SCSA1208	FUNDAMENTALS OF CYBERSECURITY	L	T	P	Credits	Total Marks
		3	0	0	3	100

COURSE OBJECTIVES

- To introduce the basic concepts of cyber security
- To acquire knowledge on cyber threats and attacks
- To become aware of significant security technologies and tools
- To impart knowledge on cipher methods and cryptographic algorithms
- To explore various protocols for establishing secured communication

UNIT 1 INTRODUCTION TO CYBERSECURITY 9 Hrs.

Introduction – Need for Security – Security Approaches – Principles of Security – Components – Balancing Security & Access – Software Development Life Cycle – Security Systems Development Life Cycle – Security Professionals and the organization

UNIT 2 CYBERSECURITY – THREATS & ATTACKS 9 Hrs.

Threats: Intellectual Property - Software Attacks – Deviations in QoS – Espionage – Forces of Nature – Human Error – Information Extortion – Missing, inadequate or incomplete organization policy – Missing, inadequate or incomplete controls – sabotage – Theft – Hardware Failures – Software Failures
Attacks: Malicious Code – Hoaxes – Back Doors – Password Crack – Brute Force – Dictionary – DoS and DDoS – Spoofing – Man-in-the-Middle – Spam – Email Bombing – Sniffers – Social Engineering – Pharming – Timing Attack

UNIT 3 SECURITY TOOLS & TECHNOLOGIES 9 Hrs.

Firewall and VPNs – Intrusion Detection and Prevention Systems – Other Security Tools - Access Control – Firewalls – Protecting Remote Connections – Intrusion Detection and Prevention Systems – Honeypots, Honeynets and Padded Cell Systems

UNIT 4 CYRPTOGRAPHY 9 Hrs.

Cryptology Terminology - Cipher methods – Cryptographic Algorithms – Cryptographic tools –Attacks on cryptosystems - Physical Security.

UNIT 5 PROTOCOLS FOR SECURE COMMUNICATION 9 Hrs.

Basic Concepts – SHTTP, SSL & SET – S/MIME, PEM & PGP – WEP, WPA & WPA2 – IPSEC & PGP

Max. 45 Hrs.

COURSE OUTCOME

On the completion of the course, the students will be able to
C01: Understand the basic concepts, need, approaches, principles and components of security.
CO2: Explain the various cyber threats and attacks.
CO3: Describe the various Security Technologies and Tools.
CO4: Explain the basic principles of cryptography and algorithms.
CO5: Examine the various protocols for secure communication.
CO6: Explore the significant aspects of cybersecurity.

TEXT / REFERENCE BOOKS

1. Michael E. Whitman, Herbert J. Mattord," Principles of Information Security", CENGAGE Learning, 4th Edition.
2. William Stallings," Cryptography and Network Security – Principles and Practice", Pearson Education, 7th Edition.
3. Atul Kahate," Cryptography and Network Security", Mc Graw Hill, 4th Edition.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 Exam Duration: 3 Hrs.
PART A: 10 Questions carrying 2 marks each – No choice 20 Marks
PART B: 2 Questions from each unit of internal choice, each carrying 16 marks 80 Marks