ST.ANN'S COLLEGE OF ENGINEERING & TECHNOLOGY ::CHIRALA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

LECTURE SCHEDULE

NAME OF THE SUBJECT: Cryptography and Network Security **ACADEMIC YEAR:2017-18**

NAME OF THE FACULTY: T.SESHASAI

Year & Sem/Section: IV CSE-I SEM 'A'

No. of Lectures per week : 4+1* (Tutorial)

S.NO	DATE	TOPICS	UNIT
1	19.Jun.17	Introduction, Security attacks	I
2	20.Jun.17	services & mechanisms, Symmetric Cipher Model,	
3	22.Jun.17	Substitution Techniques,	
4	23.Jul.17	Transposition Techniques,	
5	24.Jul.17	Cyber threats and their defence, Phishing Defensive,measures,	
6	27.Jul.17	Tutorial	
7	29.Jul.17	web based attacks, SQL injection & Defence techniques,	
8	30.Jul.17	Buffer overflow & format string vulnerabilities,	
9	01.Jul.17	TCP session hijacking, ARP attacks, route table modification, UDP hijacking, man-in-the-middle attacks	
10	03.Jul.17	Tutorial	
11	04.Jul.17	Slip test	
12	06.Jul.17	Traditional Block Cipher Structure, DES,	II
13	07.Jul.17	Block Cipher Design Principles,	
14	10.Jul.17	AES-Structure, Transformation functions,	
15	11.Jul.17	Tutorial	
16	13.Jul.17	Key Expansion	
17	14.Jul.17	Blowfish	
18	15.Jul.17	CAST-128	
19	17.Jul.17	IDEA, Block Cipher Modes of Operations	
20	18.Jul.17	Tutorial	
21	20.Jul.17	slip test	
22	21.Jul.17	Number Theory: Prime and Relatively Prime Numbers,	III
23	22.Jul.17	Modular Arithmetic, Fermat's and Euler's Theorems,	
24	24.Jul.17	The Chinese Remainder theorem,	
25	25.Jul.17	Tutorial	
26	27.Jul.17	Discrete logarithms.	
27	28.Jul.17	Public Key Cryptography: Principles,	
28	29.Jul.17	public key cryptography algorithms,	
29	31.Jul.17	public key cryptography algorithms,	
30	01.Aug.17	Tutorial	
31	03.Aug.17	RSA Algorithms,	
32	04.Aug.17	RSA Algorithms,	
33	05.Aug.17	Diffie Hellman Key Exchange,	
34	07.Aug.17	Diffie Hellman Key Exchange,	
35	08.Aug.17	Elgamal encryption & decryption	
36	10.Aug.17	Elliptic Curve Cryptography	
37	11.Aug.17	Revision	
38	12.Aug.17	Revision	
39	17.Aug.17	Revision	
40	18.Aug.17	Revision	
41	18.Aug.17	Revision	
42	21.Aug.17	Revision	

43	22.Aug.17	Tutorial	
44	24.Aug.17	Application of Cryptographic hash Functions,	
45	28.Aug.17	Requirements & Security,	
46	29.Aug.17	Secure Hash Algorithm,	
47	31.Aug.17	Secure Hash Algorithm	IV
48	01.Sep.17	Message Authentication Functions,	
49	04.Sep.17	Message Authentication Functions,	
50	05.Sep.17	Requirements & Security	
51	07.Sep.17	HMAC & CMAC.	
52	08.Sep.17	HMAC & CMAC	
53	11.Sep.17	NIST Digital Signature Algorithm	
54	12.Sep.17	NIST Digital Signature Algorithm	
55	14.Sep.17	Tutorial	
56	15.Sep.17	Key management & distribution	
57	16.Sep.17	Slip test	
58	18.Sep.17	User Authentication: Remote user authentication principles,	
59	19.Sep.17	User Authentication: Remote user authentication principles,	
60	21.Sep.17	Tutorial	
61	22.Sep.17	Kerberos	
62	23.Sep.17	Transport Level Security: Web Security Requirements,Secure Socket Layer (SSL)	V
63	25.Sep.17	Transport Layer Security (TLS), Secure Shell(SSH)	
64	26.Sep.17	Electronic Mail Security: Pretty Good Privacy (PGP) and S/MIME	
65	03.Okt.17	Slip test	
66	05.Okt.17	IP Security: IP Security Overview,	
67	06.Okt.17	IP Security Architecture,	
68	07.Okt.17	Authentication Header, Encapsulating Security Payload,	
69	09.Okt.17	Approaches for IDS/IPS	
70	10.Okt.17	Combining Security Associations and Key Management.	
71	12.Okt.17	Combining Security Associations and Key Management	
72	13.Okt.17	Intrusion detection: Signature based IDS	
73	14.Okt.17	Host based IDS/IPS	VI
74	16.Okt.17	Revision	
75	17.Okt.17	Revision	
76	19.Okt.17	Revision	
77	20.Okt.17	Revision	
78	21.Okt.17	Tutorial	
79	23.Okt.17	Revision	

TEXT BOOKS:

1. Cryptography & Network Security: Principles and Practices, William Stallings, PEA, Sixth edition.
2. Introduction to Computer Networks & Cyber Security, Chwan Hwa Wu, J.David Irwin, CRC press
3. Hack Proofing your Network, Russell, Kaminsky, Forest Puppy, Wiley Dreamtech.

REFERENCE BOOKS:

1. Everyday Cryptography, Fundamental Principles & Applications, Keith Martin, Oxford
2. Network Security & Cryptography, Bernard Menezes, Cengage,2010

FACULTY **HOD**

HOD