NETWORK SECURITY AND CRYPTOGRAPHY LAB

COURSE CODE: 15CS1108

L	T	P	C
0	0	3	2

COURSE OUTCOMES:
At the end of the course the student shall be able to

CO1: Apply methods of conventional encryption.

CO2: Solve the problem of public key encryption using number theory.

CO3: Develop Key-Exchange Algorithms

CO4: Implement authentication protocol

CO5: Verify network security protocol

LIST OF EXPERIMENTS:

1. Implement Caesar cipher encryption and decryption
2. Implement Hill cipher encryption
3. Implement play fair cipher encryption
4. Implement fast modular exponentiation algorithm.
5. Implement Rabin-Miller Primality Testing Algorithm.
6. Implement the Euclid Algorithm to generate the GCD of an array of 10 integers.
7. Implement Extended Euclid Algorithm to find multiplicative inverse of a number
8. Implement the encryption and decryption of 8-bit data using Simplified DES Algorithm (created by Prof. Edward Schaefer).
9. Implement RSA algorithm for encryption and decryption.
10. Implement Diffie-Hellman Key Exchange Algorithm.
11. Implement CRT (Chinese Remainder Theorem).
12. Configure a mail agent to support Digital Certificates, send a mail and verify the correctness of this system using the configured parameters.