		Theory Hrs	Practical Hrs	Tutorial Hrs	Theory Credit	Practical/Oral Credit	Tutorial Credits	Total Credits
CAL601	**Cryptography and Network Security Lab**	**-**	02	-	-	01	**-**	01

Subject Code	**Subject Name**	**Examination Scheme**								
		Theory Marks					**Term Work**	**Practical & Oral**	**Oral**	**Total**
		In-Sem Evaluations				**End Sem Exam**				
		IA1	**IA2**	**Avg. IA**	**Mid Sem Exam**					
CAL601	**Cryptography and Network Security Lab**	--	--	--	--	--	25	--	25	50

Course Objectives:

1. To make familiarize with classical encryption techniques.
2. To explore the working principles and utilities of various cryptographic algorithms.
3. To understand cryptographic utilities to build programs for secure communication.

Course Outcomes: At the end of the course learner will able to

1. Implement simple ciphers by applying the knowledge of symmetric cryptography.
2. Analyze and implement public key cryptosystem and Digital signature scheme.
3. Appraise and implement various key exchange and hashing algorithms.
4. Explore the different network reconnaissance tools like sniffers, port scanners etc. to gather network related information.
5. Use open source technologies for transport layer security and set up firewalls.
6. Explore various network attacks.

Prerequisites:

1. Engineering Mathematics
2. Computer Networks

Suggested List of Experiments

Sr. No.	Detailed Content	CO Mapping
1	Design and implement any product cipher.	CO1
2	Implement and perform analysis of RSA public key cryptosystem.	CO2
3	Implement RSA Digital signature scheme.	CO2
4	Implement Diffie Hellman Key exchange algorithm	CO3
5	Implement a program to test integrity of message using MD-5, SHA-1 and use crypt APIs.	CO3
6	Study and use network reconnaissance tools like WHOIS, dig, traceroute, nslookup, nmap to gather information about networks and domain registrars.	CO4
7	Install packet sniffer tool (e.g. Wireshark) to capture packets and apply different filters.	CO5
8	Detect ARP spoofing using ARPWATCH and Wireshark.	CO5
9	Simulate DOS attack using Hping3 and Wireshark.	CO5
10	Setting up personal Firewall using iptables	CO5
11	Set up IPSEC under LINUX.	CO5
12	Simulate buffer overflow attack using Splint, Cppcheck.	CO6

Text Books:

1. Behrouz A. Ferouzan, ―Cryptography & Network Security‖, Tata Mc Graw Hill
2. William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013
3. Bernard Menezes, ―Cryptography & Network Security‖, Cengage Learning.
4. Network Security Bible, Eric Cole, Second Edition, Wiley.

Reference Books:

1. Applied Cryptography, Protocols Algorithms and Source Code in C, Bruce Schneier, Wiley.
2. Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.

Term Work:

The Term work Marks are based on the weekly experimental performance of the students, Oral performance and regularity in the lab. Students are expected to be prepared for the lab ahead of time by referring the manual and perform the experiment under the guidance and discussion. Next week the experiment write-up to be corrected along with oral examination.

End Semester Examination: End of the semester, there will be oral evaluation based on the laboratory work and the corresponding theory syllabus.