



STANLEY
COLLEGE OF ENGINEERING & TECHNOLOGY FOR WOMEN
(Approved by AICTE , New Delhi | Affiliated to Osmania University ,Hyderabad)
Address : Chapel Road, Abids ,Hyderabad

CS 561

NETWORK SECURITY

UNIT-I

Introduction: Attributes of Security, Integrity, Authenticity, Non-repudiation, Confidentiality, Authorization, Anonymity, Types of Attacks, DoS, IP Spoofing, Replay, Man-in-the-Middle attacks, General Threats to Computer Network, Worms, Viruses, -Trojans

UNIT-II

Secret Key Cryptography : DES, Triple DES, AES, Key distribution, Attacks, Public Key Cryptography: RSA, ECC, Key Exchange (Diffie-Hellman), Java Cryptography Extensions, Attacks

UNIT-III

Integrity, Authentication and Non-Repudiation : Hash Function (MD5, SHA5), Message Authentication Code (MAC), Digital Signature (RSA, DSA Signatures), Biometric Authentication.

UNIT-IV

PKI Interface : Digital Certificates, Certifying Authorities, PGP Key Interface, System Security using Firewalls and VPN's. Smart Cards : Application Security using Smart Cards, Zero Knowledge Protocols and their use in Smart Cards, Attacks on Smart Cards

UNIT-V

Applications: Kerberos, Web Security Protocols (SSL), IPSec, Electronic Payments, E-cash, Secure Electronic Transaction (SET), Micro Payments, Case Studies of Enterprise Security (.NET and J2EE)

Suggested Reading:

1. William Stallings, "Cryptography and Network Security", 4th Edition. Pearson, . 2009.
2. Behrouz A Forouzan, "Cryptography and Network Security" , TMH, 2009
3. Joseph Migga Kizza, "A Guide to Computer Network Security", Springer, 2010
4. Dario Cataiano, "Contemporary Cryptology", Springer, 2010