

**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 'A'**

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	12-Jun-18	Substitution Techniques,	
4	13-Jun-18	Transposition Techniques,	
5	14-Jun-18	Cyber threats and their defense, Phishing Defensive measures,	
6	18-Jun-18	web based attacks, SQL injection & Defense techniques,	
7	19-Jun-18	Buffer overflow & format string vulnerabilities,	
8	19-Jun-18	Tutorial	
9	20-Jun-18	TCP session hijacking, ARP attacks,	
10	21-Jun-18	Route table modification, UDP hijacking, man-in-the-middle attacks	
11	22-Jun-18	PPT's on I Unit	
12	25-Jun-18	Slip Test-I	2
13	26-Jun-18	Traditional Block Cipher Structure, DES,	
14	26-Jun-18	Tutorial	
15	27-Jun-18	Block Cipher Design Principles,	
16	28-Jun-18	AES-Structure, Transformation functions,	
17	29-Jun-18	Key Expansion,	
18	02-Jul-18	Blowfish,	
19	03-Jul-18	CAST-128,	
20	03-Jul-18	Tutorial	
21	04-Jul-18	IDEA, Block Cipher Modes of Operations	
22	05-Jul-18	PPT's on II Unit	
23	06-Jul-18	Slip Test-2	3
24	09-Jul-18	Number Theory: Prime and Relatively Prime Numbers,	
25	10-Jul-18	Modular Arithmetic, Fermat's and Euler's Theorems,	
26	10-Jul-18	Tutorial	
27	11-Jul-18	The Chinese Remainder theorem,	
28	12-Jul-18	Discrete logarithms.	
29	13-Jul-18	Public Key Cryptography: Principles,	
30	16-Jul-18	public key cryptography algorithms,	
31	17-Jul-18	public key cryptography algorithms,	
32	17-Jul-18	Tutorial	
33	18-Jul-18	RSA Algorithms,	
34	19-Jul-18	RSA Algorithms,	
35	20-Jul-18	Diffie Hellman Key Exchange,	
36	23-Jul-18	Diffie Hellman Key Exchange,	
37	24-Jul-18	Elgamal encryption & decryption	
38	24-Jul-18	Tutorial	
39	25-Jul-18	Elliptic Curve Cryptography	
40	26-Jul-18	PPT's on III Unit	
41	27-Jul-18	Revision	
42	30-Jul-18	Revision	
43	31-Jul-18	Revision	
44	31-Jul-18	Tutorial	

45	01-Aug-18	Revision	4
46	02-Aug-18	Revision	
47	03-Aug-18	Revision	
48	06-Aug-18	Revision-MID I	
49	07-Aug-18	Revision-MID I	
50	07-Aug-18	Revision-MID I	
51	08-Aug-18	Revision-MID I	
52	09-Aug-18	Revision-MID I	
53	10-Aug-18	Revision-MID I	
54	13-Aug-18	Application of Cryptographic hash Functions,	
55	14-Aug-18	Requirements & Security,	
56	14-Aug-18	Secure Hash Algorithm,	
57	16-Aug-18	Secure Hash Algorithm	
58	17-Aug-18	Message Authentication Functions,	
59	20-Aug-18	Message Authentication Functions,	
60	21-Aug-18	Requirements & Security	
61	21-Aug-18	Tutorial	
62	23-Aug-18	HMAC & CMAC	
63	24-Aug-18	HMAC & CMAC	
64	27-Aug-18	NIST Digital Signature Algorithm	
65	28-Aug-18	NIST Digital Signature Algorithm	
66	28-Aug-18	Tutorial	
67	29-Aug-18	Key management & distribution	
68	30-Aug-18	PPT's on UNIT-4	
69	31-Aug-18	Slip Test-3	
70	04-Sep-18	User Authentication: Remote user authentication principles,	
71	04-Sep-18	Tutorial	
72	05-Sep-18	User Authentication: Remote user authentication principles,	
73	06-Sep-18	Kerberos	
74	07-Sep-18	Transport Level Security: Web Security Requirements, Secure Socket Layer (SSL)	
75	10-Sep-18	Electronic Mail Security: Pretty Good Privacy (PGP) and S/MIME	
76	11-Sep-18	PPT's on UNIT-5	
77	11-Sep-18	Slip Test-4	
78	12-Sep-18	IP Security: IP Security Overview,	
79	17-Sep-18	IP Security Architecture,	
80	18-Sep-18	Authentication Header, Encapsulating Security Payload	
81	18-Sep-18	Tutorial	
82	19-Sep-18	Combining Security Associations and Key Management.	
83	20-Sep-18	Combining Security Associations and Key Management	
84	24-Sep-18	Intrusion detection: Overview,	
85	25-Sep-18	Approaches for IDS/IPS	
86	25-Sep-18	Tutorial	
87	26-Sep-18	Signature based IDS	
88	27-Sep-18	Host based IDS/IPS	
89	28-Sep-18	PPT's on Unit-6	
90	01-Oct-18	Revision	
91	03-Oct-18	Revision	
92	04-Oct-18	Revision	
93	05-Oct-18	Revision	
94	08-Oct-18	Revision-II MID	
95	09-Oct-18	Revision-II MID	
			5
			6

96	09-Oct-18	Revision-II MID	
97	10-Oct-18	Revision-II MID	
98	11-Oct-18	Revision-II MID	
99	12-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