L. D. College of Engineering, Ahmedabad – 15
LESSON PLAN

Over all Term Planning	
Branch:	Information Technology
Semester:	B.E 7th SEM
Subject Name:	Information and Network Security
Subject Code:	2170709
Affiliating University:	Gujarat Technological University
Starting date of the term:	18/6/2018
Ending date of the term:	17/10/2018
Course Teacher:	Prof. Pradip R. Patel

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks			Practical Marks			
L	T	P	C	ESE (E)	PA (M)		ESE (V)		PA (I)	
					PA	ALA	ESE	OEP		
4	0	2	6	70	20	10	20	10	20	150

L- Lectures; T- Tutorial/Teacher Guided Student Activity; P- Practical; C- Credit; ESE- End Semester Examination; PA- Progressive Assessment;

Syllabus

Sr. No.	**Content**	**Total HRS**	**% Weightage**
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	3	5%
2	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation	10	25%
3	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	4	5%
4	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	7	15%
5	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	4	10%
6	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers	3	10%
7	Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	4	8%
8	Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure	4	7%
9	Remote user authentication with symmetric and asymmetric	4	5%

	encryption, Kerberos		
10	Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH	5	10%

Reference Books:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Information Security Principles and Practice By Mark Stamp, Willy India Edition
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
4. Cryptography and Network Security Atul Kahate, TMH
5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
6. Information Systems Security, Godbole, Wiley-India
7. Information Security Principles and Practice, Deven Shah, Wiley-India
8. Security in Computing by Pfleeger and Pfleeger, PHI
9. Build Your Own Security Lab : A Field Guide for network testing, Michael Gregg, Wiley India

Lesson Plan

No of lectures: 2

Sr. No	Topic	Planned Date	Actual Date	Mode of Delivery	Resources required
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks	18/06/18 20/06/18 25/06/18 27/06/18 02/07/18			
2	Substitution and Transposition techniques	04/07/18 09/07/18 11/07/18			
3	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher **Quiz**	16/07/18 18/07/18 23/07/18 25/07/18 30/07/18			
4	AES with structure, its transformation functions, key expansion, example and implementation	01/08/18 06/08/18 08/08/18 13/08/18 20/08/18			
5	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode **Quiz**	27/08/18 29/08/18 05/09/18			
6	Remote user authentication with symmetric and asymmetric encryption, Kerberos	10/09/18 12/09/18 17/09/18			

7	Web Security threats and approaches, SSL architecture and protocol	19/09/18 24/09/18 26/09/18			
8	Transport layer security HTTPS and SSH **Quiz**	01/10/18 03/10/18			
9	Revision and Question Paper Solving	08/10/18 10/10/18			

Faculty Sign