NETWORK SECURITY AND DATA MINING LAB

Course code: 13CS2116 **L P C**
0 3 2

Prerequisites : DBMS, Network protocols.

Course Educational Objectives:
The objective of this course is that To understand the principles of encryption algorithms; conventional and public key cryptography practically and various data mining real time applications.

Course outcomes:
- To know the methods of conventional encryption.
- To understand the concepts of public key encryption and number theory
- To understand authentication
- The Student will gain the knowledge on various networks tools like Weka and Rosetta..
- Plan, design and deploy the necessary data mining technologies to support a software system.

The following programs should be implemented preferably on platform using C language (for 1-5) and other standard utilities available with UNIX systems (for 6-9) :-

Part A :
1. Implement the encryption anddecryption 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

Part –B:

1. Implementation of multi dimensional data model using oracle warehouse builder/SQL Server.
2. Introduction to Weka: All the features of Weka software will be explored in this assignment.
   Implementation of the following programs in C/C++:
3. Implementation of Apriori algorithm
4. Implementation of FP tree algorithm
5. Implementation of Naïve Bayesian classification algorithm
6. Introduction to ROSETTA: All the features of Rosetta software .
7. Generate lower and upper boundary values for a database using Rosetta.
8. Classify a database using Rosetta for an input excel database file.
9. Generate the decision rules and partition an input database using Rosetta.