Bhoj Reddy Engineering College for Women: Hyderabad

Department of Information Technology

Lesson plan of faculty member for the academic year 2017–18

Class: IV B Tech Branch-Section: IT-A 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	Introduction, The need for security	12 July 2017
2	Security Attacks, Security Services	13 July 2017
3	Principles of security	15 July 2017
4	Tutorial (G1,G2) – Types of security	13, 15 July 2017
5	Security mechanisms	18 July 2017
6	A model for Internetwork security	19 July 2017
7	Cryptography introduction	20 July 2017
8	Substitution techniques	22 July 2017
9	Tutorial (G1,G2) – Concepts preparation	20, 22 July 2017
10	Transposition techniques	25 July 2017
11	Encryption and decryption	26 July 2017
12	Symmetric and Asymmetric key cryptography	27 July 2017
13	Steganography	29 July 2017
14	Tutorial (G1,G2,G3) - Revision	27, 29, 24 July 2017
15	Key range and key size ,Types of Attacks	1 August 2017
UNIT-II: **Symmetric Key Ciphers**		
16	Block cipher principles	2 August 2017
17	Algorithms(DES)	3 August 2017
18	AES, Blowfish	5 August 2017
19	Tutorial (G1,G2,G3) – DES Example	3, 5 August 2017,31 July
20	Differential and linear cryptanalysis	8 August 2017
21	Block cipher modes of operation	9 August 2017
22	RC4	10 August 2017
23	Location and placement of encryption function	12 August 2017
24	Tutorial (G1,G2,G3) – AES example	10, 12, 7 August 2017
25	Key distribution Asymmetric key ciphers	16 August 2017
26	Algorithms(RSA)	17 August 2017
27	Diffie-Hellman	19 August 2017
28	Tutorial (G1,G2,G3) - RSA	17, 19 August 2017
29	ECC	22 August 2017
30	Key distribution	23 August 2017
UNIT-III: **Message Authentication Algorithms and Hash Functions**		
31	Authentication requirements	24 August 2017
32	Functions	26 August 2017
33	Tutorial (G1,G2,G3) – Message Authentication	24, 26, 21 August 2017
34	Message authentication codes	29 August 2017
35	Hash functions	30 August 2017
36	Secure hash algorithm	31 August 2017
37	Tutorial (G1,G3)-hashing	31, 28 August 2017
38	whirlpool	4 September 2017
39	HMAC,CMAC	5 September 2017
40	Public key infrastructure	9 September 2017
41	Tutorial (G2,G3)-hashing	9, 4 September 2017
42	Knapsack algorithm	12 September 2017
43	Digital signatures	13 September 2017

44	Kerberos	14 September 2017
45	Authentication service	16 September 2017
46	Tutorial (G1,G2,G3) – Kerberos	14,16,11 September 2017
47	Biometric authentication	19 September 2017
48	Revision	21 September 2017
UNIT-IV: **E-Mail Security**		
49	Pretty good privacy	23 September 2017
50	Tutorial (G1,G2,G3) - PGP	21, 23,18 September 2017
51	S/MIME	3 October 2017
52	IP Security Architecture	4 October 2017
53	Authentication header	5 October 2017
54	Encapsulating security payload	7 October 2017
55	Tutorial (G1,G2) – S/MIME	5, 7 October 2017
56	Combining Security Associations	10 October 2017
57	Key management	11 October 2017
UNIT-V: Web Security, Firewalls		
58	Web security considerations	12 October 2017
59	Tutorial (G1,G3) – Revision	12, 9 October 2017
60	Secure socket layer	17 October 2017
61	Transport layer security	19 October 2017
62	Transaction Intruders	21 October 2017
63	Tutorial (G1,G2,G3) - TLS	19, 21, 16 October 2017
64	Intruders	24 October 2017
65	Intrusion detection, Password management	25 October 2017
66	Virus, Virus related threats, Countermeasures	26 October 2017
67	Cross site scripting vulnerability, Intruders	28 October 2017
68	Tutorial (G1,G2,G3) - Test	26, 28, 23 October 2017
69	Firewall design principles, Types of firewalls	31 October 2017
70	Case studies on cryptography and security	1 November 2017
71	Secure inter-branch payment transactions	2 November 2017
72	Case studies on cryptography	7 November 2017
73	Tutorial (G1,G2,G3) - Revision	2, 6 November ,30 October 2017

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: M. Sandhya Rani

Name and signature of Head of the Department: Mr K. Sandeep Kumar