Bhoj Reddy Engineering College for Women: Hyderabad
Department of Information Technology
Lesson plan of faculty member for the academic year 2016–17

Class: IV B Tech   Branch-Section: IT-B   Semester: I
Subject: Information Security   Lectures per week: 4+1 (Tutorial)

Lecture Number	Topics to be covered	Date (s)
UNIT – I: Attaks on Computers and Computer Security, Cryptography		
1	The need for security	13 June 2016
2	Security Attacks, Security Services	14 June 2016
3	Principles of security	17 June 2016
4	Security mechanisms	18 June 2016
5	Tutorial (G3,G1,G2) - Security Approaches	15, 16, 17 June 2016
6	A model for Internetwork security	20 June 2016
7	Cryptography introduction	21 June 2016
8	Substitution techniques	24 June 2016
9	Transposition techniques	25 June 2016
10	Tutorial (G3,G1,G2) - Techniques	22, 23,24 June 2016
11	Encryption and decryption	27 June 2016
12	Symmetric and Asymmetric key cryptography	28 June 2016
13	Stegnography	1 July 2016
14	Key range and key size , Types of Attacks	2 July 2016
15	Tutorial (G3,G1,G2) - Cryptography	29, 30 June,1 July 2016
UNIT-II: Symmetric Key Ciphers		
16	Symmetric key cipher	4 July 2016
17	Block cipher principles	5 July 2016
18	Algorithms(DES)	8 July 2016
19	AES	9 July 2016
20	Tutorial (G2) - DES	8 July 2016
21	Blowfish	11 July 2016
22	Differential and linear cryptanalysis	12 July 2016
23	Block cipher modes of operation	15 July 2016
24	RC4	16 July 2016
25	Tutorial (G3,G1,G2) - AES	13, 14, 15 July 2016
26	Location and placement of encryption function	18 July 2016
27	Key distribution Asymmetric key ciphers	19 July 2016
28	Algorithms(RSA)	22 July 2016
29	Diffie-Hellman	23 July 2016
30	Tutorial (G3,G1,G2) - RSA	20, 21, 22 July 2016
31	ECC	25 July 2016
32	Key distribution	26 July 2016
UNIT-III: Message Authentication Algorithms and Hash Functions		
33	Authentication requirements	29 July 2016
34	Functions	30 July 2016
35	Tutorial (G3,G1,G2) – Message Authentication	27, 28, 29 July 2016
36	Message authentication codes	2 August 2016
37	Hash functions	5 August 2016
38	Secure hash algorithm, whirlpool	6 August 2016
39	Tutorial (G3,G1,G2) - Hashing	3, 4, 5 August 2016
40	HMAC	16 August 2016
41	CMAC	19 August 2016
42	Digital signatures	20 August 2016
43	Kerberos	22 August 2016
44	Authentication service	23 August 2016

45	Public key infrastructure	26 August 2016
46	Knapsack algorithm	27 August 2016
47	Tutorial (G3, G2) - HMAC	17,1 8, 19 August 2016
48	Biometric authentication	29 August 2016
UNIT-IV: E-Mail Security		
49	Preety good privacy	30 August 2016
50	S/MIME	2 September 2016
51	IP security architecture	3 September 2016
52	Tutorial (G3,G1,G2) - PGP	31 August, 2 September 2016
53	Authentication header	6 September 2016
54	Encapsulating security payload	9 September 2016
55	Combining security associations	10 September 2016
56	Tutorial (G3,G1,G2) – S/MIME	7, 8, 9 September 2016
UNIT-V: Web Security, Firewalls		
57	Web security considerations	13 September 2016
58	Secure socket layer	16 September 2016
59	Transport layer security	17 September 2016
60	Tutorial (G3,G1,G2) - SSL	14, 15, 16 September 2016
61	Transaction Intruders ,Virus	19 September 2016
62	Intruders	20 September 2016
63	Intrusion detection	23 September 2016
64	Password management	24 September 2016
65	Tutorial (G3,G1,G2) - TLS	21, 22, 23 September 2016
66	Virus related threats	26 September 2016
67	Countermeasures	27 September 2016
68	Firewall design principles	1 October 2016
69	Tutorial (G3,G1) - Firewall	28, 29 September 2016
70	Types of firewalls	3 October 2016
71	Case studies on cryptography and security	4 October 2016
72	Tutorial (G1,G2) - Virus	27, 28 October 2016
73	Secure inter-branch payment transactions	28 October 2016
74	Cross Site scripting vulnerablility	29 October 2016
75	Tutorial (G3) - Intruders	3 November 2016
76	Virtual elections	31 October 2016
77	Revision	2 November 2016

Text books:
1. Cryptography and Network Security: William Stallings, Pearson Education 4th Edition.
2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 2nd Edition.
3. Cryptography and Network Security: C K Shyamala , N Harini, Dr T R Padmanabhan,Wiley India, 1st edition.

Name and signature of the faculty: Ch Sushma

Name and signature of Head of the Department: Mr G Srinivasa Rao