

(CS604) NETWORK SECURITY & CRYPTOGRAPHY

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

Introduction : Security Trends, Security attacks, Security services, Security Mechanisms, A Model for Network Security Model, 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, Multiple encryption and Triple DES, Block Cipher Modes of Operation, RC4. Cast-128, Blowfish Algorithms

UNIT - III

Public - Key Encryption and Hash Functions : 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 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

System Security : Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction, Intruders, Intrusion Detection, Password Management, Malicious Software, Firewalls, Trusted Systems.

TEXT BOOK :

1. William Stallings, "Cryptography and Network security", 4th ed., Pearson Education, 2005.

REFERENCE BOOKS :

1. William Stallings "Network Security Essentials" (Applications and Standards) 2nd ed., Pearson Education, 2007.
2. Eric Malwald "Fundamentals of Network Security" 3rd ed., (Dreamtech press), 2010.