

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-B

Semester: I

Subject: Information Security

Lectures per week: 4+1 (Tutorial)

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

44	Tutorial (G3,G1,G2)-kerberos	12, 13, 15 September 2017
45	Public key infrastructure	18 September 2017
46	Knapsack algorithm	19 September 2017
47	Biometric authentication	22 September 2017
48	Revision	23 September 2017
UNIT-IV: E-Mail Security		
49	Tutorial (G3,G2)-Revision of unit-III	19, 22 September 2017
50	Pretty good privacy	4 October 2017
51	S/MIME	6 October 2017
52	IP security architecture	7 October 2017
53	Tutorial (G3,G1) - PGP	3, 4 October 2017
54	Authentication header	9 October 2017
55	Encapsulating security payload	10 October 2017
56	Combining security associations	13 October 2017
57	Tutorial (G3,G1,G2) – S/MIME	10, 11, 13 October 2017
UNIT-V: Web Security, Firewalls		
58	Web security considerations	16 October 2017
59	Secure socket layer	17 October 2017
60	Transport layer security	20 October 2017
61	Transaction Intruders ,Virus	21 October 2017
62	Tutorial (G3,G2) – SSL,TLS	17, 20 October 2017
63	Intruders, Intrusion detection	23 October 2017
64	Password management, Countermeasures	24 October 2017
65	Firewall design principles, Types of firewalls	27 October 2017
66	Case studies on cryptography and security	28 October 2017
67	Tutorial (G3,G1,G2) - test	24, 25, 27 October 2017
68	Secure inter-branch payment transactions	30 October 2017
69	Cross Site scripting vulnerability	31 October 2017
70	Viruses, Virus related threats	3 November 2017
71	Tutorial (G3,G1,G2) – test	31 October, 1, 3 November 2017
72	Virtual elections	6 November 2017
73	Revision	7 November 2017
74	Tutorial (G3)- Revision	7 November 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: K. Sandeep Kumar