IT2352 CRYPTOGRAPHY AND NETWORK SECURITY L T P C

3 0 0 3

UNIT I 9

Security trends – Attacks and services – Classical crypto systems – Different types of ciphers – LFSR sequences – Basic Number theory – Congruences – Chinese Remainder theorem – Modular exponentiation – Fermat and Euler's theorem – Legendre and Jacobi symbols – Finite fields – continued fractions.

UNIT II 9

Simple DES – Differential cryptoanalysis – DES – Modes of operation – Triple DES –AES – RC4 – RSA – Attacks – Primality test – factoring.

UNIT III 9

Discrete Logarithms – Computing discrete logs – Diffie-Hellman key exchange – ElGamal Public key cryptosystems – Hash functions – Secure Hash – Birthday attacks - MD5 – Digital signatures – RSA – ElGamal – DSA.

UNIT IV 9

Authentication applications – Kerberos, X.509, PKI – Electronic Mail security – PGP, S/MIME – IP security – Web Security – SSL, TLS, SET.

UNIT V 9

System security – Intruders – Malicious software – viruses – Firewalls – Security Standards.

TOTAL:45 PERIODS

TEXT BOOKS:

1. Wade Trappe, Lawrence C Washington, " Introduction to Cryptography with coding theory", 2nd ed, Pearson, 2007.

2. William Stallings, "Crpyptography and Network security Principles and Practices", Pearson/PHI, 4th ed, 2006.

REFERENCES:

1. W. Mao, "Modern Cryptography – Theory and Practice", Pearson Education, Second Edition, 2007.

2. Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing Third Edition – Prentice Hall of India, 2006