17CS004 CRYPTOGRAPHY AND NETWORK SECURITY

L	T	P	C
3	-	3	5

Course Description and Objective:
This course focuses on offering the knowledge of applying cryptographic algorithms for network security. It also deals with the understanding and controlling of malicious software like viruses and worms. The objective of this course is to enable the student to understand and apply various security algorithms in applications such as e-mail, web and other data transfer mechanisms.

Course Outcomes
The student will be able to:

- ✓ Understand and implement different types of conventional and modern cryptographic algorithms.
- ✓ Apply various encryption techniques for network security.
- ✓ Develop programs involving symmetric and asymmetric ciphers.
- ✓ Familiarize with web security and transport level security protocols.

Skills:

- ✓ Identify and resolve different types of security vulnerabilities.
- ✓ Differentiate classical encryption methods with modern encryption algorithms.
- ✓ Develop secured client/server environment.
- ✓ Apply different security mechanisms for different layers.
- ✓ Compare and evaluate different encryption algorithms.

Activities:

- ✓ Design and implementation of a network.
- ✓ Build secured applications using sockets and TCP/IP.
- ✓ Manage security In small business network applications.
- ✓ Application of S/MIME, PGP in e-mail 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.509Authentication 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.

LIST OF EXPERIMENTS

List of Programs

1. Implement substitution and transposition ciphers.
2. Develop simplified data encryption standard algorithm (S-DES).
3. Write a program to implement RSA algorithm.
4. Demonstrate the usage of wireshark to identify abnormal activity in network communication.
5. Demonstrate usage of NMAP (Zenmap) tool in network scanning.
6. Demo of eavesdropping attack and its prevention using SSH.
7. Configuration and deployment of firewall.

Text Books

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

Reference Books

1. William Stallings, “Network Security Essentials Applications and Standards”, 2nd ed., Pearson Education, 2003.
2. Charlie Kaufman, Radis Perlman and Mike Speciner, “Network Security – Private Communication in a Public World” 2nd ed., Pearson Education, 2003.
3. Cyrus Piekari, Anton Chuvakin, “Security Warrior”, 2nd ed., Oreilly, 2005.
4. Peborab Russell, G.T. Gangeni Sr, “Computer Security Basics”, 2nd ed., Oreilly Publishers, 2006.