Name of Department:- Computer Science and Engineering

1. Subject Code: TIT 704 Course Title: **Cryptography and Network Security**
2. Contact Hours: L: 3 T: - P: -
3. Semester: VII

4. Pre-requisite: TCS 604 Computer Networks - I

5. Course Outcomes: After completion of the course students will be able to

i. Classify security vulnerabilities involved in data communication over Internet and make use of classical algorithms to address the vulnerabilities.
ii. Make use of modern block ciphers to secure data transmission and storage
iii. Analyze challenges involved in key distribution and select approache that can be adopted
iv. Analyze strengths of public key algorithms and explore applications in exchange, authentication and hashing of messages.
v. Appreciate application of algorithms for ensuring access control, authentication, secured transmission of data at different layers.
vi. Appraiserisks related to wireless, web, cloud security and measures to be adopted to secure organizational network.

6. Detailed Syllabus

UNIT	CONTENTS	Contact Hrs
Unit - I	Introduction to security attacks, services and mechanism, introduction to cryptography. Conventional Encryption: Conventional encryption model, classical encryption techniques- substitution ciphers and transposition ciphers, cryptanalysis, stenography, stream and block ciphers.	**8**
Unit - II	Modern Block Ciphers: Block ciphers principals, Shannon's theory of confusion and diffusion, Modes of operations of block ciphers: ECB, CBC, OFB, CFB, Advanced Encryption Standard (AES) Traffic confidentiality, Key distribution, random numbers, Pseudo random number generation using Linear Congruential and Blum BlumShub algorithms	**10**
Unit – III	Prime and relative prime numbers, modular arithmetic, Primality testing, Euclid's Algorithm for GCD and Extended Euclid's Algorithm for Multiplicative inverse Principals of public key crypto systems, RSA algorithm, security of RSA, key management, Diffle-Hellman key exchange algorithm Message Authentication: Requirements, Message Authentication Functions Cryptographic Hash Functions:Applications of Cryptographic Hash Functions, Secure Hash Algorithm (SHA)-512	**8**
Unit – IV	Authentication Applications: Kerberos and X.509 directory authentication service, electronic mail security-S /MIME IP Security: Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management.	**9**
Unit – V	Wireless Network Security: Wireless Network Threats, Wireless Security Measures, Mobile Device Security, Security Threats and Security Strategy, IEEE 802.11 Wireless LAN Overview, The Wi-Fi Alliance, IEEE 802 Protocol Architecture, IEEE 802.11 Network Components and Architectural Model, IEEE 802.11 Services.Concept of Wireless LAN security and brief of phases of operation Web and Cloud Security: Web Security Considerations, Transport Layer Security, HTTPS,Cloud Security risks and Countermeasures; Data protection in cloud. System Security: The Need for Firewalls, Firewall Characteristics, Types of Firewalls	**10**
	Total	**45**

Text Books:

1. William Stallings, "Cryptography and Network Security: Principals and Practice", 7th Edition, Pearson, 2017
2. William Stallings, "Network Security Essentials – Applications and Standards", 4th edition, Pearson Education, 2011

Reference Books

1. Behrouz A Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security"Mc-GrawHill, 3rd Edition, 2015
2. Johannes A. Buchmann, "Introduction to Cryptography", Springer-Verlag, 2012