

L.D. College of Engineering
Information Technology Department

Teaching Scheme			
Theory	Tutorial	Practical	Total
4	0	2	6
Subject Name:		Information and Network Security	Duration: Term start date : 18/6/2018 Term End date:17/10/2018
Subject Code:		2170709	
Branch & Semester:		(B.E. – V)	
Days		WED-1 THU-1	

Name of Faculty: Prof. J.S.VITHALPURA

Sr. No	Topic	Planned date	Actual date
1	Public Key Cryptosystems	20/6/18	
	Public Key Cryptosystems with Applications	21/6/18	
	Requirements and Cryptanalysis		
	Arithmetic of cryptography	27/6/18	
	RSA algorithm,	28/6/18	
	its computational aspects and security	4/7/18	
2	Diffie-Hillman Key Exchange algorithm,	5/7/2018	
	Man-in-Middle attack	11/7/2018	
	Design problem /Quiz	12/7/2018	
	Cryptographic Hash Functions, their application	18/7/2018 19/7/2018	
	Simple hash functions, its requirements and security	25/7/2018	
	Hash functions based on Cipher Block Chaining	26/7/2018	
3	Secure Hash Algorithm (SHA)	1/8/2017	
	Design problem /Quiz	2/8/2018	
	Message Authentication Codes, its requirements and security	8/8/2018	
	MACs based on Hash Functions	9/8/2018	
	Macs based on Block Ciphers	16/8/2018	
	Design problem /Quiz		

