

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: D.Nagesh Babu****Year & Sem/Section: IV CSE-I SEM 'B'****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	1-Jul-17	TCP session hijacking, ARP attacks, route table modification, UDP hijacking, man-in-the-middle attacks	
10	3-Jul-17	Tutorial	
11	4-Jul-17	Slip test	II
12	6-Jul-17	Traditional Block Cipher Structure, DES,	
13	7-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	III
22	21-Jul-17	Number Theory: Prime and Relatively Prime Numbers,	
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	1-Aug-17	Tutorial	
31	3-Aug-17	RSA Algorithms,	
32	4-Aug-17	RSA Algorithms,	
33	5-Aug-17	Diffie Hellman Key Exchange,	
34	7-Aug-17	Diffie Hellman Key Exchange,	
35	8-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	IV
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	
48	1-Sep-17	Message Authentication Functions,	
49	4-Sep-17	Message Authentication Functions,	
50	5-Sep-17	Requirements & Security	
51	7-Sep-17	HMAC & CMAC.	
52	8-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,	V
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)	
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	3-Oct-17	Slip test	
66	5-Oct-17	IP Security: IP Security Overview,	
67	6-Oct-17	IP Security Architecture,	
68	7-Oct-17	Authentication Header, Encapsulating Security Payload,	
69	9-Oct-17	Approaches for IDS/IPS	
70	10-Oct-17	Combining Security Associations and Key Management.	
71	12-Oct-17	Combining Security Associations and Key Management	
72	13-Oct-17	Intrusion detection: Signature based IDS	VI
73	14-Oct-17	Host based IDS/IPS	
74	16-Oct-17	Revision	
75	17-Oct-17	Revision	
76	19-Oct-17	Revision	
77	20-Oct-17	Revision	
78	21-Oct-17	Tutorial	
79	23-Oct-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