BC302 INFORMATION SECURITY

Objective of the Course :
This Course focuses towards the introduction of network security using various cryptographic algorithms. Underlying network security applications. It also focuses on the practical applications that have been implemented and are in use to provide e_mail and web security.

UNIT - I Classical Encryption Techniques – Symmetric Cipher Model – Substitution Techniques – Transposition Techniques – Rotor Machines – Steganography

UNIT - II BLOCK CIPHERS AND DATA ENCRYPTION STANDARD Block Cipher Principles – Data Encryption Standard – Strength of DES – Differential and Linear Cryptanalysis - Block Cipher Design Principles.- Advanced Encryption Standard – Evaluation Criteria of AES – AES Cipher – More on Symmetric Ciphers – Multiple encryption and Triple DES – Block Cipher Modes of Operation – RC4.

UNIT - III PUBLIC-KEY ENCRYPTION AND HASH FUNCITONS Principles of Public –Key Cryptosystems – RSA Algorithm – Key Management – Message Authentication and Hash Functions – Authentication Requirements – Authentication Functions – Message Authentication – Hash Functions – Security of Hash Functions and MACs- Digital Signatures - Authentication Protocols – Digital Signature Standard.

UNIT - IV NETWORK SECURITY INTRODUCTION Security Trends – Security attacks – Security services – Security Mechanisms – A Model for Network Security Model APPLICATIONS Kerberos – X.509 Authentication Service – Public Key Infrastructure – Pretty Good Privacy – S/MIME- IP Security Overview – IP Security architecture-Authentication Header – Encapsulating Security Payload – Combining Security associations – Key Management

UNIT - V Web Security- Secure Socket Layer and Transport Layer Security – Secure Electronic Transaction. SYSTEM SECURITY Intruders – Intrusion Detection – Password Management – Malicious Software - Firewalls – Trusted Systems.

TEXT BOOKS : 1. William Stallings, “Cryptography and Network security”, 4th ed., Pearson Education, 2010.
2. William Stallings “Network Security Essentials Applications and Standards”, 2nd ed.,Pearson Education, 2009.
REFERENCE BOOKS : 1. Eric Malwald, “Fundamentals of Network Security “, 4th ed., Pearson Education, 2010.
2. Charlie Kaufman, “Radis Perlman and Mike Speciner ,Network Security – Private Communication in a Public World”, 1st ed., Pearson Education,2009 .
3. Buchmann, Springer ,”Introduction to Cryptography”, 2nd ed., Pearson Education, 2009.