IT9404 **SECURITY LABORATORY** L T P C
0 0 3 2

AIM:

To understand and implement the various security algorithms.

OBJECTIVE:

To enable students to implement security for operating systems and databases.

EXPERIMENTS:

1. Write programs to implement the following **number theory** concept

- Prime and Relatively Prime Numbers
- Arithmetic Modulo 8 and Multiplication Modulo 8
- Fermat's Theorem and Euler's Totient Function

2. Write programs to implement the following **cryptography algorithms**

- Playfair cipher and Hill cipher
- Simplified DES algorithm
- RSA algorithm

3. Write programs to implement the following **hash algorithms**

- MD5
- SHA-1

4. Write programs to implement the following **Authentication**

- Digital Signature and Digital Certificate
- Kerberos System
- X.509

5. Write programs to implement the following **Trusted OS** issues

- Write a program to implement a set of rules combining the secrecy controls of the Bell-La Padula with integrity controls of the Biba model.
- Write a program to implement UNIX operating system structure files by using a tree. Each file is at a leaf of the tree, and the unique path from the root of the leaf identifies the file. Each interior node is sub directory, which specifies the names of the paths leading form that node. A user can block access through a node by restricting access to the sub directory. Device a method that uses this structure to implement discretionary access policy.

6. Write a program to implement the following database security issues.

- Cryptography in databases.
- Access Control list.
- Two phase locking technique.

7. Write a program to implement Hacking windows.

- BIOS Passwords.
- Windows login password
- Internet explorer users
- Changing windows visuals
- Accessing restricted drives.

TOTAL= 45 PERIODS