Course Code: BTCS 701-18	Course Title : Network Security and Cryptography	3L:0T:0P	3Credits

Detailed Contents:

UNIT 1: Introduction (3 Hours)
Introduction to Cryptography, Security Threats, Vulnerability, Active and Passive attacks, Security services and mechanism, Conventional Encryption Model, CIA model.

[5hrs] (CO 1)

UNIT 2: Math Background
Modular Arithmetic, Euclidean and Extended Euclidean algorithm, Prime numbers, Fermat and Euler's Theorem

[5hrs] (CO 1)

UNIT 3: Cryptography
Dimensions of Cryptography, Classical Cryptographic Techniques Block Ciphers (DES, AES) : Feistal Cipher Structure, Simplifies DES, DES, Double and Triple DES, Block Cipher design Principles, AES, Modes of Operations Public-Key Cryptography : Principles Of Public-Key Cryptography, RSA Algorithm, Key Management, Diffie-Hellman Key Exchange, Elgamal Algorithm, Elliptic Curve Cryptography

[12hrs] (CO 2)

UNIT 4 Hash and MAC Algorithms
Authentication Requirement, Functions, Message Authentication Code, Hash Functions, Security of Hash Functions and Macs, MD5 Message Digest Algorithm, Secure Hash Algorithm, Digital Signatures, Key Management: Key Distribution Techniques, Kerberos

[6hrs] (CO 3)

UNIT 5 Security in Networks
Threats in networks, Network Security Controls – Architecture, Encryption, Content Integrity, Strong Authentication, Access Controls, Wireless Security, Honeypots, Traffic flow security, Firewalls – Design and Types of Firewalls, Personal Firewalls, IDS, Email Security – PGP, S/MIME

[7hrs] (CO 4)

Course Outcomes:
After undergoing this course, the students will be able to:
CO1: Understand the fundamental principles of access control models and techniques, authentication and secure system design
CO2: Have a strong understanding of different cryptographic protocols and techniques and be able to use them.
CO3: Apply methods for authentication, access control, intrusion detection and prevention.
CO4: Identify and mitigate software security vulnerabilities in existing systems.

Suggested Readings/ Books:
1. Cryptography And Network Security Principles And Practice Fourth Edition, William Stallings, Pearson Education
2. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall PTR
3. Network Security Essentials: Applications and Standards, by William Stallings. Prentice Hall
4. Cryptography: Theory and Practice by Douglas R. Stinson, CRC press.
