NETWORK SECURITY AND CRYPTOGRAPHY

COURSE CODE: 15CS1105 **L T P C**
3 0 0 3

Pre-requisites: Computer Networks

COURSE OUTCOMES:
At the end of the course the student shall be able to

CO1: Discuss various classical encryption techniques, block ciphers and data encryption standard.
CO2: Describe the various cryptography systems and key management & distribution schemes.
CO3: Explain hash and MAC algorithms
CO4: Apply various network application security schemes.
CO5: Explain intruder detection mechanisms, types of malicious software, firewall characteristics

UNIT-I (8-10 Lectures)
INTRODUCTION : Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. CLASSICAL **ENCRYPTION TECHNIQUES:** Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography.

BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD: Block Cipher Principles, The Data Encryption Standard (DES), A DES Example, The Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles.
Multiple Encryption and Triple DES, Electronic Codebook Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode. STREAM CIPHERS : Stream Ciphers, RC4.

UNIT-II (8-10 Lectures)
PSEUDORANDOM NUMBER GENERATION: Principles of Pseudorandom Number Generation, Pseudorandom Number Generators. NUMBER THEORY-: Divisibility and the Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms. PUBLIC-KEY CRYPTOGRAPHY, RSA AND OTHER PUBLIC-KEY CRYPTOSYSTEMS: Principles of Public-Key Cryptosystems, The RSA Algorithm, DiffieHellman Key Exchange, ElGamal Cryptosystem.

UNIT-III (8-10 Lectures)
CRYPTOGRAPHIC HASH FUNCTIONS: Applications of Cryptographic Hash Function, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA).

MESSAGE AUTHENTICATION CODES : Message Authentication Requirements, Message Authentication Functions, Message Authentication Codes, Security of MACs, MACs Based on Hash Functions (HMAC).

DIGITAL SIGNATURES- Digital Signatures, ElGamal Digital Signature Scheme, Schnorr Digital Signature Scheme, Digital Signature Standard (DSS).

UNIT-IV (8-10 Lectures)

KEY MANAGEMENT AND DISTRIBUTION: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Public Key Infrastructure.

USER AUTHENTICATION PROTOCOLS: Remote User Authentication Principles, Remote User Authentication Using Symmetric Encryption, Kerberos, Remote User Authentication Using Asymmetric Encryption.

ELECTRONIC MAIL SECURITY: Pretty Good Privacy (PGP), S/MIME.

UNIT-V (8-10 Lectures)

TRANSPORT-LEVEL SECURITY : Web Security Issues; Secure Sockets Layer (SSL), Transport Layer Security (TLS), HTTPS, Secure Shell (SSH). IP SECURITY: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations.

INTRUDERS- Intruders, Intrusion Detection. MALICIOUS SOFTWARE : Types of Malicious Software, Viruses, Worms.

FIREWALLS : The Need for Firewalls, Firewall Characteristics, Types of Firewalls, Firewall Configurations.

TEXT BOOKS:

William Stallings: Cryptography And Network Security- Principles And Practice, 5th Edition, Pearson/PHI, 2011.

REFERENCES:

1. William Stallings, "Network Security Essentials (Applications and Standards)", 4th Edition, Pearson Education. ,2012.
2. Charlie Kaufman, Radia Perlman and Mike Speciner: "Network Security – Private Communication in a Public World", 2nd Edition, Pearson/PHI, 2002.
3. Eric Maiwald: "Fundamentals of Network Security", 1st Edition, Dreamtech Press, 2003.
4. Whitman: "Principles of Information Security", 3rd Edition, Thomson, 2009.
5. Robert Bragg, Mark Rhodes: "Network Security: The complete reference", 1st Edition, TMH, 2004.
6. Buchmann: "Introduction to Cryptography", 2nd Edition, Springer , 2004.

Web Reference : http://nptel.ac.in/courses/106105031/

***