AMIRAJ COLLEGE OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER ENGINEERING

TERM DATE: 20 JUNE -2016 - 21 OCTOBER - 2016

HOURS	DETAILS OF TOPIC TO BE COVERED	PLANNED DATES	ACTUAL DATES
I	**UNIT 1**		
1	Symmetric Cipher Model	**20/6/2016**	
2	Cryptography		
3	Cryptanalysis		
4	Attacks : Active attacks	**TO**	
5	Passive attacks		
6	Substitution techniques		
7	Transposition techniques	**29/6/2016**	
II	**UNIT 2**		
8	Stream ciphers	**1/7/2016**	
9	block ciphers		
10	Block Cipher structure		
11	Data Encryption standard (DES)		
12	Example of DES	**TO**	
13	Example of DES		
14	strength of DES		
15	Design principles of block cipher		
16	AES with structure		
17	AES transformation functions	**22/7/2016**	
III	**UNIT 3**		
18	Multiple encryption and triple DES	**25/7/2016**	
19	Electronic Code Book		
20	Cipher Block Chaining Mode	**TO**	
21	Cipher Feedback mode		
22	Output Feedback mode		
23	Counter mode	**29/7/2016**	
IV	**UNIT 4**		
24		**1/9/2016**	
25	Application of Public Key Cryptosystems		
26	Requirements of Public Key Cryptosystems		
27	Cryptanalysis		
28	RSA algorithm	**TO**	
29	RSA algorithm		
30	Its computational aspects and security		
31	Diffie-Hillman Key Exchange algorithm		

32	Diffie-Hillman Key Exchange algorithm		
33	Man-in-Middle attack	**15/9/2016**	
V	**UNTI 5**		
34	Cryptographic Hash Functions	**16/9/2016**	
35	Application of Cryptographic Hash Functions		
36	Simple hash	**TO**	
37	Hash functions based on Cipher Block Chaining		
38	Secure Hash Algorithm (SHA)	**21/9/2016**	
VI	**UNIT 6**		
39	Message Authentication Codes	**22/9/2016**	
40	its requirements and security		
41	MACs based on Hash Functions	**TO**	
42	MACs based on Hash Functions		
43	Macs based on Block Ciphers	**26/9/2016**	
VII	**UNTI 7**		
44	Digital Signature	**28/9/2016**	
45	its properties		
46	requirements and security	**TO**	
47	various digital signature schemes (Elgamal and Schnorr)		
48	NIST digital Signature algorithm	**29/9/2016**	
VIII	**UNTI 8**		
49	Key management and distribution	**30/9/2016**	
50	symmetric key distribution using symmetric encryption		
51	symmetric key distribution using asymmetric encryptions	**TO**	
52	Distribution of public keys		
53	X.509 certificates		
54	Public key infrastructure	**5/10/2016**	
IX	**UNTI 9**		
55	Remote user authentication with symmetric encryption	**6/10/2016**	
56	Remote user authentication with asymmetric encryption	**TO**	
57	Kerberos	**10/10/2016**	
X	**UNTI 10**		
58	Web Security threats	**13/10/2016**	
59	Web Security approaches		
60	SSL architecture		

61	SSL protocol	**TO**	
62	Transport layer security		
63	HTTPS		
64	SSH	**14/10/2016**	