**Information & Cyber Security**

**Unit I:** Need of Information Security: Legal, Ethical and Professional Issues Attributes of security- authentication, access control, confidentiality, authorization, integrity, non-reproduction. OSI Security Architecture: attacks, services and mechanisms. Security Attacks, Security services, A model of Internetwork Security. Conventional Encryption: Classical Encryption Techniques and Problems on classical ciphers, Security architecture.

**Unit II:** Introduction to Secret key and cryptography, Encrypt given messages using DES, AES, IDEA, Problems on cryptography algorithms, Principles, finite fields, stream cipher, block cipher modes of operation, DES, Triple DES, AES, IDEA, RC5, key distribution.

**Unit III:** Introduction to Public key and Cryptography, Encrypt given messages using ECC, Problems on key generation, cryptography algorithms Principles, Introduction to number theory, RSA- algorithm, security of RSA, Key management- Diffie-Hellman key exchange, man-in-the-middle attack, Elliptical curve cryptography

**Unit IV:** Message Authentication and Hash Functions: Authentication Requirements and Functions, Hash Functions and their Security, MD5 Message Digest Algorithm, Kerberos. Key Management: Digital Certificates-Certificate types, X.509 Digital Certificate format, Digital Certificate in action, Public Key Infrastructure-Functions, PKI Architecture, Certificate Authentication.

**Unit V:** Introduction to Network, Transport and Periphery Security, Study of IPSEC, TLS, and SSL. Firewalls - design principles, trusted systems, Intrusion Detection System, Intrusion Prevention System. Implementation and analysis of IPSEC, TLS and SSL, Introduction to cryptography - Classical cryptography. 29

**Unit VI:** Software Vulnerability: Phishing, Buffer Overflow, Cross-site Scripting (XSS), SQL Injection. Electronic Payment: Payment Types, Enabling Technologies-Smart Cards and Smart Phones, Cardholder Present E-Transaction-Attacks, Chip Card Transactions, Payment over Internet-Issues and Concerns, Secure Electronic Transaction, Online Rail Ticket Booking. Electronic Mail Security: Pretty Good Privacy, S/MIME

**Text Book:** 1. Cryptography and network security - principles and practices, William Stallings, Pearson Education, 2002.

**Reference Books:** 1. Network Security and Cryptography, Bernard Menezes, Cengage Learning.

 2. Information System Security, Nina Godbole, Wiley India, 2008.

3. Network security, private communication in a public world, Charlie Kaufman, Radia Perlman and Mike Speciner, Prentice Hall, 2002.

4. Security architecture, design deployment and operations, Christopher M. King and Curtis Patton, RSA press, 2001.

5. Network Security - The Complete Reference, Robert Bragg and Mark Rhodes, Tata McGraw Hill, 2004.