7^{th} Semester	RIT7D003	Network Security	L-T-P 3-0-0	3 Credits

Module I : **[10 hours]**

INTRODUCTION & NUMBER THEORY

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 **[12 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

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 **[8 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 SSL Attacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET).

Books:

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013. (UNIT I,II,III,IV).
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002. (UNIT V).
3. Behrouz A. Ferouzan, “Cryptography & Network Security”, Tata Mc Graw Hill, 2007.
4. Man Young Rhee, “Internet Security: Cryptographic Principles”, “Algorithms and Protocols”, Wiley Publications, 2003.
5. Charles Pfleeger, “Security in Computing”, 4th Edition, Prentice Hall of India, 2006.