UNIT - 2

SYMMETRIC CIPHERS: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Simplified DES, Data encryption standard (DES), The strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of Operation, Evaluation Criteria for Advanced Encryption Standard, The AES Cipher.

UNIT - 3

Principles of Public-Key Cryptasystems, The RSA algorithm, Key Management, Diffie - Hellman Key Exchange, Elliptic Curve Arithmetic, Authentication functions, Hash Functions.

UNIT - 4

Digital signatures, Authentication Protocols, Digital Signature Standard.

UNIT - 5

Web Security Consideration, Security socket layer (SSL) and Transport layer security, Secure Electronic Transaction.

UNIT - 6

Intruders, Intrusion Detection, Password Management.

UNIT - 7

MALICIOUS SOFTWARE: Viruses and Related Threats, Virus Countermeasures.

UNIT - 8

Firewalls Design Principles, Trusted Systems.

TEXT BOOK:

1. **Cryptography and Network Security**, William Stalling, Pearson Education, 2003.

REFERENCE BOOKS:

1. **Cryptography and Network Security**, Behrouz A. Forouzan, TMH, 2007.
2. **Cryptography and Network Security**, Atul Kahate, TMH, 2003.

OPTICAL NETWORKS

Subject Code : **10EC833** IA Marks : 25