EC4142PE: NETWORK SECURITY AND CRYPTOGRAPHY (PE – IV)

	L	T	P	C
B. Tech. VI Year I Sem.	**L**	**T**	**P**	**C**
Prerequisite: Nil	**3**	**0**	**0**	**3**

Course Objectives:

1. Understand the basic concept of Cryptography and Network Security, their mathematical models
2. To understand the necessity of network security, threats/vulnerabilities to networks and countermeasures
3. To understand Authentication functions with Message Authentication Codes and Hash Functions.
4. To provide familiarity in Intrusion detection and Firewall Design Principles

Course Outcomes: Upon completing this course, the student will be able to

1. Describe network security fundamental concepts and principles
2. Encrypt and decrypt messages using block ciphers and network security technology and protocols
3. Analyze key agreement algorithms to identify their weaknesses
4. Identify and assess different types of threats, malware, spyware, viruses, vulnerabilities

UNIT- I

Security Services, Mechanisms and Attacks, A Model for Internetwork security, Classical Techniques: Conventional Encryption model, Steganography, Classical Encryption Techniques.

Modern Techniques: Simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Block Cipher Design Principles.

UNIT- II

Encryption: Triple DES, International Data Encryption algorithm, Blowfish, RC5, Characteristics of Advanced Symmetric block Ciphers. Placement of Encryption function, Traffic confidentiality, Key distribution, Random Number Generation.

UNIT – III

Public Key Cryptography: Principles, RSA Algorithm, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptograpy.

Number Theory: Prime and Relatively prime numbers, Modular arithmetic, Fermat’s and Euler’s theorems, Testing for primality, Euclid’s Algorithm, the Chinese remainder theorem, Discrete logarithms.

UNIT- IV

Message Authentication and Hash Functions: Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash functions and MACs.

Hash and Mac Algorithms: MD-5, Message digest Algorithm, Secure Hash Algorithm.

Digital signatures and Authentication protocols: Digital signatures, Authentication Protocols, Digital signature standards.

Authentication Applications: Kerberos, Electronic Mail Security: Pretty Good Privacy, SIME/MIME.

UNIT – V

IP Security: Overview, Architecture, Authentication, Encapsulating Security Payload, Key Management. Web Security: Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction.

Intruders, Viruses and Worms: Intruders, Viruses and Related threats.

Fire Walls: Fire wall Design Principles, Trusted systems.

TEXT BOOKS:

1. Cryptography and Network Security: Principles and Practice - William Stallings, Pearson Education.
2. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH,2004.

REFERENCE BOOKS:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Fundamentals of Network Security by Eric Maiwald (Dreamtech press)
3. Principles of Information Security, Whitman, Thomson.
4. Introduction to Cryptography, Buchmann, Springer.