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:2018-19**

NAME OF THE FACULTY: T.Seshasai

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

No. of Lectures per week : 5+1* (Tutorial)

S.NO	DATE	TOPICS	UNIT
1	11-Jun-18	Introduction:Securityattacks	
2	11-Jun-18	services&mechanisms	
3	**12-Jun-18**	SymmetricCipherModel	
4	13-Jun-18	SubstitutionTechniques	
5	**14-Jun-18**	TransportationTechniques	
6	**18-Jun-18**	Cyberthreatsandtheirdefense	
7	**18-Jun-18**	Tutorial	
8	19-Jun-18	PhishingDefensivemeasures	I
9	**20-Jun-18**	webbasedattacks,SQLinjection&Defense	
10	21-Jun-18	Bufferoverflow&formatstringvulnerabilities	
11	**22-Jun-18**	TCPsessionhijacking(ARPattacks,routetablemodification)	
12	25-Jun-18	UDPhijacking (man-in-the-middleattacks)	
13	25-Jun-18	Tutorial	
14	**26-Jun-18**	Revision	
15	27-Jun-18	Slip test	
16	**28-Jun-18**	TraditionalBlockCipherStructure	
17	29-Jun-18	DES,BlockCipherDesignPrinciples	
18	**2-Jul-18**	AES-Structure	
19	**2-Jul-18**	Tutorial	
20	3-Jul-18	AES-Structure	
21	**4-Jul-18**	Transformationfunctions	
22	5-Jul-18	KeyExpansion,Blowfish	II
23	**6-Jul-18**	CAST-128	
24	9-Jul-18	IDEA,Block Cipher Modes ofOperations	
25	9-Jul-18	Tutorial	
26	**10-Jul-18**	Revision	
27	11-Jul-18	slip test	
28	**12-Jul-18**	NumberTheory:PrimeandRelativelyPrimeNumbers	
29	13-Jul-18	ModularArithmetic	
30	**16-Jul-18**	Fermat'sandEuler'sTheorems	
31	**16-Jul-18**	Tutorial	
32	17-Jul-18	TheChinese Remainder theorem	
33	**18-Jul-18**	DiscreteAlogarithms	
34	19-Jul-18	PublicKeyCryptography:Principles	
35	**20-Jul-18**	publickeycryptographyalgorithms	
36	23-Jul-18	publickeycryptographyalgorithms	
37	23-Jul-18	Tutorial	
38	**24-Jul-18**	RSAAlgorithms	
39	25-Jul-18	RSAAlgorithms	
40	**26-Jul-18**	DiffieHellmanKeyExchange	III
41	27-Jul-18	Elgamalencryption&decryption	
42	**30-Jul-18**	EllipticCurveCryptography	
43	**30-Jul-18**	Tutorial	

44	31-Jul-18	Revision	
45	**1-Aug-18**	Revision	
46	2-Aug-18	Revision	
47	**3-Aug-18**	Revision	
48	6-Aug-18	MID EXAM-I	
49	**7-Aug-18**	MID EXAM-I	
50	8-Aug-18	MID EXAM-I	
51	**9-Aug-18**	MID EXAM-I	
52	10-Aug-18	MID EXAM-I	
53	**13-Aug-18**	ApplicationofCryptographicHashFunctions	
54	**13-Aug-18**	Tutorial	
55	14-Aug-18	Requirements&Security	
56	16-Aug-18	SecureHashAlgorithm	
57	**17-Aug-18**	MessageAuthenticationFunctions	
58	20-Aug-18	Requirements&Security	
59	20-Aug-18	Tutorial	
60	**21-Aug-18**	HMAC&CMAC	IV
61	**23-Aug-18**	DigitalSignatures	
62	24-Aug-18	NISTDigital SignatureAlgorithm	
63	**27-Aug-18**	Keymanagement&distribution	
64	**27-Aug-18**	Tutorial	
65	28-Aug-18	Revision	
66	**29-Aug-18**	Revision	
67	30-Aug-18	Slip test	
68	**31-Aug-18**	User Authentication	
69	**4-Sep-18**	Remote userauthentication principles	
70	5-Sep-18	Kerberos	
71	**6-Sep-18**	TransportLevelSecurity	
72	7-Sep-18	WebSecurityRequirements	
73	**10-Sep-18**	SecureSocketLayer(SSL)	
74	**10-Sep-18**	Tutorial	
75	11-Sep-18	TransportLayerSecurity(TLS),	V
76	**12-Sep-18**	SecureShell(SSH)	
77	17-Sep-18	ElectronicMailSecurity	
78	17-Sep-18	Tutorial	
79	**18-Sep-18**	PrettyGoodPrivacy(PGP)andS/MIME	
80	19-Sep-18	Revision	
81	**20-Sep-18**	Tutorial	
82	**24-Sep-18**	slip test	
83	**24-Sep-18**	IP Security: IP Security Overview	
84	25-Sep-18	IP SecurityArchitecture	
85	**26-Sep-18**	AuthenticationHeader	
86	27-Sep-18	EncapsulatingSecurity Payload	
87	**28-Sep-18**	CombiningSecurityAssociationsandKey Management	VI
88	1-Oct-18	Intrusion detection: Overview	
89	1-Oct-18	Tutorial	
90	3-Oct-18	ApproachesforIDS/IPS:signature & host based	
91	4-Oct-18	Revision	
92	5-Oct-18	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**