I Year I Semester	L	P	C
Code: 17ES132	4	0	3

NETWORK SECURITY & CRYPTOGRAPHY
(ELECTIVE-I)

UNIT-I: Introduction

Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork security. Classical Techniques: Conventional Encryption model, Steganography, Classical Encryption Techniques.

UNIT-II:

Modern Techniques:

Simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operations.

Algorithms:

Triple DES, International Data Encryption algorithm, Blowfish, RC5, CAST-128, RC2, Characteristics of Advanced Symmetric block cifers.

Conventional Encryption:

Placement of Encryption function, Traffic confidentiality, Key distribution, Random Number Generation.

Public Key Cryptography:

Principles, RSA Algorithm, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptography.

UNIT-III:

Number Theory:

Prime and Relatively prime numbers, Modular arithmetic, Fermat‟s and Euler‟s theorems, Testing for primality, Euclid‟s Algorithm, the Chinese remainder theorem, Discrete logarithms.

Message authentication and Hash Functions:

Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash functions and MACs.

UNIT-IV:

Hash and Mac Algorithms: MD File, Message digest Algorithm, Secure Hash Algorithm, RIPEMD-160, HMAC.

Digital signatures and Authentication Protocols: Digital signatures, Authentication Protocols, Digital signature standards.

Authentication Applications: Kerberos, X.509 directory Authentication service. Electronic Mail Security: Pretty Good Privacy, S/MIME.

UNIT-V:

IP Security: Overview, Architecture, Authentication, Encapsulating Security Payload, Combining security Associations, KeyManagement.

Web Security: Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction.

Intruders, Viruses and Worms: Intruders, Viruses and Related threats.

Fire Walls: Fire wall Design Principles, Trusted systems.

TEXT BOOKS:

1. Cryptography and Network Security: Principles and Practice - William Stallings, 2000,PE.

REFERENCE BOOKS:

1. Principles of Network and Systems Administration, Mark Burgess,JohnWiey.