NETWORK SECURITY AND CASE TOOLS LAB

Course Code: 13CS1109

L	T	P	C
0	0	3	2

Course Educational Objective:

To understand the principles of encryption algorithms; conventional and public key cryptography practically.

Course Outcomes:

- To know the methods of conventional encryption.
- To understand the concepts of public key encryption and number theory
- Student will be capable of representing a program, module even a system in the form of diagrams. Student will also get the knowledge of developing background code along with the drawing of diagrams.

PART -A

1. Implement Linear Congruential Algorithm to generate 5 pseudorandom Numbers,BBS algorithm to generate pseudo random numbers
2. Implement Caesar cipher encryption and decryption
3. Implement Hill cipher encryption
4. Implemnet play fair cipher encryption
5. Implemnt fast modular exponentiation algorithm.
6. Implement Rabin-Miller Primality Testing Algorithm.

7 Implement the Euclid Algorithm to generate the GCD of an array of 10 integers.

8. Implement Extended Euclid Algorithm to find multiplicative inverse of a number
9. Implement the encryption and decryption of 8-bit data using Simplified DES Algorithm (created by Prof. Edward Schaefer).

10. Implement RSA algorithm for encryption and decryption.
11. Implement Diffie-Hellman Key Exchange Algorithm.
12. Implement CRT (Chinese Remainder Theorem).

PART-B

1. The student should take up the case study of Unified Library application which is mentioned in the theory, and Model it in different views i.e Use case view, logical view, component view, Deployment view, Database design, forward and Reverse Engineering, and Generation of documentation of the project.
2. Student has to take up another case study of his/her own interest and do the same what ever mentioned in first problem. Some of the ideas regarding case studies are given in reference books which were mentioned in theory syllabus can be referred for some idea.

   Note : The analysis, design, coding, documentation, database design of mini project which will be carried out in 4th year should be done in object-oriented approach using UML and by using appropriate software which supports UML, otherwise the mini project will not be evaluated.
3. Take an example subnet of hosts. Obtain broadcast tree for it