

B. Sc. (IT) Final Semester -V
Paper III
Network Security

Unit I

Introduction, Security Concepts, Threats and Risks, Attacks – Passive and Active, Security Services, Confidentiality, Authentication, Non-Repudiation, Integrity, Access Control, Availability, Model for Internetwork Security, Internet Standards and RFCs Access Control Mechanisms ,Access Matrix, HRU, TAM, ACL and capabilities

Unit II

Access Control Models, Chinese Wall, Clark-Wilson, Bell-LaPadula, Non- Interference and Role Base Model. Cryptography, Secret Key and Public Key Cryptosystems, Symmetric Ciphers, Block Ciphers and Stream Ciphers, DES, IDEA and Key Escrow, RSA and ElGamal.

Unit III

Secure Hash and Key management, Digital Signature and Non-repudiation, cryptanalysis. Network Security, Objectives and Architectures, Internet Security Protocols, IP encapsulating Security Protocol, Network and Transport Layer Security.

Unit IV

Network Security Applications, Authentication Mechanisms: a) Passwords, b) Cryptographic authentication protocol, c) Smart Card, d) Biometrics, e) Digital Signatures and seals, f) Kerberos, g) X.509 LDAP Directory. Web Security : a) SSL Encryption b) TLS, SET, E-mail Security, PGP's / MIME, IP Security, Access and System Security , Intruders, Intrusion Detection and Prevention , Firewall a) Hardware Firewall b) Software Firewall c) Application Firewall d) Packet Filtering. e). Packet Analysis, Proxy Servers, Firewall setting in Proxy, ACL in Proxy.