CSE 5161 INFORMATION SYSTEMS

LAB I

ADVANCED CRYPTOGRAPHY LAB

(PAT II OF IS LAB I)

[0 0 3 1]

LAB MANUAL

I Sem M.Tech (CSIS)

(2022)

DEPT. OF COMPUTER SCIENCE & ENGG.

M. I. T., MANIPAL

INSTRUCTIONS TO STUDENTS

1. Students should be regular and come prepared for the lab practice.
2. In case a student misses a class, it is his/her responsibility to complete that missed experiment(s).
3. Students should bring and maintain an observation book exclusively for the lab.
4. Once the experiment(s) get executed, they should show the program and results to the instructors and copy the same in their observation book.
5. Prescribed textbook and class notes can be kept ready for reference if required.
6. They should implement the given experiment individually.
7. Questions for lab tests and exam need not necessarily be limited to the questions in the manual, but could involve some variations and / or combinations of the questions.

Course Objectives

- To implement number theoretic algorithms and classical ciphers
- To implement and analyze public key cryptosystems
- To implement hashing and digital signatures
- To understand and implement a research paper

Course Outcomes

A student who successfully completes this course would be able to

- Implement the number theoretic algorithms and classical ciphers
- Analyse various public key cryptosystems including hashing and digital signatures
- Implement research paper on cryptography

PROCEDURE FOR EVALUATION

This lab would be one part of the Information Systems Lab I and the student will be evaluated for 100 marks based on following criteria and that will be reduced for 50 marks.

There will be 2 phases.

In the first phase, continuous evaluation of the experiments conducted between Week1 and Week 8.

Continuous evaluation → for 60 marks

Four evaluations, each for 10 marks→ one evaluation per two weeks

In the Second Phase, students will be working on Mini project between Week 9 to Week 12. Any research paper may be referred for this purpose. This will be evaluated for 20 Marks.

Mini Project →20 Marks

Final end semester Examination→ 20 Marks

CONTENTS

Week 1 : Implementation of Basic Number theoretic Algorithms C/C++/Java

1. Write a program to find the GCD of two numbers using Euclid algorithm
2. Write a program to find the modular multiplicative inverse of a number using extended Euclidian Algorithm

Week 2 : Implementation of Advanced Number theoretic Algorithms C/C++/Java

1. Write a program to solve a set of congruences using Chinese Remainder Theorem.
2. Implement the algorithm for fast exponentiation in congruences

Week 3: Implementation of classical ciphers in C/C++/Java

Implement the following classical ciphers in C/C++/Java

(i) Caesar Cipher
(ii) Hill Cipher
(iii) Playfair Cipher

Week 4: Implementation of public key cryptosystems in C/C++/Java

Implement the following public key cryptosystems

(i) RSA
(ii) ECC
(iii) El Gamal

Week 5: Implementation of Galois Field arithmetic operations in C/C++/Java

(i) GF(2^3)
(ii) GF(2^4)
(iii) GF(2^5)

Week 5: Implementation of hash algorithms in C/C++/Java

Implement the following hash algorithms

(i) MD5
(ii) SHA 512

Week 6: Implementation of digital signature algorithms in C/C++/Java

Implement the following digital signature algorithms

(i) RSA
(ii) El Gamal
(iii) Schnorr

Week 7: Implementation of digital signature/key exchange algorithms in C/C++/Java

Implement the following digital signature/key exchange algorithms

(i) DSS
(ii) Elliptic Curve Digital Signature scheme
(iii) Diffie Hellman Key exchange algorithm

Week 9 - Week 12: Mini Project

Students have to implement a research paper on Light weight cryptography in groups

Week 13: Test

References:

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay – "Cryptography and Network Security", McGraw Hill, 2nd Edition, 2008
2. William Stallings,"Cryptography And Network Security Principles And Practice", Fifth Edition, Pearson Education, 2013