CRYPTOGRAPHY AND SECURITY LAB

Course code: 13CS2208 **L P C**
0 3 2

Pre requisites: Network security and Cryptography, CPC.

Course Educational Objectives:
The objective of this course is that to understand the principles of encryption algorithms, conventional and public key cryptography practically with real time applications.

Course Outcomes:
By the end of the course students will

1. Know the methods of conventional encryption.
2. Understand the concepts of public key encryption and number theory
3. Understand various applications of cryptography and security issues practically.

The following programs should be implemented preferably on platform Windows/Unix using C
language (for 1-5) and other standard utilities available with UNIX systems (for 6-15) :-

1. Implement the encryption and decryption of 8-bit data using Simplified DES Algorithm (created by Prof. Edward Schaefer) in C
2. Write a program to break the above DES coding
3. Implement Linear Congruential Algorithm to generate 5 pseudo-random numbers in C
4. Implement Rabin-Miller Primality Testing Algorithm in C
5. Implement the Euclid Algorithm to generate the GCD of an array of 10 integers in C
6. a)Implement RSA algorithm for encryption and decryption in C
   b) In an RSA System, the public key of a given user is e=31,n=3599. Write a program to find private key of the User.
7. Configure a mail agent to support Digital Certificates, send a mail and verify the correctness of this system using the configured parameters.

8. Configure SSH (Secure Shell) and send/receive a file on this connection to verify the correctness of this system using the configured parameters.
9. Configure a firewall to block the following for 5 minutes and verify the correctness of this system using the configured parameters:
    (a) Two neighborhood IP addresses on your LAN
    (b) All ICMP requests
    (c) All TCP SYN Packets
10. Configure S/MIME and show email-authentication.
11. Implement encryption and decryption with openssl.
12. Implement Using IP TABLES on Linux and setting the filtering rules.
13. Implementation of proxy based security protocols in C or C++ with features like Confidentiality, integrity and authentication.
14. Working with Sniffers for monitoring network communication (Ethereal)
15. Using IP TABLES on Linux and setting the filtering rules