SRM UNIVERSITY
FACULTY OF ENGINEERING AND TECHNOLOGY

SCHOOL OF COMPUTING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
COURSE PLAN

Course Code : 15CS434E
Course Title : Network Security
Semester : V
Course Duration : July 2017 – November 2017

Day		
	Hour	Timing
Day 1		
Day 2		
Day 3	8	2.20 - 3.10
Day 4		
Day 5	6,7	12.30 – 2.15

Location : Tech Park

Faculty Details

Section	Name	Office	Office hour	Mail id
1	Dr. A. Jeyasekar	Tech Park	8.45AM -4.00PM	Jeyasekar.a@ktr.srmuniv.ac.in
2	G.K. Sandhia			Sandhia.g@ktr.srmuniv.ac.in

Required Text Books:

1. Williams Stallings "Cryptography and Network Security – Principles and Practice", Sixth Edition, Pearson Publication, 2016
2. Bernard Menezes "Network Security and Cryptography", Cengage Learning, Third Impression 2014
3. Atul Kahate "Cryptography and Network Security", Tata McGraw Hill Publication Company Limited, 2006
4. Charlie Kaufman et al "Network Security – Private Communication in a Public World", Second Edition, PHI Learning Private Limited, 2011
5. Charles P. Pfleeger et al "Security in Computing ", Third Edition, Pearson Education, 2004

Prerequisite : Nil

Objectives

To understand the various types services i.e. Confidentiality, Authentication, Data Integrity, Non-Repudation and Access control and the mechanisms used to mitigate the security risks

Assessment Details

Attendance	:	5 Marks
Cycle Test – I	:	15 Marks
Surprise Test – I	:	5 Marks
Model Exam	:	25 Marks
Total	**:**	**50 Marks**

Test Schedule

S.No.	DATE	TEST	DURATION
1	As per Calander	Cycle Test - I	2 periods
2	As per Calander	Model Exam	3 Hrs

Outcomes

Students who have successfully completed this course will have full understanding of the following concepts

Course outcome	Program outcome
To understand the application of mathematics in cryptography	Ability to understand the application of mathematics in cryptography
To learn different types of security system used traditionally and its general format	Ability to understand the mechanism used in the classical encryption system and different type of block cipher mode of operation
To understand encrypt/decrypt a message using Secret Key and Public Key Cryptography	Ability to encrypt/decrypt a message using Secret Key and Public Key Cryptography
To understand the various types of authentication algorithm	Ability to understand the various types of authentication algorithm
To understand the security measure taken over internet	Ability to Understand the security measure taken over Internet security
To understand the various types of vulnerabilities and detection system	Ability to understand the various types of vulnerabilities and detection system

Detailed Session Plan

Session No.	Topics to be covered	Time (min)	Ref	Teaching Method	Testing Method
UNIT I: SECRET KEY CRYPTOGRAPHY					
1	Introduction to network security, Classical Encryption Techniques,	50	1	BB	Open Discussion and Quiz
2	SDES	50	1	BB	Objective type test

					Quiz
3	SDES	50	1	BB	Quiz
4	Block Cipher and Data Encryption Standard (DES)	50	1	BB	Quiz
5	Block Cipher and Data Encryption Standard (DES)	50	1	BB	Quiz
6	Block Cipher and Data Encryption Standard (DES)	50	1	BB	Quiz Objective type test
7	Attack, Linear Cryptanalysis	50	2	BB	Quiz, Assignment
8	Block Cipher Operation	50	1	BB	Group discussion Comparative study
9	AES	50	1	BB	Group discussion Comparative study
UNIT II: PUBLIC KEY CRYPTOGRAPHY					
10	Mathematical Background for Cryptography	50	2	BB	Quiz
11	Mathematical Background for Cryptography	50	2	BB	Quiz Brain storming
12	Mathematical Background for Cryptography	50	2	BB	Quiz Surprise Test
13	Fermat's and Euler's Theorems, Testing for Primality	50	1	BB	Group discussion Quiz
14	Public Key Cryptography and RSA	50	2	BB	Group discussion, Quiz
15	Public Key Cryptography and RSA	50	2	BB	Quiz, Assignment
16	Discrete Logarithm and its application	50	2	BB	Quiz Group discussion Objective type test
17	Elliptic Curve Cryptography	50	2	BB	Quiz Group discussion
18	Elliptic Curve Cryptography	50	2	BB	Quiz, Comparative study
UNIT III: AUTHENTICATION					
19	Cryptographic Hash	50	2	BB	Quiz Surprise Test
20	Key Management	50	2	BB	Quiz Group discussion
21	Key Management	50	2	BB	Quiz Comparative study
22	Authentication – I	50	2	BB	Quiz Group discussion
23	Authentication – I	50	2	BB	Quiz
24	Authentication - II	50	2	BB	Quiz Brain storming
25	Authentication -II	50	2	BB	Quiz Brain storming
26	Secure Hash Algorithm (SHA)	50	1	BB	Group discussion Assignment
27	Secure Hash Algorithm (SHA)	50	1	BB	Group discussion Quiz

UNIT IV: INTERNET SECURITY					
28	IP Security	50	2	BB	Group discussion Assignment
29	IP Security	50	2	BB	Group discussion Assignment
30	Transport Layer Security	50	2	BB	Objective type test
31	Wireless LAN Security	50	2	BB	Quiz Group discussion Comparative study
32	Wireless LAN Security	50	2	BB	Objective type test
33	Cell Phone Security	50	2	BB	Objective type test
34	Web Service Security	50		BB	Quiz Group discussion
35	Web Service Security	50	2	BB	Objective type test
36	Web Service Security	50	2	BB	Group discussion
UNIT V: Vulnerability and Intrusion Detection System					
37	Non-Cryptographic Protocol Vulnerabilities	50	2	BB	Comparative study
38	Non-Cryptographic Protocol Vulnerabilities	50	2	BB	Comparative study
39	Software Vulnerabilities	50	2	BB	Brain storming
40	Software Vulnerabilities	50	2	BB	Brain storming
41	Virus, Worms and other Malwares	50	2	BB	Group discussion
42	Virus, Worms and other Malwares	50	2	BB	Assignment
43	Firewall	50	2	BB	Group Discussion and Assignment
44	Intrusion Prevention and Detection	50	1	BB	Group Discussion and Assignment
45	Intrusion Prevention and Detection	50	1	BB	Group Discussion and Assignment

Signature of the Course Coordinator
(Dr. A. Jeyasekar)

Signature of the HOD/CSE
(Dr. B. Amutha)