CRYPTOGRAPHY AND NETWORK SECURITY

PC 604 CS

Instruction: 3L+1T periods per week *Duration of SEE: 3 hours*
CIE:30 marks *SEE: 70marks*
Credits: 3

Course Objectives:-

- Understand security concepts, Ethics in Network Security.
- Obtain knowledge on mechanisms to encounter threats
- Appreciate and apply relevant cryptographic techniques
- Apply authentication services and security mechanisms
- Comprehend computer network access control and ethics in network security.

Course Outcomes: At the end of the course the students will be able to -

- Develop familiarity with cryptography and security techniques
- Master fundamentals of secret and public cryptography
- Utilize the master protocols for security services
- Identify network security threats and counter-measures
- Propose network security designs using available secure solutions

UNIT- I

Basic Principles: Security Goals, Cryptographic Attacks, Services and Mechanisms, Mathematics of Cryptography

UNIT –II

Symmetric Encryption: Mathematics of Symmetric Key Cryptography, Introduction to Modern Symmetric Key Ciphers,Data Encryption Standard, Advanced Encryption Standard.

UNIT- III

Asymmetric Encryption: Mathematics of Asymmetric Key Cryptography, Asymmetric Key Cryptography

UNIT –IV

Data Integrity, Digital Signature Schemes & Key Management: Message Integrity and Message Authentication, Cryptographic Hash Functions, DigitalSignature, Key Management

UNIT-V

Network Security: Security at Application layer (PGP and S/MIME), Security at the Transport Layer(SSL and TLS), Security at the Network Layer(IPSec, System Security)

Text Book

1. Cryptography and Network Security, Behrouz A Forouzan, Debdeep Mukhopadhyay, (3e) Mc Graw Hill.

Reference Books

1. Cryptography and Network Security, William Stallings, (6e) Pearson.
2. Everyday Cryptography, Keith M.Martin, Oxford.
3. Network Security and Cryptography, Bernard Meneges, Cengage Learning
4. Cryptography and Network Security – by Atul Kahate – TMH.
5. Cyber Security Operations Handbook – by J.W. Rittiaghouse and William M.Hancok – Elseviers.
6. Khairol Amali Bin Ahmad , Khaleel Ahmad , Uma N. Dulhare ,Functional Encryption ,EAI/Springer Innovations in Communication and Computing,1st ed. 2021 Edition