CRYPTOGRAPHY AND NETWORK SECURITY

Module 1 10Hrs

Introduction to Information Security: Security Goals, Attacks, Security Services and Mechanisms, **Mathematical Background**: Integer and Modular Arithmetic, Matrices, Linear Congruence. Groups, Rings, and Fields, GF(p), Euclidean and Extended Euclidean Algorithms, Polynomial Arithmetic, GF(2n). Random Number Generation, Prime Numbers, Fermat's and Euler's Theorems, Primality Testing Methods, Factorization, Chinese Remainder Theorem, Quadratic Congruence, Discrete Logarithms.

Module 2 10Hrs

Traditional Encryption Methods: Symmetric Cipher Model, Substitution Ciphers, Transposition Ciphers, Block and Stream Ciphers, Rotor Cipher, Steganography. **Symmetric Key Ciphers**: Data Encryption Standard, Advanced Encryption Standard. **Asymmetric Key Ciphers**: RSA Cryptosystem, ElGamal Cryptosystem, Elliptic Curve Cryptosystem.**Message Integrity, Authentication**: Message Integrity, Random Oracle Model, Message Authentication, MAC Algorithms. Cryptographic Hash Functions: MD Hash Family, Whirlpool, Secure Hash Algorithm. Digital Signature and Authentication: Digital Signature Schemes, Variations and Applications, Entity Authentication.Key Management: Diffie-Hellman Key Exchange.

Module 3 10Hrs

Network and System Security:Security at the Application Layer: e-mail security, PGP and S/MIME. Security at the Transport Layer: Secure Socket Layer (SSL) and Transport Layer Security (TLS). Security at the Network Layer: IP Security. **System Security**: Malicious Software, Malicious Programs, Viruses, Worms, Malware, Intrusion Detection System, Firewalls.

Text Books:

1. B. A. Forouzan & D Mukhopadhyay ,Cryptography and Network Security., McGraw Hill, 2nd ed.2010

References:

1. B. Menezes ,Network Security and Cryptography., Cengage Learning, 1st ed.2010
2. Stallings ,Cryptography and Network Security., PHI, 4th ed.2010