Course code	Course name	L-T-P-Credits	Year of Introduction
AE465	INFORMATION SECURITY	3-0-0-3	2016

Prerequisite : Nil

Course Objective

- To understand the threat models and the basic types of authentication mechanisms
- To analyse cryptographic techniques, protocols, formats, and standards.
- To analyse different log files and understand Cyber laws to recover and secure the data.

Syllabus

Introduction to security and services-Cryptography- Securing the systems-Network security topics-Network perimeter security-Computer forensics and Cyber laws

Expected outcome

At the end of the semester students will be able

i. to apply cryptographic algorithms to avoid data accessing by unauthorized users
ii. to implement security algorithms as per the need of organization.

Text Books

1. Bruce Schneier, "*Applied Cryptography"*, Second Edition, John Wiley & Sons, 1996
2. Charlie Kaufman, Radia Perlman, and Mike Speciner, "*Network Security*: Private Communication in a Public World", 2nd Edition, Prentice Hall, 2002.
3. Rick Lehtinen, G. T. Gangemi, SR.,"*Computer Security Basics"*, Second Edition, O'Reilly Pubs, June 2006.

Reference Books:

1. Marije, "*Computer Forensics and Cyber Crime"*: An Introduction, Prentice Hall, 2004.
2. Stephen Northcutt, Karen Kent, and Lenny Zeltser, "*Inside Network Perimeter Security",* Sams Publications, 200
3. William Stallings, "*Cryptography and Network Security"*, Fourth Edition, Prentice Hall, 2005

Course Plan

Module	Contents	Hours	Semester Exam Marks
I	Introduction to security and services, vulnerabilities and countermeasures, malicious code, goals of security-prevention, detection, and recovery.	6	15%
II	Cryptography-Types of encryption, confidentiality using symmetric encryption, PKI, RSA, Key management, Diffie- Hellman, ECC, CA, etc., authentication protocols.	6	15%
	FIRST INTERNAL EXAMINATION		
III	Securing the systems-Network security protocols: SSL, IPSEC, Kerberoes, X.509 Authentication service, Electronic mail security S/MME, Application security- SSL, PGP, SET.	7	15%

IV	Network security topics: Network layer security – IPSec – overview, IP and IPv6, IPSec Protocols: AH and ESP, Tunnel Mode and transport mode. Internet Key exchange Protocol- IPSec cookies.	7	15%
SECOND INTERNAL EXAMINATION			
V	Network perimeter security-Secured router configuration, firewall, design principles, trusted systems, VPN, IDS, IPS penetration testing, NAT.	8	20%
VI	Computer forensics and Cyber laws- data recovery, security policies and procedures, Security lifestyle management, security audit, managed security services.	8	20%
END SEMESTER EXAMINATION			

QUESTION PAPER PATTERN:

Maximum Marks:100 Exam Duration: 3 Hours

Part A

Answer any two out of three questions uniformly covering Modules 1 and 2 together. Each question carries 15 marks and may have not more than four sub divisions.

(15 x 2 = 30 marks)

Part B

Answer any two out of three questions uniformly covering Modules 3 and 4 together. Each question carries 15 marks and may have not more than four sub divisions.

(15 x 2 = 30 marks)

Part C

Answer any two out of three questions uniformly covering Modules 5 and 6 together. Each question carries 15 marks and may have not more than four sub divisions.

(20 x 2 = 40 marks)