L	T	P	C
3	-	-	3

21BC106 FUNDAMENTALS OF NETWORK SECURITY

Course Description and Objectives:
This Course focuses towards the introduction of network security using various cryptographic algorithms and understanding network security applications. It also focuses on the practical applications that have been implemented and are in use to provide email and web security.

Course Outcomes:

The student will be able to,

- Understand the fundamentals of networks security, security architecture, threats and
- vulnerabilities
- Apply the different cryptographic operations of symmetric cryptographic algorithms
- Apply the different cryptographic operations of public key cryptography
- Apply the various Authentication schemes to simulate different applications.
- Understand various Security practices and System security standards

Skills:

- Understanding of: Classical encryption techniques.
- Analyze Block ciphers and the Data Encryption Standard, Basics of finite fields.
- Apply Message authentication, Hash functions and algorithms, Digital signatures and authentication protocols.

Activities:

- Will develop their skills in: the programming of symmetric and/or asymmetric ciphers and their use in the networks.
- Will learn protocols used in Web Security and Transport Layer Security

Syllabus

UNIT - I **12 Hours**

INTRODUCTION: Security trends, Model of network security – Security attacks, services and mechanisms – OSI security architecture

UNIT - II **12 Hours**

CLASSICAL ENCRYPTION TECHNIQUES: Substitution techniques, Transposition techniques, Steganography- Foundations of modern cryptography

UNIT - III **12 Hours**

SYMMETRIC KEY CRYPTOGRAPHY: SDES – Block cipher Principles of DES – Strength of DES- Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Advanced Encryption Standard.

UNIT - IV **12 Hours**

PUBLIC KEY CRYPTOGRAPHY: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange. MESSAGE AUTHENTICATION AND INTEGRITY:

Authentication requirement Authentication function – MAC – Hash function – Security of hash function and MAC – SHA –Digital signature.

UNIT - V **12 Hours**

SECURITY PRACTICE AND SYSTEM SECURITY: Electronic Mail security – PGP, IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses –Firewalls.

TEXTBOOK:

William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

REFERENCES BOOKS:

1. C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security, Wile India Pvt.Ltd
2. BehrouzA.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.
3. Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: PRIVATE Communication in a PUBLIC World, Prentice Hall, ISBN 0-13-046019-2