IV Year B.Tech. CSE I - Semester	**L**	**T**	**P**	**To**	**C**
	-	-	3	3	2

CS449 CRYPTOGRAPHY AND NETWORK SECURITY LAB

Course Description & Objective:

After the success full completion of this course the student is enable towards learning and overcome security attacks in future.

Course Outcomes:

- Understand computer security principles and discuss ethical issues for theft of information. Identify threat models and common computer network security goals
- Explain various encryption algorithms, hashing functions, one-way authentication and public key cryptology
- Analyze firewalls, DOS attacks and defense types. Dramatize example scenarios in DNS and IPSec applications

Programming:

1. Write program for Ceaser cipher encryption and decryption
2. Write program for Mono alphabetic cipher encryption and decryption
3. Implementation of Play Fair cipher
4. Implementation of Vigenere cipher (Polyalphabetic substitution)
5. Implementation of Hill cipher
6. Implementation of Rail Fence cipher
7. Implementation of S-DES algorithm for data encryption
8. Implement RSA asymmetric (public key and private key)-Encryption
9. Implement Euclidean and Extended Euclidean algorithm for calculating the GCD
10. Working with PGP

Text Books:

1. Cryptography and Network security by William Stallings, Pearson Education, Fourth Edition

2. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education, Second Edition

Reference Books:

1. Fundamentals of Network Security by Eric Malwald (Dreamtech press)

2. Network Security – Private Communication in a Public World by Charlie Kaufman, Radis Perlman and Mike Speciner,Pearson Education

3. Introduction to Cryptography Buchmann, Springer

4. Problem solving with C++, The OOP, Fourth edition, W.Savitch, Pearson education.

5. C Programming with problem solving, J.A. Jones & K. Harrow, Dreamtech Press.