CRYPTOGRAPHY AND NETWORK SECURITY

Course Code: 13CS1107	L	T	P	C
	4	0	0	3

Pre-requisite: Computer Networks.

Course Educational Objectives:

To make the student learn different encryption techniques along with hash functions, MAC, digital signatures and their use in various protocols for network security and system security.

Course Outcomes:

The student who successfully completes this course will be able to:

- Analyze and design classical encryption techniques and block ciphers.
- Understand and analyze data encryption standard.
- Understand and analyze public-key cryptography, RSA and other public-key cryptosystems
- such as Diffie-Hellman Key Exchange, ElGamal Cryptosystem, etc.
- Understand key management and distribution schemes and design User Authentication
- Protocols.
- Analyze and design hash and MAC algorithms, and digital signatures.
- Design network application security schemes, such as PGP, S/MIME, IPSec, SSL, TLS,
- HTTPS, SSH, etc.
- Know about Intruders and Intruder Detection mechanisms, Types of Malicious software,
- Firewall Characteristics, Types of Firewalls, Firewall Location and Configurations.

UNIT-I (12 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.

BLOCK CIPHER OPERATION:

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 (12 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, Diffie-Hellman Key Exchange, ElGamal Cryptosystem.

UNIT-III (12 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 (12 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 (12 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:

1.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 REFERENCES

http://www.nptel.iitm.ac.in/courses/106105031/