Lab Code	Lab Name	Credit
CSL602	Cryptography & System Security Lab	**1**

Prerequisite: Computer Network	
Lab Objectives:	
1	To apply various encryption techniques
2	To study and implement various security mechanism
3	To explore the network security concept and tools
Lab Outcomes: At the end of the course, the students will be able to	
1	To be able to apply the knowledge of symmetric and asymmetric cryptography to implement simple ciphers.
2	To explore the different network reconnaissance tools to gather information about networks.
3	To explore and use tools like sniffers, port scanners and other related tools for analysing packets in a Network.
4	To be able to set up firewalls and intrusion detection systems using open-source technologies and to explore email security.
5	To be able to explore various attacks like buffer-overflow and web application attack.

	Suggested List of Experiments
Sr. No	**Title of Experiment**
1	Design and Implementation of a product cipher using Substitution and Transposition ciphers.
2	Implementation and analysis of RSA crypto system.
3	Implementation of Diffie Hellman Key exchange algorithm
4	For varying message sizes, test integrity of message using MD-5, SHA-1, and analyse the performance of the two protocols. Use crypt APIs.
5	Study the use of network reconnaissance tools like WHOIS, dig, traceroute, ns lookup to gather information about networks and domain registrars.

6	Study of packet sniffer tools : wireshark, : 1. Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode. 2. Explore how the packets can be traced based on different filters.
7	Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc.
8	Detect ARP spoofing using nmap and/or open-source tool ARPWATCH and wireshark. Use arping tool to generate gratuitous arps and monitor using wireshark
9	Simulate DOS attack using Hping, hping3 and other tools
10	Simulate buffer overflow attack using Ollydbg, Splint, Cpp check etc
11	a. Set up IPSEC under LINUX. b. Set up Snort and study the logs.
12	Setting up personal Firewall using iptables
13	Explore the GPG tool of linux to implement email security
14	SQL injection attack, Cross-Cite Scripting attack simulation
15	Case Study /Seminar: Topic beyond syllabus related to topics covered. Or Two Written Assignments

Term Work:	
1	Term work should consist of 10 experiments.
2	Journal must include at least 2 assignments on content of theory and practical of "Cryptography and System Security "
3	The final certification and acceptance of term work ensures that satisfactory performance of laboratory work and minimum passing marks in term work.
4	The distribution of marks for term work shall be as follows: Lab Performance 15 Marks Assignments/Case study 05 Marks Attendance (Theory & practical) 05 Marks