IV/IV B. TECH. FIRST SEMESTER
INFORMATION SECURITY LAB (Required)

Course Code: CS 7L3 **Credits: 2**
Lecture:-- **Internal assessment: 25 Marks**
Lab: 3period/week **Semester end examination: 50 Marks**

Prerequsite: Information Security

At the end of this course student will:

CO1) Implement the basic cryptographic algorithms to learn how to encrypt and decrypt the messages

CO2) Implement exchange of secret keys without sharing or third party intervention

CO3) Implement digital signatures for the purpose of authentication

CO4) Understand about phishing and find out how to phished popular bank sites in general.

Course Objectives:

1. Practical implementation based on the security applications using JAVA

Syllabus:

1. Write a JAVA program to implement the DES algorithm logic.
2. Write a Java program that contains functions, which accept a key and input text to be

   encrypted/decrypted. This program should use the key to encrypt/decrypt the input by using the

   triple Des algorithm. Make use of Java Cryptography package.
3. Write a JAVA program to implement the Blowfish algorithm logic.
4. Using Java cryptography, encrypt the text “Hello world” using Blowfish. Create your own key

   using Java keytool.
5. Write a Java program to implement RSA algorithm.
6. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider

the end user as one of the parties(Alice) and the JavaScript application as the other party(Bob)

7. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.

8. Calculate the message digest of a text using the MD5 algorithm in JAVA.

9. Explore the Java classes related to digital certificates.

10. Create a digital certificate of your own by using the Java key tool.

11. Write a Java program to encrypt users passwords before they are stored in a database table, and to retrieve them whenever they are to be brought back for verification..

12. Write a program in java, which performs a digital signature on a given text.

13. Study phishing in more detail. Find out which popular bank sites have been phished and how.