ST.ANN'S COLLEGE OF ENGINEERING & TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
LECTURE SCHEDULE

NAME OF THE SUBJECT: **Cryptography and Network Security** ACADEMIC YEAR:**2018-19**
NAME OF THE FACULTY: **Mr.D.Nagesh Babu**
Year & Sem/Section: **IV CSE-I SEM 'C'**
No. of Lectures per week **: 5+1* (Tutorial)**

S.NO	DATE	TOPICS	UNIT
1	11-Jun-18	Introduction, Security attacks	1
2	12-Jun-18	services & mechanisms, Symmetric Cipher Model,	
3	13-Jun-18	Substitution Techniques,	
4	14-Jun-18	Transposition Techniques,	
5	18-Jun-18	Cyber threats and their defense, Phishing Defensive measures,	
6	19-Jun-18	web based attacks, SQL injection & Defense techniques,	
7	20-Jun-18	Buffer overflow & format string vulnerabilities,	
8	21-Jun-18	TCP session hijacking, ARP attacks,	
9	22-Jun-18	Tutorial	
10	23-Jun-18	Route table modification, UDP hijacking, man-in-the-middle attacks	
11	25-Jun-18	PPT's on I Unit	
12	26-Jun-18	Slip Test-I	
13	27-Jun-18	Traditional Block Cipher Structure, DES,	2
14	28-Jun-18	Block Cipher Design Principles,	
15	29-Jun-18	Tutorial	
16	30-Jun-18	AES-Structure, Transformation functions,	
17	02-Jul-18	Key Expansion,	
18	03-Jul-18	Blowfish,	
19	04-Jul-18	CAST-128,	
20	05-Jul-18	IDEA, Block Cipher Modes of Operations	
21	06-Jul-18	Tutorial	
22	07-Jul-18	PPT's on II Unit	
23	09-Jul-18	Slip Test-2	
24	10-Jul-18	Number Theory: Prime and Relatively Prime Numbers,	3
25	11-Jul-18	Modular Arithmetic, Fermat's and Euler's Theorems,	
26	12-Jul-18	The Chinese Remainder theorem,	
27	13-Jul-18	Tutorial	
28	14-Jul-18	Discrete logarithms.	
29	16-Jul-18	Public Key Cryptography: Principles,	
30	17-Jul-18	public key cryptography algorithms,	
31	18-Jul-18	public key cryptography algorithms,	
32	19-Jul-18	RSA Algorithms,	
33	20-Jul-18	Tutorial	
34	21-Jul-18	RSA Algorithms,	
35	23-Jul-18	Diffie Hellman Key Exchange,	
36	24-Jul-18	Diffie Hellman Key Exchange,	
37	25-Jul-18	Elgamal encryption & decryption	
38	26-Jul-18	Elliptic Curve Cryptography	
39	27-Jul-18	Tutorial	
40	28-Jul-18	PPT's on III Unit	
41	30-Jul-18	Revision	
42	31-Jul-18	Revision	
43	01-Aug-18	Revision	
44	02-Aug-18	Revision	

SNIET-CSE

45	03-Aug-18	Revision	
46	04-Aug-18	Revision	
47	06-Aug-18	Revision-MID I	
48	07-Aug-18	Revision-MID I	
49	08-Aug-18	Revision-MID I	
50	09-Aug-18	Revision-MID I	
51	10-Aug-18	Revision-MID I	
52	11-Aug-18	Revision-MID I	
53	13-Aug-18	Application of Cryptographic hash Functions,	4
54	14-Aug-18	Requirements & Security,	
55	16-Aug-18	Secure Hash Algorithm,	
56	17-Aug-18	Tutorial	
57	18-Aug-18	Secure Hash Algorithm	
58	20-Aug-18	Message Authentication Functions,	
59	21-Aug-18	Message Authentication Functions,	
60	23-Aug-18	Requirements & Security	
61	24-Aug-18	Tutorial	
62	25-Aug-18	HMAC & CMAC	
63	27-Aug-18	HMAC & CMAC	
64	28-Aug-18	NIST Digital Signature Algorithm	
65	29-Aug-18	NIST Digital Signature Algorithm	
66	30-Aug-18	Key management & distribution	
67	31-Aug-18	Tutorial	
68	04-Sep-18	PPT's on UNIT-4	
69	05-Sep-18	Slip Test-3	
70	06-Sep-18	User Authentication: Remote user authentication principles,	5
71	07-Sep-18	Tutorial	
72	08-Sep-18	User Authentication: Remote user authentication principles,	
73	10-Sep-18	Kerberos	
74	11-Sep-18	Transport Level Security: Web Security Requirements, Secure Socket Layer (SSL)	
75	12-Sep-18	Electronic Mail Security: Pretty Good Privacy (PGP) and S/MIME	
76	15-Sep-18	PPT's on UNIT-5	
77	17-Sep-18	Slip Test-4	
78	18-Sep-18	IP Security: IP Security Overview,	6
79	19-Sep-18	IP Security Architecture,	
80	20-Sep-18	Authentication Header, Encapsulating Security Payload	
81	22-Sep-18	Combining Security Associations and Key Management.	
82	24-Sep-18	Combining Security Associations and Key Management	
83	25-Sep-18	Intrusion detection: Overview,	
84	26-Sep-18	Approaches for IDS/IPS	
85	27-Sep-18	Signature based IDS	
86	28-Sep-18	Host based IDS/IPS	
87	29-Sep-18	PPT's on Unit-6	
88	01-Oct-18	Revision	
89	03-Oct-18	Revision	
90	04-Oct-18	Revision	
91	05-Oct-18	Revision	
92	06-Oct-18	Revision	
93	08-Oct-18	Revision-II MID	
94	09-Oct-18	Revision-II MID	
95	10-Oct-18	Revision-II MID	

CSE-CSE

96	11-Oct-18	Revision-II MID	
97	12-Oct-18	Revision-II MID	
98	13-Oct-18	Revision-II MID	

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**

SACET-CSE