SCSA1602	NETWORK SECURITY	L	T	P	Credits	Total Marks
		3	*	0	3	100

COURSE OBJECTIVES

- To understand the fundamentals of Cryptography.
- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
- To explore the various key distribution and management schemes.
- To understand how to deploy encryption techniques to secure data in transit across data networks.
- To learn various mechanisms for network security to protect against the threats in the networks.

UNIT 1 INTRODUCTION 9 Hrs.

Services, Mechanisms and attacks - The OSI Security Architecture- A Model for Network Security – Classical Encryption Technique – Symmetric Cipher Model – Substitution Technique – Rotor Machines – Steganography.

UNIT 2 BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD (DES) 9 Hrs.

Simplified DES- Block Cipher principles – The Data Encryption Standard – The strength of DES – Confidentiality using symmetric encryption – Placement of encryption - Traffic confidentiality – Key distribution - Random number generation.

UNIT 3 PUBLIC KEY ENCRYPTION AND KEY MANAGEMENT 9 Hrs.

Introduction to number theory – Public key cryptography and RSA – Key Management Diffie-hellman Key exchange.

UNIT 4 AUTHENTICATION AND HASH FUNCTIONS 9 Hrs.

Authentication requirements – Authentication functions – message authentication codes – Hash functions – Security of hash functions and MAC'S – MD 5 (Message Digest Algorithm) – HMAC.

Digital Signatures and authentication protocols:

Digital Signatures – Authentication protocols – Digital Signature Standard – Kerbews – X.509 Authentication Service.

UNIT 5 NETWORK SECURITY AND SYSTEM SECURITY 9 Hrs.

Electronic Mail Security – IP Security – Web Security – Intruders – Malicious S/Ws – Firewalls.

Max.45 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 - Implement various symmetric encryption techniques for given applications.
CO2 - Illustrate various public key encryption techniques.
CO3 - Understand various key encryption mechanisms and key management strategies that can be applied for real time transactions.
CO4 - Evaluate authentication and hash algorithms.
CO5 - Summarize the basic network security mechanisms.
CO6 - Basic concepts of system level security.

TEXT / REFERENCE BOOKS

1. William Stallings, "Cryptography and Network Security", 6th edition, Pearson Education, 2013.
2. Behrouz A. Forouzan "cryptography and network security", ACM Digital Library, 2007
3. Man Young Rhee,"Internet security: cryptographic principles", "Algorithms and Protocols" Whey publications, 2003
4. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India, 2002.
5. Joey Holland, "Cryptography: Principles and Practice" Larsen and Keller, 2017.
6. Sahadeo Padhye, Rajeev A. Sahu, Vishal Saraswat, "Introduction of Cryptography", CRC press, 2018.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks : 100 **Exam Duration : 3 Hrs.**

PART A : 10 Questions of 2 marks each-No choice **20 Marks**
PART B : 2 Questions from each unit with internal choice, each carrying 16 marks **80 Marks**