CNS

UNIT 1

1) OSI Security architecture
2) Classical Encryption techniques - substitution techniques, transposition techniques
3) Euclid's algorithm- Fermats and Eulers theorem
4) Chinese remainder theorem. (Theory & problems)
5) Problems based on Playfair cypher & Hill cipher
6) Stenography

UNIT 2

1) Data Encryption Standard (DES) - 3DES
2) Advanced Encryption Standard (AES)
3) RSA algorithm (Theory & problems)
4) Diffie Hellman Key exchange (Theory & problems)
5) Elliptic curve cryptography.

Unit 3

1) MD5
2) SHA
3) HMAC
4) DSA/DSS
5) Brithday Attack
6) Properties of Hash Functions

UNIT 4

1) Kerberos - V4, V5, Inter Relam (Kerberos Realms), Difference between V4 & V5
2) Firewall types and design
3) Firewall configuration
4) Intrusion detection system
5) Antivirus

UNIT 5

1) Pretty Good Privacy
2) S/MIME.
3) architecture of IP Security
4) SSL Architecture / TLS
5) Authentication Header-Encapsulation Security Payload (ESP).