PIT7J001 Cryptography & Network Security 3-0-0

OBJECTIVES: The student should be made to:

- Understand OSI security architecture and classical encryption techniques.
- Acquire fundamental knowledge on the concepts of finite fields and number theory.
- Understand various block cipher and stream cipher models.
- Describe the principles of public key cryptosystems, hash functions and digital signature.
- Module I : INTRODUCTION & NUMBER THEORY [10 hours]

Services, Mechanisms and attacks-the OSI security architecture-Network security model- Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography).FINITE FIELDS AND NUMBER THEORY: Groups,
Rings, Fields-Modular arithmetic-Euclid‟s algorithm-Finite fields- Polynomial Arithmetic –

Prime numbers-Fermat‟s and Euler‟s theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms.

Module II : BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY [10 hours]

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management – Diffie Hellman Key exchange-Elliptic curve arithmetic-Elliptic curve cryptography.

Module III : HASH FUNCTIONS AND DIGITAL SIGNATURES [10 hours]

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD5 – SHA – HMAC – CMAC – Digital signature and authentication protocols
– DSS – EI Gamal – Schnorr.

SECURITY PRACTICE & SYSTEM SECURITY [8 hours]

Authentication applications – Kerberos – X.509 Authentication services – Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls – Firewall designs – SET for E-Commerce Transactions. Intruder – Intrusion detection system – Virus and related threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of cryptography and security.

Module IV : E-MAIL, IP & WEB SECURITY [9 hours]

E-mail Security: Security Services for E-mail-attacks possible through E-mail – establishing keys privacy-authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy- S/MIME. IPSecurity: Overview of IPSec – IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSLAttacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET).
TOTAL: 45 PERIODS

OUTCOMES: Upon Completion of the course, the students should be able to:

- Compare various Cryptographic Techniques
- Design Secure applications

-

TEXT BOOKS:

William Stallings, Cryptography and Network Security, 6th Edition, Pearson Eat, March 2013. (UNIT I,II,III,IV