SREENIVASA INSTITUTE of TECHNOLOGY and MANAGEMENT STUDIES

II MCA - II Semester

L	P	C
4	0	4

16MCA225B INFORMATION SECURITY

Course Objectives

- Understand Security threats, vulnerabilities and attacks and enlist them for any networked application.
- Apply detective and preventive counter measures in different scenarios after evaluating Symmetric and asymmetric encryption methods to achieve confidentiality.
- Analyze the use of Authentication applications, Web, IP and Email security
- Evaluate the need of Intrusion Detection and Firewalls

Syllabus:

UNIT I : Introduction and Symmetric Encryption

Security Trends, the OSI Security Architecture, Security Attacks, Security Services Security Mechanisms, A Model for Network Security, Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography.

UNIT II : Symmetric Ciphers

Block Cipher principles, the Data Encryption Standard, the strength of DES, Differential and Linear Cryptanalysis, Block cipher Design principles.

Finite Fields: Groups, Rings and Fields- Modular Arithmetic - the Euclidean Algorithm- Finite Fields of the Form GF(p)

Advanced Encryption Standard: Evaluation Criteria for AES- the AES cipher, More on Symmetric Ciphers- triple DES, Block cipher modes of operation, Stream Ciphers.

UNIT III : Public Key Encryption and Hash Functions

Prime Numbers, Principles of Public-key Cryptosystems, RSA, Key Management, Diffie-Hellman Key Exchange, Authentication Requirements, Functions, Message authentication codes, Hash Functions, Secure hash algorithm, HMAC, Digital signatures, Authentication Protocols.

Authentication Applications: Kerberos, X.509Authentication Service.

UNIT IV: Electronic Mail Security and IP Security

Pretty Good Privacy, S/MIME, IP Security Overview, IP Security Architecture, Authentication header, Encapsulating Security Payload, Combining Security Associations, Key Management.

UNIT V : Web Security and Intruders, Firewalls

Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS),
Intruders, Intrusion Detection, Password Management, the Need for Firewalls, Firewall Characteristics, Types of Firewalls, Firewall Basing, Firewall Location and Configurations

Course Outcome:

- Understand and appreciate the importance of Network security in Today`s world and apply security services and mechanisms in evaluating networked systems and also while creating new applications.
- Analyze and apply best suited Network Security mechanisms and standards in various applications.

TEXT BOOKS:

1. Cryptography and Network Security, 4/e, 2006, William Stallings, Pearson Education, New Delhi.
2. William Stallings, "Network Security Essentials: Applications and Standards", 4th Edition,
3. Pearson Education.

REFERENCE BOOKS:

1. Principles and Practices of Information Security, 4/e, 2012, Michal E. Whitman and Herbert J. Mattord, Cengage Learning, New Delhi.
2. Fundamentals of Network Security, 1/e, 2008, Eric Maiwald (Dreamtech press),New Delhi.
3. Network Security - Private Communication in a Public World, 2/e, 2002, Charlie Kaufman, Radia Perlman and Mike Speciner, Pearson/PHI.New Delhi.