 hrs
Unit IV	**Key Management and Distribution**: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Public Key Infrastructure. **User Authentication**: Remote user Authentication Principles, Remote User-Authentication Using Symmetric Encryption, Kerberos, Remote User-Authentication Using Asymmetric Encryption, Federated Identity Management.	10 hrs
Unit V	**Transport-Level Security**: Web security Considerations, Secure Socket Layer and Transport layer Security, Transport Layer Security. **E-Mail Security**: Pretty Good Privacy, S/MIME. **IP Security**: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange	10 hrs

REFERENCE BOOKS

[1] William Stallings, “*Cryptography and Network Security”*, PHI, Fifth Edition,2011

[2] AtulKahate, “*Cryptography and Network Security”*, Tata McGraw- Hills, Eighth Reprint, 2006.

[3] Eric Maiwald, “*Information Security Series*, *Fundamental of Network security”*, DreamtechPress