Subject Name: EC2035 Cryptography and Network Security

Staff Name : V.Thiyagarajan, AssistantProfessor

Year : Final Year –ECE ‘B’ Section

**Syllabus:**

**UNIT I INTRODUCTION**

OSI Security Architecture - Classical Encryption techniques – Cipher Principles – DataEncryption Standard – Block Cipher Design Principles and Modes of Operation -Evaluation criteria for AES – AES Cipher – Triple DES – Placement of EncryptionFunction – Traffic Confidentiality

**UNIT II PUBLIC KEY CRYPTOGRAPHY**

Key Management - Diffie-Hellman key Exchange – Elliptic Curve Architecture andCryptography - Introduction to Number Theory – Confidentiality using SymmetricEncryption – Public Key Cryptography and RSA.

**UNIT III AUTHENTICATION AND HASH FUNCTION**

Authentication requirements – Authentication functions – Message Authentication Codes– Hash Functions – Security of Hash Functions and MACs – MD5 message Digestalgorithm - Secure Hash Algorithm – RIPEMD – HMAC Digital Signatures –Authentication Protocols – Digital Signature Standard

**UNIT IV NETWORK SECURITY**

Authentication Applications: Kerberos – X.509 Authentication Service – Electronic MailSecurity – PGP – S/MIME - IP Security – Web Security.

**UNIT V SYSTEM LEVEL SECURITY**

Intrusion detection – password management – Viruses and related Threats – VirusCounter measures – Firewall Design Principles – Trusted Systems**.**

**TEXT BOOKS** 1. William Stallings, “Cryptography And Network Security – Principles and Practices”,

Pearson Education, Third Edition, 2003.

2. Behrouz A. Foruzan, “Cryptography and Network Security”, Tata McGraw-Hill, 2007

**REFERENCES:**

1. Bruce Schneier, “Applied Cryptography”, John Wiley & Sons Inc, 2001.

2. Charles B. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing”, Third Edition,

Pearson Education, 2003

3. Wade Trappe and Lawrence C. Washington , “ Introduction to Cryptography with

4. coding theory” , Pearson Education, 2007.

5. Wenbo Mao, “ Modern Cryptography Theory and Practice” , Pearson Education,

2007

6. Thomas Calabrese, “Information Security Intelligence : Cryptographic Principles and

Applications”, Thomson Delmar Learning,2006.

7. AtulKahate, “Cryptography and Network Security”, Tata McGraw-Hill,