KL University
Department of Electronics & Computer Engineering
M.Tech (wcsn) First Semester 2015-2017

Course Code	**: 15-EM51E2**
Course Title	**: Cryptography wireless security**
Course Structure	**: 3-0-0**
Credits	**: 3**

SYLLABUS:

Unit 1: Introduction and Symmetric Key Encryption

Attacks-Services-Mechanisms-OSI Security architecture-Model for Network Security-Symmetric Cipher Model- Substitution and Transposition Techniques- Simplified DES-DES Block Cipher Principles-The Strength of DES-Differential and Linear Cryptanalysis-Block Cipher Design Principles- Block Cipher Modes of Operation- -AES cipher-Triple DES.

Unit 2: Number Theory and Public Key Encryption

Prime Numbers-Fermat’s and Euler’s Theorems-Testing of Primality-The Chinese Remainder Theorem-Discrete Logarithms-Principles of Public Key Cryptosystems-The RSA Algorithm-Key Management-Diffie-Hellman Key Exchange-Elliptic Curve Arithmetic- Elliptic Curve Cryptography.

Unit 3: Message Authentication and Hash Functions

Authentication Requirements- Authentication functions-message Authentication Codes- Hash Functions- Security of Hash Functions and MACs-MD5 Message Digest Algorithm-Digital Signatures- Authentication Protocols-Digital Signature Standard.

Unit 4: Network Security Practice

Authentication Application-Kerberos-Electronic Mail Security-Pretty Good Privacy-S/MIME-IP Security Overview-IP Security Architecture-Authentication Header Encapsulation Security Payload- Web Security Considerations-Secure Sockets Layer and Transport Layer Security-Secure Electronic Transaction.

Unit 5: System Security

Intruders- Intrusion Detection-Password Management-Viruses and Related Threats-Viruses Counter Measures-Firewall Design Principles-Types of Firewalls-Firewalls Configurations-Trusted Systems

Text book:

1. William Stallings, “Cryptography and Network Security-Principles and practice”, 3rd Edition Prentice Hall, 2003.

Reference Books:

1. Michael E.Whitman and Herbert J.Mattord, “Principles of Information security,” 1st Edition, 2003.
2. Bruce Schneier,”Applied Cryptography,” 2nd Edition, Toha Wiley and Sons, 1996