16CS403 INFORMATION SECURITY

Hours Per Week :

L	T	P	C
3	-	2	4

Total Hours :

L	T	P
45	-	30

CS	WA/RA	SSH	SA	S	BS
5	5	40	8	5	2

Course Description and Objectives:

This course focuses on offering the knowledge of applying cryptographic algorithms for network security. It also deals with the understanding and controling of malicious software like viruses and warms. 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:

- apply various encryption techniques for network security.
- develop programs involving symmetric and asymmetric ciphers.
- familiarize with web security and transport level security protocols.

SKILLS :

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

UNIT - 1 **L-09**

NETWORK SECURITY INTRODUCTION: Security attacks, Security services, Security Mechanisms, A Model for Network Security; Model Classical Encryption Techniques - Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Rotor Machines and Steganography.

UNIT - 2 **L-09**

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; More on Symmetric Ciphers- Multiple encryption and Triple DES, Block Cipher Modes of Operation and RC4.

UNIT - 3 **L-09**

PUBLIC-KEY ENCRYPTION AND HASH FUNCITONS: 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 and Digital Signature Standard.

UNIT - 4 **L-09**

NETWORK SECURITY APPLICATIONS: Kerberos, X.509 Authentication Service, Public Key Infrastructure, Pretty Good Privacy, S/MIME, IP Security Overview, IP Security architecture, Authentication Header, Encapsulating Security Payload, Combining Security associations and Key Management.

UNIT - 5 **L-09**

WEB SECURITY: Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction.

SYSTEM SECURITY: Intruders, Intrusion Detection, Password Management, Malicious Software, Firewalls and Trusted Systems.

LABORATORY EXPERIMENTS

Course Outcomes:

The student will be able to:

- understand and Implement different types of conventional and modern cryptographic algorithms.
- implement and maintain common firewall types and architectures.
- gain knowledge and use different types of tools like Wire Shark and NMAP.

LIST OF EXPERIMENTS:

Total Hours: 30

1. Implement Ceaser, Playfair and Rail Fence Ciphers.
2. Develop Simplified Data Encryption Standard algorithm (S-DES).
3. Write a program to implement RSA algorithm.

ACTIVITIES:

- *Design and implementation of a secured client/server model.*
- *Build secured applications using sockets and TCP/IP.*
- *Manage security In small business network applications.*
- *Identify application of S/MIME in Mobile communication.*

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. William Stallings, "Cryptography and Network security", 4th edition, Pearson Education, 2010.
2. William Stallings, "Network Security Essentials Applications and Standards", 2nd edition, Pearson Education, 2009.

REFERENCE BOOKS :

1. Eric Malwald, "Fundamentals of Network Security", 4th edition, Pearson education, 2010.
2. Charlie Kaufman, "Radis Perlman and Mike Speciner, Network Security – Private Communication in a Public World", 1st edition, Pearson Education, 2009 .
3. Buchmann, "Introduction to Cryptography", 2nd edition, Pearson Education,Springer, 2009.