22CS401 CRYPTOGRAPHY AND NETWORK SECURITY

Source: https://www.brainkart.com/subject/CRYPTOGRAPHY-AND-NETWORK-SECURITY-PRINCIPLES-AND-PRACTICE_136/

Hours Per Week :

L	T	P	C
2	0	2	3

PREREQUISITE KNOWLEDGE: Computer networks.

COURSE DESCRIPTION AND OBJECTIVES:

This course focuses on the modern concepts of network security using various cryptographic algorithms and underlying network security applications. It enables to understand various symmetric and asymmetric cryptographic techniques. It focuses on providing security services in applications such as e-mail functioning, web security and secure electronic transactions protocol and system security.

MODULE-1

UNIT-1 **8L+0T+8P=16 Hours**

INTRODUCTION

Introduction To Computer and Network Security Concepts: Computer Security Concepts, Need of data security, privacy, and authentication, Security attacks, Security services, Security mechanisms, Fundamental Security Design Principles, Attack Surfaces and Attack trees, A model for network security.

Classical Encryption Techniques: Symmetric cipher model, Substitution techniques, Transposition techniques

UNIT-2 **8L+0T+8P=16 Hours**

PRIVACY PRESERVATION USING CRYPTOGRAPHY

Symmetric Ciphers: Block cipher principles, Data encryption standard, Strength of DES, Blockcipher design principles, AES cipher, Multiple encryption and triple DES, Block cipher modes ofoperation, RC4.

Asymmetric Ciphers and Cryptographic Hash Functions: Principles of public keycryptosystems, RSA algorithm, Diffie-Hellman Key Exchange, Message Authentication requirements,Authentication functions, Message authentication Codes, Hash functions, Security of hash functionsand MACs, Digital signature standard.

PRACTICES:

- Implement Substitution and Transposition Ciphers
  - Ceaser cipher
  - Playfair cipher
  - Hill cipher
  - Rail fence cipher
- Implement Symmetric Cipher
  - S-DES
  - RC4
- Implement Asymmetric Cipher
  - RSA
  - Diffie-Hellman
  - Hash Function

SKILLS:

- ✓ *Design various security services for appropriate applications.*
- ✓ *Identifying the appropriate firewall, password management and anti-virus models for specific applications.*
- ✓ *Test and resolve threats and malfunctions in network.*
- ✓ *Apply different security mechanisms for web applications.*
- ✓ *Build authentication system for security protocols.*

MODULE-2

UNIT-1 **8L+0T+8P=16 Hours**

SECURITY APPLICATIONS

Network Security Applications: Kerberos, X.509 authentication service, Public key infrastructure,

E-Mail Security: Pretty good privacy, S/MIME.

IP Security Overview: IP security architecture, Authentication header, Encapsulating security payload, Combining security associations, key management.

UNIT-2 **8L+0T+8P=16 Hours**

WEB AND SYSTEM SECURITY

Web Security: Secure socket layer and transport layer security, HTTPS, Secure Shell (SSH)

System Security: Intruders, Intrusion detection, Malicious software, Firewalls

PRACTICES:

- Configure IP Address in a system in LAN (TCP/IP Configuration)
- Configure DNS to establish interconnection between systems
- Configuring Windows Firewall
- Adding users, setting permissions
- Configure Mail server
- Demonstrate the usage of Wireshark to identify abnormal activity in network communication.
- Demonstrate usage of NMAP (Zenmap) Tool in Network Scanning.

COURSE OUTCOMES:

Upon successful completion of this course, students will have the ability to:

CO No.	Course Outcomes	Blooms Level	Module No.	Mapping with POs
1	Apply cryptographic techniques in various security service solutions effectively in everyday professional and social contexts.	Apply	1,2	1,2
2	Analyze the usage of secure protocols to safeguard sensitive data using internet.	Analyze	1,2	1,2
3	Usage of tools to Identify abnormal activity in network communication to take appropriate action.	Apply	2	5
4	Apply various security protocols to safe guard the data internet using SSL/TCL.	Apply	2	1,2

TEXT BOOK:

1. William Stallings, “Cryptography and Network security”, 7th Edition, Pearson Education, 2017.

REFERENCE BOOKS:

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