Detailed syllabus

Cycle 1 : Number theory and Cryptographic experiments -

1) Installation of GMP library
2) Euclidean algorithm for computing the GCD of two integers
3) Extended Euclidean algorithm
4) Modular Arithmetic over Zn
5) Polynomial Arithmetic over GF(2^n)
6) Substitution Technique
7) DES
8) AES
9) Chinese Remainder Theorem
10) RSA
11) Diffie-Hellman Key Exchange
12) Elgamal Cryptographic System
13) Elliptic curve cryptography
14) Elgamal and DSS Digital signature scheme

Cycle 2 : Network Security experiments

1. Design and Implement a protocol with the details as given below
    a. User A likes to allow to read his encrypted messages by User B without revealing his private key
    b. User A generates a new key pair which is shared between User B and Proxy
    c. User A delegates a proxy to reencrypt /partial decrypt the encrypted message of User A using new key in the key pair
    d. Proxy sends the modified encrypted message to UserB
    e. User B decrypts the encrypted message using new key in the key pair

Use key exchange algorithm between User A and Proxy, User A and User B

Encryption and decryption can be using any PKC

2 A network in which the nodes are logically connected using tree structure, a layered encryption and decryption is followed in the protocol. Design and code the protocol with the following details

1. The nodes are divided into left sub tree and right sub tree
2. Among the nodes in the same level one is elected as leader on both left and right subtree separately.
3. There is only one key is allotted at each level
4. The key is shared among all nodes in the same level
5. When the document is to be encrypted the leader collects the shares from other nodes and encryption is done by the leader
6. The encrypted document travels from lower level to upper level through leader in left sub tree and encrypted at each level
7. When the document reaches root it travels from higher level to lower level

8. Each level the key for decryption is collected by leader from the nodes in the same level
9. Decryption is done at each level and reaches a destination.

3. A network in which each node can act as a client or server for the other computers in the network, allowing shared access to various resources such as files, peripherals, etc without the need for a central server.

- Design and code security association/agreement between server and client b.
- Procedure for key management c.
- Design and code for authentication between server and client vice versa

4. Design and implement a communication system with the following details

- The users are divided logically into groups.
- Each user can have many public and private key pairs.
- Each users maintains a table in which public key is stored.
- Each user maintains private keys in another table along with the id of the public key which is in encrypted form.
- The encryption and decryption is based on the public key id sent along with the cipher text. Use any public key cryptography for encryption and decryption

5. Design and implement secure communication between two groups A and B:

- A server is connected to n number of registered users.
- The users are divided into two groups such as A and B.
- Members can be added and removed dynamically.
- The communication is between two group leaders (Assume the leaders are already elected).
- Each group leader authenticates his members by using any authentication technique before any communication happens.
- The server generates a common (public key, private key) for each group and divides the private key into shares and dispatches to the users of respective groups.
- A user from group A can communicate to group B user through the leader and vice versa.
- The encryption and decryption is using key par (public key, private key), which is the common practice.

6. Implement PGP email security - The design is available in the text book

7.Implement Kerberos version 4 authentication protocol between server and the client - The design is available in the text book