SCHEME OF COURSE WORK
Department of Information Technology

Course Details:

COURSE TITLE	**INFORMATION SECURITY**		
COURSE CODE	**13IT1105**	**L T P C**	**4 1 0 3**
PROGRAM	**B.TECH**		
SPECIALIZATION	**INFORMATION TECHNOLOGY**		
SEMESTER	**VII**		
PRE REQUISITES	**COMPUTER NETWORKS,BASIC MATHEMATICS**		
COURSES TO WHICH IT IS A PRE REQUISITE	**NETWORK SECURITY AND CRYPTOGRAPHY**		

Course Outcomes (COs):

1	Discuss Security Architecture.
2	Explain different Public-Key Cryptography Algorithms and Hash Functions.
3	Discuss key management, distribution and authentication techniques.
4	Analyze transport level security and electronic mail security.
5	Discuss Security at IP layer.

Program Outcomes (POs):

A graduate of mechanical engineering will be able to

1	Ability to plan and execute software project modules, testing and delivery mechanisms.
2	Ability to use industry ready modern technologies through advanced data structures, expertise in web technologies.
3	Ability to think critically on the software related issues to provide viable solutions.
4	Ability to solve software related problems effectively and efficiently.
5	Ability to conduct research on up-coming fields of software development and to innovate into new Directions.
6	Ability to manage a software team and to maintain financial records as per standards.
7	Ability to effectively communicate with clients, peers and society at large.
8	Ability to take up lifelong learning to be in tune with the new software related technologies.
9	Ability to follow ethical practices in the software industry and accept social responsibility.
10	Ability to learn independently from mistakes and surge forwards with positive attitude.

Course Outcome versus **Program Outcomes:**

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	M	M		S	S		M	M				
CO2		M			S			M				
CO3			S	M	M							
CO4		S			S							
CO5	M				S							

S - Strongly correlated, *M - Moderately* correlated, *Blank - No correlation*

Assessment Methods	Assignment / Quiz / Mid-Test / End Exam

Teaching- Learning & Evaluation

Week	Topic/ Contents	Course Outcomes	Sample questions	Teaching learning strategy	Assessment method & schedule
1	OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A model for Internetwork security	CO-1	1. What are various security services offered by the system. 2. Write about various types of security attacks possible in a computer system	□ □ Lecture □ □Discussion	Assignment-1 (Week 1 - 8) Mid-Test 1 Quiz-1 (Week-9)
2	Classical Encryption Techniques, Block Cipher Principles	CO-1	1. What is difference between stream cipher and block cipher?	□ □ Lecture □ □ Discussion	Assignment-1 Mid-Test 1 Quiz-1 (Week 9)
3	Advanced Encryption Standard, Stream Ciphers, RC4	CO-1	1. With a neat diagram explain simple DES scheme of encryption and decryption.	□ □ Lecture □ □ Discussion	Assignment-1 (Week 1 - 8) Mid-Test 1 Quiz-1 (Week-9)
4	Public-Key Cryptography and RSA	CO-2	1. Explain about cipher block modes of operation in detail. 2.What are key pairs in Diffie-Hellman key exchange algorithm.	□ □ Lecture □ □ Discussion	Assignment-1 (Week 1 - 8) Mid-Test 1 Quiz-1 (Week9)
5	Cryptographic Hash Functions, Message Authentication Codes	CO-2	1. Define secure hash function with an example.	□ □ Lecture □ □ Discussion	Assignment-1 (Week 1 - 8) Mid-Test 1 Quiz-1 (Week9)
6	Security of MACs, MACs Based on Hash Functions	CO-2	1. Define MAC. 2. Types of MAC algorithms.	□ □ Lecture □ □ Discussion	Assignment-1 (Week 1 - 8) Mid-Test 1 Quiz-1 (Week9)
7	Digital Signature Standard	CO-2	1. What is a digital signature?	□ □ Lecture □ □ Discussion	Assignment-1 (Week 1 - 8) Mid-Test 1 Quiz-1 (Week9)
8	Key Management and Distribution	CO-3	1. Explain about key distribution technique.	□□ Lecture □ □ Discussion	Assignment-1 (Week 1 - 8) Mid-Test 1 Quiz-1 (Week9)
9	Mid Test 1				
10	Symmetric Key Distribution using Asymmetric Encryption	CO-3	1.What are the types of authentication in X.509	□ □ Lecture □ □ Discussion	Assignment 1 (Week 1 - 8) Mid-Test 1 Quiz-1 (Week9)

11	Distribution of Public Keys, X.509 Certificates, Kerberos	CO-3	1.Write in detail about X.509 certificate authority 2.In Kerberos how are services exchanged between two realms	□ □ Lecture □ □ Discussion	Assignment -2 (Week10- 17) Mid-Test 2 Quiz-2 (Week 18)
12	Transport-Level Security: Web Security Issues.	CO-4	1.Write in detail about transport layer security	□ □ Lecture □ □ Discussion	Assignment -2 (Week10- 17) Mid-Test 2 Quiz-2 (Week 18)
13	Secure Sockets Layer (SSL), Transport Layer Security (TLS),	CO-4	1. What is alert protocol in SSL? Explain. 2.How is dual signature used in SSL	□ □ Lecture □ □ Discussion	Assignment -2 (Week10- 17) Mid-Test 2 Quiz-2 (Week 18)
14	HTTPS Electronic Mail Security: Pretty Good Privacy, S/MIME	CO-4	1.Mention content types of S/MIME.	□ □ Lecture □ □ Discussion	Assignment -2 (Week10- 17) Mid-Test 2 Quiz-2 (Week 18)
15	IP Security :IP Security Overview, IP Security Policy	CO-5	1. Mention the various services offered by IP Security.	□ □ Lecture □ □ Discussion	Assignment -2 (Week10- 17) Mid-Test 2 Quiz-2 (Week 18)
16	Encapsulating Security Payload, Combining Security Associations	CO-5	1. What is ESP? 2. With a neat diagram explain protocol context of SNMP.	□ □ Lecture □ □ Discussion	Assignment -2 (Week10- 17) Mid-Test 2 Quiz-2 (Week 18)
17	Internet Key Exchange, Intruders, Malicious Software, Firewalls	CO-5	1. Write short notes on a) Firewall b) Intruder.	□ □ Lecture □ □ Discussion	Assignment 2 (Week10- 17) Mid-Test 2 Quiz-2 (Week 18)
18	Mid-Test 2				
19/20	END EXAM				