K L University
Department of Electronics & Computer Engineering
M.Tech (Embedded Systems)

Course No. : **15-EM52C3**
Course Title : **Cryptography & Network Security**
Course Structure : **3-0-0**
SYLLABUS:

UNIT-I

Introduction: Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetworksecurity. Classical Techniques: Conventional Encryption model, Steganography, Classical EncryptionTechniques.

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, and 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, Key Management
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 Book:

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

References:

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