CS 411: Cryptography And Network Security (3-0-0: 3)

Basic encryption and decryption – Encryption techniques – Secret key cryptography – Data Encryption Standard – Advanced Encryption Standard – Hash and MAC algorithms

Public Key encryptions – Introduction to number theory - RSA algorithm– Diffie-Hellman – Digital Signature standard – Elliptic Curve cryptography - Digital signatures and authentication

Secure sockets – IPsec -Internet Key Exchanging (IKE) – IKE phases – encoding – Internet security – Threats to privacy – Packet sniffing – Spoofing - Security standards–Kerberos.X.509 Authentication Service.

Security protocols – Transport layer protocols – SSL - Firewalls design principles. Intrusion detection – password management – Viruses and related Threats – Virus Counter measures, Virtual Private Networks.

Text Books:

1. Behrouz A. Forouzan, “Cryptography and Network Security”, McGraw-Hill publication.
2. William Stallings , “Cryptography and Network Security: Principles and Standards”, Prentice Hall India.

References:

C. P. Pleeger, “Security in Computing”, Pearson Education Asia.
1. W. Stallings, “Network Security Essentials: Applications and standards”, Person Education Asia.