Semester Plan
(Theory)

TCET/FRM/IP-02/09 **Revision: A**

Semester: VII **Course: CMPN**

Subject: CPC 702: Cryptography & System Security **Class: BE-CMPN A**

Sr.No.	Prerequisite/ Bridge course:	Duration (Week /Hrs)	Modes of Learning	Recommended Sources
1	Basics of Network: TCP/IP Model , Network Management/ Monitoring Tools	4 hours	Self Learning/ Revision	B.A. Forouzan, "Data Communications and Networking", TMH, Fourth Edition

Sr. No	Module No.	Lesson No	Topics Planned (Technology to be used)	Teaching Aids Required	Planned /Completion Date	Resource Book Reference	Remarks
1		L1.1	Semester Orientation: Theory	Power point presentation, Chalk & Board	7/10/2017		
2		L1.2	Semester Orientation: OBE	Power point presentation, Chalk & Board	7/11/2017		
3		L1.3	Semester Orientation: Theory	Power point presentation, Chalk & Board	7/12/2017		
4	Module 1	L1.4	Security Attacks, Security Goals, Computer Criminals	Power point presentation, Chalk & Board	7/12/2017	2.2	
5	Module 1	L2.1	Methods of defense, Security Services, Security Mechanisms	Power point presentation, Chalk & Board	7/17/2017	2.2	
6	Module 2	L2.2	Basics of Cryptography: Symmetric Cipher Model	Power point presentation, Chalk & Board & Flip Classroom	7/17/2017	1.3	
7	Module 2	L2.3	Substitution Techniques	Chalk & Board,	7/18/2017	1.3	
8	Module 2	L2.4	Transportation Techniques	Power point presentation, Chalk & Board	7/18/2017	1.3	
9	Module 2	L2.5	Other Cipher Properties- Confusion, Diffusion, Block and Stream Ciphers	Chalk & Board	7/20/2017	1.3	
10	Module 2	L3.1	**Secret Key Cryptography:** Data Encryption Standard(DES)	Power point presentation, Chalk & Board	7/25/2017	1.3	
11	Module 2	L3.2	Strength of DES	Chalk & Board, Animation	7/27/2017	1.3	

12	Module 2	L3.3	Block Cipher Design Principles and Modes of Operations	Chalk & Board, Animation	7/28/2017	1.3	
13	Module 2	L3.4	Triple DES, International Data Encryption algorithm	Power point presentation, Chalk & Board	7/28/2017	1.3	
14	Module 2	L4.1	Blowfish, CAST-128	Chalk & Board, Animation	8/1/2017	1.3	
15	Module 3	L4.2	Public Key Cryptography: Principles of Public Key Cryptosystems	Chalk & Board, Animation	8/2/2017	1.3	
16	Module 3	L4.3	RSA Algorithm, DiffieHellman Key Exchange	Chalk & Board, Animation & Flip Classroom	8/4/2017	1.3	
17	Module 3	L4.4	**Cryptographic Hash Functions:** Applications	Chalk & Board, Animation	8/4/2017	1.3	
18	Module 3	L5.1	Secure Hash Algorithm, Message Authentication Codes	Power point presentation, Chalk & Board	8/8/2017	1.3	
19	Module 3	L5.2	Message Authentication Requirements and Functions	Chalk & Board, Animation	8/10/2017	1.3	
20	Module 3	L5.3	HMAC, Digital signatures, Digital Signature Schemes	Chalk & Board, Animation	8/11/2017	1.3	
21	Module 3	L5.4	Authentication Protocols, Digital Signature Standards	Chalk & Board, Animation	8/11/2017	1.3	
22	Module 4	L6.1	Authentication Applications: Kerberos	Chalk & Board, Animation	8/18/2017	1.3	
23	Module 4	L6.2	Key Management and Distribution	Power point presentation, Chalk & Board	8/18/2017	1.3	
24	Module 4	L7.1	X.509 Directory, Authentication service,	Chalk & Board, Animation	8/24/2017	1.3	
25	Module 4	L8.1	Public Key Infrastructure	Chalk & Board, Animation	8/31/2017	1.3	
26	Module 4	L8.2	Electronic Mail Security: Pretty Good Privacy, S/MIME	Chalk & Board	9/1/2017	1.3	
27	Module 5	L8.3	**Program Security, Operating System Security, Database Security, IDS and Firewalls:** Secure programs	Chalk & Board	9/1/2017	2.2	
28	Module 5	L9.1	Non-malicious Program Errors, Malicious Software– Types, Viruses	Chalk & Board	9/5/2017	2.2	
29	Module 5	L9.2	Virus Countermeasures, Worms, Targeted Malicious Code, Controls against Program Threats	Chalk & Board,	9/7/2017	2.2	

30	Module 5	L9.3	Memory and Address protection, File Protection Mechanism,User Authentication	Power point presentation, Chalk & Board	9/8/2017	2.2	
31	Module 5	L9.4	Security Requirement, Reliability and Integrity	Chalk & Board,	9/8/2017	2.2	
32	Module 5	L10.1	Sensitive data, Inference, Multilevel Databases Intruders	Chalk & Board, Animation	9/12/2017	2.2	
33	Module 5	L10.2	Intrusion Detection, Password Management	Power point presentation, Chalk & Board	9/14/2017	2.2	
34	Module 5	L10.3	Firewalls-Characteristics, Types of Firewalls	Chalk & Board, Animation	9/15/2017	2.2	
35	Module 5	L10.4	Placement of Firewalls, Firewall Configuration, Trusted systems	Power point presentation, Chalk & Board	9/15/2017	2.2	
36	Module 6	L11.1	**IP Security** Overview, Architecture, Authentication Header	Power point presentation, Chalk & Board	9/19/2017	2.2	
37	Module 6	L11.2	Encapsulating Security Payload, Combining security Associations, Internet Key Exchange	Chalk & Board, Animation	9/21/2017	2.2	
38	Module 6	L11.3	Web Security: Web Security Considerations,	Chalk & Board, Animation	9/22/2017	2.2	
39	Module 6	L11.4	Secure Sockets Layer and Transport Layer Security, Electronic Payment	Power point presentation, Chalk & Board	9/22/2017	2.2	
40	Module 6	L12.1	Non-cryptographic protocol Vulnerabilities, DoS, DDoS, Session Hijacking and Spoofing,	Chalk & Board, Animation	9/26/2017	2.2	
41	Module 6	L13.1	Software Vulnerabilities-Phishing, Buffer Overflow,	Chalk & Board, Animation	10/3/2017	2.2	
42	Module 6	L13.2	Format String Attacks, SQL Injection.	Chalk & Board, Animation	10/5/2017	2.2	
43		L13.3	Revision	Chalk & Board, Animation	10/6/2017		
44		L13.4	Revision	Chalk & Board, Animation	10/6/2017		
45		L 14.1	University Paper Discussion	Chalk & Board, Animation	10/12/2017		
46		L14.2	University Paper Discussion	Chalk & Board, Animation	10/13/2017		
Remark: Course:		Syllabus Coverage:		Practice Session: 2		**Content Beyond Syllabus:** Introduction to Web Security & its attacks, Real time Attacks & Cyber crime	
No. of (lectures planned)/(lecture taken): 50							
Advanced course: Digital Forensics				20 Hours	Online NPTEL videos with Hands on Training in Laboratory	**Web sources:** 1. NPTEL-https://onlinecourses.nptel.ac.in 2. www.tutorialpoint.com1. Instructor's study material, **Textbook reference:** 1. Kevin Mandia, Chris Prosise, "Incident Response and computer forensics", Tata McGrawHill, 2006	

Text Books:

1.1. Cryptography and Network Security: Principles and Practice 5th edition, William Stallings, Pearson. 1.2. Network Security and Cryptography 2nd edition, Bernard Menezes, Cengage Learning. 1.3. Cryptography and Network, 2nd edition, Behrouz A Fourouzan, Debdeep Mukhopadhyay, TMH

Reference Books:

2.1 Cryptography and Network Security by Behrouz A. Forouzan, TMH 2.2. Security in Computing by Charles P. Pfleeger, Pearson Education. 2.3. Computer Security Art and Science by Matt Bishop, Addison-Wesley.

Digital Reference:

3.1 www.nptel.ac.in

3.2 www.tutorialpoint.com

Sd/-

Ms. Vidyadhari Singh	Sd/-	Sd/-
Name & Signature of Faculty	Signature of HOD	Signature of Principal /Dean (Academics)
Date:	Date:	Date:

Note:

1. Plan date and completion date should be in compliance
2. Courses are required to be taught with emphasis on resource book, course file, text books, reference books, digital references etc.
3. Planning is to be done for 15 weeks where 1st week will be AOP, 2nd -13th for effective teaching and 14th -15th week for effective university examination oriented teaching, mock practice session and semester consolidation.
4. According to university syllabus where lecture of 4 hrs/per week is mentioned minimum 55 hrs and in case of 3 lectures per week minimum 45 lectures are to be engaged are required to be engaged during the semester and therefore accordingly semester planning for delivery of theory lectures shall be planned.
5. In order to improve score in NBA, faculty members are also required to focus course teaching beyond university prescribed syllabus and measuring the outcomes w.r.t learning course and programme objectives.
6. Text books and reference books are available in syllabus. Here only additional references w.r.t. non –digital/ digital sources can be written (if applicable)
7. Technology to be used in class room during lecture shall be written below the topic planned within the bracket.