IT9402 **CRYPTOGRAPHY AND SECURITY** **L T P C**
3 0 0 3

AIM:

To introduce the fundamentals of Cryptography and its application to security.

OBJECTIVES:

- To understand the mathematics behind Cryptography
- To understand the standard algorithms used to provide confidentiality provide integrity and authenticity.
- To get a working knowledge of network security, data base security and DS security issues in order to build secure systems.

UNIT I MATHEMATICAL FUNDAMENTALS **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 ENCRYPTION TECHNIQUES **9**

Simple DES – Differential cryptoanalysis – DES – Modes of operation – Triple DES – AES – RC5, RC4 – RSA – Attacks – Primality test – factoring.

UNIT III KEY EXCHANGE AND AUTHENTICATION TECHNIQUES **9**

Discrete Logarithms – Computing discrete logarithms – Diffie-Hellman key exchange – Elliptic curve cryptography Key exchange - ElGamal Public key cryptosystems – Message Authentication codes - Hash functions – Hash algorithms - Secure Hash – Birthday attacks - MD5 – Authentication protocols - Digital signatures – RSA, ElGamal, DSA.

UNIT IV NETWORK SECURITY PRACTICE **9**

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

UNIT V OPERATING SYSTEMS AND DATABASE SECURITY **9**

Trusted Operating systems – security models – designing trusted OS – assurance – Data base security – multi-level databases – multi-level security.

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.
3 PFleeger and Pfleeger, "Security in computing", 3rd ed, PHI/Pearson, 2003.

REFERENCES:

1. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson 2004.