Lesson Planning
June-2018

Prepared by : Hiteishi Diwanji
Term start date : 18/6/2016
Term End Date : 17/10/2018

BE SEMESTER VII(IT) A division
Subject : Information and Network Security

Subject code : 2170709
No of lectures : 2(Tuesday 1:15 to 2:15 p.m.
Thursday 11:45 to 12:45 p.m.)

Sr. No	Topic	Planned date	Actual date
1	Arithmetic of cryptography • Random number generation • Prime numbers • Totient function • Congruence relation	19/6/2018 21/6/2018 26/6/2018 28/6/2018	
2	Problem solving/quiz Video lecture (NPTEL/COURSEERA/EXPERT)	3/7/2018	
3	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	5/7/2018 10/7/2018 12/7/2018 17/7/2018 19/7/2018	
4	Problem solving/quiz	24/7/2018	
5	AES with structure, its transformation functions, key expansion, example and implementation	26/7/2018 31/7/2018	
6	Discussion of design problem(cryptography), case study	2/8/2018	
7	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	7/8/2018 9/8/2018 14/8/2018	

8	Problem solving/quiz Presentation of students(worm/virus/malware)	16/8/2018	
9	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	21/8/2018 23/8/2018 28/8/2018 30/8/2018	
10	Quiz/Design problem	4/9/2018	
6	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers	6/9/2018 11/9/2018	
7	Digital Signature, its properties, requirements and security various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	18/9/2018 20/9/2018	
8	Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure	25/9/2018	
9	Remote user authentication with symmetric and asymmetric encryption, Kerberos	27/9/2018	
10	Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH	4/10/2018	