SREE VIDYANIKETHAN ENGINEERING COLLEGE(AUTONOMOUS)

Sree Sainath Nagar, A. Rangampet-517 102

Computer Science & Engineering

Lesson Plan cum Diary 2015-'16

Name of the Subject : Information Security (14MT20507)
Class & Semester : M. Tech. (CN&IS) I-Semester
Name of the faculty Member : Mr. K.Munivara Prasad

S. No.	Topic	No. of periods required	Date(s) covered	No. of periods used	Book(s) followed	Topics for self study
Unit-I: INTRODUCTION TO CRYPTOGRAPHY						
1	Security attacks, Security services	2			T1	Substitution and Transposition techniques, Stream Ciphers, Padding, Cryptanalysis
2	Security Mechanisms, A Model for Network Security Model	1			T1	
3	Symmetric Block Encryption Algorithms - DES	1			T1	
4	DES S-Box	1				
5	Triple-DES	1			T1	
6	AES – Round function, Key expansion	1			T1	
7	AES – Key Expansion	1				
8	Cipher Block Modes of Operation - ECB	1			T1	
9	CBC, CFB	2			T1	
Total no of periods required:		11	Total no of periods used:			
Unit-II: PUBLIC-KEY ENCRYPTION						
10	Approaches to Message Authentication	1			T1	Requirements for Public-Key Cryptography, The Security of RSA, Man-in-the-Middle Attack
11	Secure Hash Functions - Hash Function Requirements	1			T1	
12	Simple Hash Functions	1			T1	
13	SHA-1 & SHA-512	2			T1	
14	Message Authentication Codes - HMAC	1			T1	
15	Public-Key Cryptography principles	1			T1	
16	RSA Public-Key Encryption Algorithm	1			T1	
17	Diffie-Hellman Key Exchange	1			T1	
18	Digital Signatures - DSS	2			T1	
Total no of periods required:		11	Total no of periods used:			

Unit-III: NETWORK SECURITY APPLICATIONS						
19	Kerberos	2			T1	Public-Key Infrastructure Working Group - IETF, VeriSign, E-Mail Threats, Public-key management
20	Public-Key Certificates	1			T1	
21	Public-Key Distribution	1			T1	
22	X.509 Certificates	2			T1	
23	Public-Key Infrastructure	1			T1	
24	Pretty Good Privacy Operations, Key rings	2			T1	
25	Multipurpose Internet Mail Extensions	1			T1	
26	S/MIME - Functionality, S/MIME Messages	1			T1	
27	S/MIME Certificate Processing, Enhanced Security Services	1			T1	
Total no of periods required:		12	Total no of periods used:			
Unit-IV: INTERNET SECURITY						
28	Secure Socket Layer - Architecture	1			T1	Web Security Threats, Open SSL, Secure Shell, HTTPS
29	SSL - Record Protocol, Handshake Protocol	1			T1	
30	Transport Layer Security – MAC, Pseudorandom Function	1			T1	
31	TLS – Cipher suites	1				
32	TLS - Cipher Suites, Client Certificate Types	1			T1	
33	IP Security: Overview	1			T1	
34	IP Security Policy - Association, Database	1			T1	
35	Encapsulating Security Payload, IKE	1			T1	
36	Network management security: Concepts of SNMP	2			T1	
37	SNMPv1 & SNMPv3	1			T1	
Total no of periods required:		12	Total no of periods used:			
Unit-V: SYSTEM SECURITY						
38	Intruders	1			T1	Password management, Honeypots, IP Spoofing
39	Intrusion Detection	2			T1	
40	Distributed Intrusion Detection	1			T1	
41	Malicious Software - Types, Viruses	1			T1	
42	Virus Countermeasures	1			T1	
43	Worms & DDoS	2			T1	
44	Firewalls – Firewall Characteristics	1			T1	

45	Types of Firewalls, Firewall Basing	2			T1	
46	Firewall Location and Configurations	1			T1	
Total no of periods required:		12	Total no of periods used:			
Grand total of periods required:		**59**	**Grand total of periods used:**			

Note: Difference between N and M should be within 5%.

Text Books:

T1: Donald Hearn and M.Pauline Baker, *Computer Graphics C Version*, 2 ed, Pearson Education, 2003.

T2: Prabat K Andleigh and Kiran Thakrar, *Multimedia Systems and Design*, 3rd Indian Reprint Edition, PHI Learning.

Reference Books:

R1: Steven Harrington, *Computer Graphics*, 2 ed, TMH

R2: Judith Jeffcoate, *Multimedia in practice technology and Applications*, PHI, 1998.

Signature of the faculty Member **Signature of the HOD**