CS6711	**SECURITY LABORATORY**	**L T P C**
		0 0 3 2

OBJECTIVES:

The student should be made to:

- Be exposed to the different cipher techniques
- Learn to implement the algorithms DES, RSA,MD5,SHA-1
- Learn to use network security tools like GnuPG, KF sensor, Net Strumbler

LIST OF EXPERIMENTS:

1. Implement the following SUBSTITUTION & TRANSPOSITION TECHNIQUES concepts:
a) Caesar Cipher
b) Playfair Cipher
c) Hill Cipher
d) Vigenere Cipher
e) Rail fence – row & Column Transformation

2. Implement the following algorithms
a) DES
b) RSA Algorithm
c) Diffiee-Hellman
d) MD5
e) SHA-1

5 Implement the SIGNATURE SCHEME - Digital Signature Standard

6. Demonstrate how to provide secure data storage, secure data transmission and for creating Digital signatures (GnuPG).

7. Setup a honey pot and monitor the honey pot on network (KF Sensor)

8. Installation of root kits and study about the variety of options

9. Perform wireless audit on an access point or a router and decrypt WEP and WPA. (Net Stumbler)

10. Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w)

TOTAL: 45 PERIODS

OUTCOMES:
At the end of the course, the student should be able to

- Implement the cipher techniques
- Develop the various security algorithms
- Use different open source tools for network security and analysis

LIST OF EQUIPMENT FOR A BATCH OF 30 STUDENTS:

SOFTWARE:

C / C++ / Java or equivalent compiler
GnuPG, KF Sensor or Equivalent, Snort, Net Stumbler or Equivalent

HARDWARE:

Standalone desktops - 30 Nos.
(or)
Server supporting 30 terminals or more.