Name of Department: - Computer Science and Engineering

1. Subject Code: TCS 619 Course Title: **Network and System Security**
2. Contact Hours: 3 - 2
3. Semester: **VI**
4. Prerequisite: TCS591
5. Course Outcomes: After completion of the course students will be able to

    1. Understand the basics of computer security
    2. Elaborate the cryptographic techniques.
    3. Discuss the transport layer security
    4. Find the pros and cons of various key distribution methods
    5. Analyze the wireless Network security
    6. Find the level of system security

6. Details of the Course: -

UNIT	CONTENTS	Contact Hrs
Unit – I	I**ntroduction** Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Models for network security, standards.	**9**
Unit - II	**Cryptography** **Symmetric Encryption and Message Confidentiality** Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Random and Pseudorandom Numbers, Stream Ciphers and RC4, Cipher Block Modes of Operation. **Public-Key Cryptography and Message Authentication 61** Approaches to Message Authentication, Secure Hash Functions, Message Authentication Codes, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures	**9**
Unit – III	**Network security Application – I** **Key Distribution and User Authentication** Symmetric Key Distribution Using Symmetric Encryption, Kerberos, Key Distribution Using Asymmetric Encryption, X.509 Certificates, Public-Key Infrastructure, Federated Identity Management **Transport-Level Security** Web Security Considerations, Secure Socket Layer and Transport Layer Security, Transport Layer Security, HTTPS, Secure Shell (SSH)	**10**
Unit – IV	**Network security Application - II** **Wireless Network Security**	**8**

	IEEE 802.11 Wireless LAN Overview, IEEE 802.11i Wireless LAN Security, Wireless Application Protocol Overview, Wireless Transport Layer Security, WAP End-to-End Security **Electronic Mail Security** Pretty Good Privacy, S/MIME, DomainKeys Identified Mail, **IP Security** IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange, Cryptographic Suites	
Unit – V	**System Security** **Intruders** Intruders, Intrusion Detection, Password Management, **Malicious Software** Types of Malicious Software, Viruses, Virus Countermeasures, Worms, Distributed Denial of Service Attacks. **Firewalls** The Need for Firewalls, Firewall Characteristics, Types of Firewalls, Firewall Basing, Firewall Location and Configurations, **Legal and Ethical Aspects** Cybercrime and Computer Crime, Intellectual Property, Privacy, Ethical Issues	**10**
	Total	**46**

Text/ Reference Books:

1. W. Stallings," Network Security Essentials". Prentice Hall, 2003.
2. Ch. P. Pfleeger, S. L. Pfleeger „*Security in Computing", 4th Edition* Prentice Hall, 2006