MANIPAL INSTITUTE OF TECHNOLOGY

(A constituent college of Manipal University, Manipal)
Manipal Karnataka 576 104

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE PLAN

Department : **Computer Science & Engineering**

Subject Name and Code : **Cryptography & Network Security (CSE -324)**

Semester & branch : **VI SEM, CSE**

Name of the faculty : **Dr. PREMA K.V. and MANOJ R.**

No of contact hours/week : **4**

Assignment portion	
Assignment no.	**Topics**
1	**L1-L7**
2	**L8-L15**
3	**L16-L22**
4	**L23-L31**
5	**L32-L42**
Test portion	
Test no.	**Topics**
1	**L1-L19**
2	**L20-L42**

Submitted by: Dr. Prema K.V.

(Signature of the faculty)
Date:09/01/2015

Approved by:

(Signature of HOD)
Date:

MIT/GEN/F-05/R0

Lecture no.	Topics to be covered
1	INTRODUCTION: Security Trends, The OSI Security Architecture, Security Attacks.
2	Security Services, Security Mechanisms, A Model for Network Security.
3	CLASSICAL ENCRYPTION TECHNIQUES: Symmetric Cipher Model.
4	Substitution Techniques.
5	Transposition Techniques. BLOCK CIPHERS: Block Cipher Principles.
6	Data Encryption Standard (DES), DES encryption and decryption
7	A DES Example, the Strength of DES.
8	Differential and Linear Cryptanalysis.
9	ADVANCED ENCRYPTION STANDARD (AES): AES Structure.
10	AES Round Functions, AES Key Expansion.
11	An AES Example.
12	Multiple Encryption and Triple DES.
13	BLOCK CIPHER MODES OF OPERATION: Electronic Codebook Mode.
14	Cipher Block Chaining Mode. Cipher Feedback Mode.
15	Output Feedback Mode, Counter Mode.
16	PSEUDORANDOM NUMBER GENERATION: Principles of Pseudorandom Number Generation.
17	Pseudorandom Number Generators.

18	Stream Ciphers.
19	RC4.
20	INTRODUCTION TO NUMBER THEORY: Prime Numbers, Fermat's and Euler's Theorems.
21	Testing for Primality.
22	The Chinese Remainder Theorem, Discrete Logarithms.
23	PUBLIC-KEY CRYPTOGRAPHY (PKC): Principles of PKC, The RSA Algorithm, The security of RSA.
24	Diffie-Hellman Key Exchange Algorithm.
25	CRYPTOGRAPHIC HASH FUNCTIONS: Applications of cryptographic hash Functions.
26	Two simple hash functions, requirements and security.
27	Hash Functions based on Cipher Block Chaining.
28	SHA-512, SHA-3.
29	MESSAGE AUTHENTICATION CODES: Message authentication requirements, message authentication functions.
30	Message authentication codes
31	HMAC
32	DIGITAL SIGNATURES: Digital Signature Standard (DSS), Digital Signature Algorithm (DSA).
33	TRANSPORT LEVEL SECURITY: Web Security Issues.
34	Secure Socket Layer (SSL).
35	Transport Layer Security.
36	ELECTRONIC MAIL SECURITY: Pretty Good Privacy (PGP): PGP services, PGP cryptographic functions.
37	PGP message compression.

38	S/MIME.
39	IP SECURITY (IPSec): IPSec Overview and policy.
40	Authentication Header.
41	Encapsulating Security Payload, Combining Security Associations.
42	Internet Key Exchange.
43	SYSTEM SECURITY: Intruders.
44	Intrusion Detection.
45	Password management.
46	MALICIOUS SOFTWARE: Types: Viruses.
47	Virus Counter measures, Worms.
48	FIREWALLS: Firewall Characteristics and Types of Firewalls.

Text Book:

1. William Stallings - Cryptography and Network Security: Principles and Practice, Prentice Hall, 5th edition, 2010.

Reference Book:

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay - Cryptography and Network Security, McGraw Hill, 2nd Edition, 2008.