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:**2019-20**
NAME OF THE FACULTY: **Mr.T.Seshasai**
Year &Sem/Section: **IV CSE-I SEM 'A'**
No. of Lectures per week **: 5+1* (Tutorial)**

SI.NO	DATE	TOPIC NAME	UNIT
1	10-06-19	U-I INTRODUCTION	UNIT - I
2	11-06-19	SECURITY GOALS	
3	12-06-19	CRYPTOGRAPHY ATTACKS	
4	13-06-19	SECURITY SERVICES	
5	14-06-19	SECURITY MECHANISMS	
6	15-06-19	MATHEMATICS OF CRYPTOGRAPHY	
7	17-06-19	MODULAR ARITHMATIC, MATRICES & LINEAR CONGRUENCE	
8	18-06-19	THE EXTENDED EUCLIDEAN ALGORITHM	
9	19-06-19	NPTL VIDEOS/PPT	
10	20-06-19	TUTORIAL	
11	21-06-19	SLIPTEST	
12	22-06-19	U-II INTRODUCTION	UNIT-II
13	24-06-19	SYMMETRIC KEY CIPHERS	
14	25-06-19	TRADITIONAL CIPHERS	
15	26-06-19	TRANSPOSITION CIPHERS	
16	27-06-19	TUTORIAL	
17	28-06-19	STREAM AND BLOCK CIPHERS	
18	29-06-19	MODERN SYMMENTRIC KEY CIPHERS	
19	01-07-19	COMPONENTS OF MODERN BLOCK CIPHER	
20	02-07-19	PRODUCT CIPHERS, FEISTEL CIPHER	
21	03-07-19		
22	04-07-19	TUTORIAL	
23	05-07-19	MODERN STREAM CIPHER	
24	06-07-19	ATTACKS DESIGNED FOR BLOCK CIPHERS	
25	08-07-19	DATA ENCRYPTION STANDARD(DES)	
26	09-07-19	DES ANALYSIS	
27	10-07-19	MULTIPLE DES	
28	11-07-19	TUTORIAL	
29	12-07-19	ADVANCED ENCRYPTION STANDARD(AES)	
30	15-07-19	THE AES CIPHER	
31	16-07-19	SLIPTEST	

32	17-07-19	U-III INTRODUCTION	UNIT -III
33	18-07-19	TUTORIAL	
34	19-07-19	ASYMMETRIC KEY CRYPTOGRAPHY	
35	20-07-19	PRIMALILY TESTING	
36	22-07-19	CHINESE REMAINDER THEOREM(CRM)	
37	23-07-19	FACTORIZATION,QUADRATIC CONGRUENCE	
38	24-07-19	DIFFERENCE BETWEEN SYMMETRIC AND ASYMMETRIC KEY	
39	25-07-19	TUTORIAL	
40	26-07-19	RSA ALGORITHM	
41	27-07-19	RABIN CRYPTOSYSTEM, CLLIPTIC CURVE CRYPTOSYSTEM	
42	29-07-19	ELGAMMAL CRYPTOSYSTEM	
43	30-07-19	NPTL VIDEOS/PPT	
44	31-07-19	SLIPTEST	
45	01-08-19	TUTORIAL	
46	02-08-19	REVISION	
47	03-08-19	REVISION	
48	05-08-19	MID-I	
49	06-08-19	MID-I	
50	07-08-19	MID-I	
51	08-08-19	MID-I	
52	09-08-19	MID-I	
53	10-08-19	MID-I	
54	13-08-19	U-IV INTRODUCTION MESSAGE INTEGRITY	UNIT-IV
55	14-08-19	RANDOM ORACLE MODEL	
56	16-08-19	MESSAGE AUTHENTICATION	
57	17-08-19	CRYPTOGRAPHIC HASH FUNCTION,ITERATED MD	
58	19-08-19	SHA 512 ALGORITHM	
59	20-08-19	DIGITAL SIGNATURE,COMPARISSION,PROCESS	
60	21-08-19	ATTACKS ON DIGITAL SIGNATURE	
61	22-08-19	TUTORIAL	
62	26-08-19	DIGITAL SIGNATURE SCHEMES,VARIATTION AND APPLICATIONS	
63	27-08-19	SYMMETRIC KEY DISTRIBUTION	
64	28-09-19	KERBEROS,SYMMETRIC KEY AGREEMENTS	
65	29-08-19	TUTORIAL	
66	30-08-19	PUBLIC KEY DISTRIBUTION, HIJACKING	
67	31-08-19	SLIPTEST	
68	03-09-19	NPTL VIDEOS/PPT	

69	04-09-19	U-V INTRODUCTION SECURITY AT APPLICATION LAYER	UNIT - V
70	05-09-19	TUTORIAL	
71	06-09-19	EMAIL SYSTEM	
72	07-09-19	PRETTY GOOD PRIVACY(PGP)	
73	09-09-19	SECURE/MULTIPURPOSE INTERNET MAIL EXTENSION(S/MIME)	
74	11-09-19	SECURITY AT TRANSPORT LAYER-SSL,TLS	
75	12-09-19	TUTORIAL	
76	13-09-19	SSL ARCHITECTURE,MESSAGE FORMATS	
77	16-09-19	NPTL VIDEOS/PPT	
78	17-09-19	SLIPTEST	
79	18-09-19	U-VI INTRODUCTION SECURITY AT NETWORK LAYER-IP SEC	UNIT - VI
80	19-09-19	TUTORIAL	
81	20-09-19	IP SECURITY(IP SEC)	
82	21-09-19	MODES OF IPSEC	
83	23-09-19	TWO SECURITY PROTOCOLS	
84	24-09-19	SECURITY ASSOCIATION, POLICY	
85	25-09-19	NPTL VIDEOS/PPT	
86	26-09-19	TUTORIAL	
87	27-09-19	INTERNET KEY EXCHANGE	
88	28-09-19	SYSTEM SECURITY ,BUFFER OVERFLOW AND MALICIOUS S/W	
89	30-09-19	INTRUSION DETECTION SYSTEM	
90	01-10-19	FIREWALL AND WORKING PRINCIPLES	
91	03-10-19	TUTORIAL	
92	04-10-19	REVISION	
93	05-10-19	REVISION	

TEXT BOOKS:

1) Cryptography and Network Security, Behrouz A Forouzan, DebdeepMukhopadhyay, (3e)Mc Graw Hill.

2) Cryptography and Network Security, William Stallings, (6e) Pearson.

3) Everyday Cryptography, Keith M.Martin, Oxford.

REFERENCE BOOKS:

1) **Network Security and Cryptography, Bernard Meneges, Cengage Learning.**

FACULTY **HOD**