CSE 5262 INFORMATION SYSTEMS

LAB II

CRYPTANALYSIS LAB

[0 0 6 2]

LAB MANUAL

II Sem M.Tech (CSIS)

(2019)

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 and cryptanalyze the classical stream ciphers
- To simulate and analyze various types of attacks on the symmetric cryptoystems
- To implement factorization, discrete logarithm and sieve algorithms for cryptanalysis of public key cryptosystems
- To cryptanalyze the hash functions

Course Outcomes

A student who successfully completes this course would be able to

- Use CrypTool to analyse the attacks on stream ciphers
- Analyse various kind of attacks on symmetric and asymmetric cryptosystems
- Analyse the attacks on hash functions.

PROCEDURE FOR EVALUATION

This lab would be one part of the Information Systems Lab II 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 40 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→ 40 Marks

CONTENTS

CONTENTS

(ii) Seive of Atkin

Week 8:
Analyse the attacks on Hash value using CryptTool

Week 9 - Week 12: Mini Project
Week 13: Test

References:

1. Antoine Joux, *"Algorithmic Cryptanalysis"*, CRC Press, 2009
2. Gregory V. Bard, *"Algebraic Cryptanalysis"*, Springer, 2009.
3. Richard J Spillman, *"Classical and Contemporary Cryptology"*, Pearson Education, 2005
4. Hans Delfs and Helmut Knebl, *"Introduction to Cryptography: Principles and Applications"*, Springer- Verlag, 2007
5. Alfred John Menezes, Paul C. van Oorschot, Scott A. Vanstone *"Handbook of Applied Cryptography"*, CRC Press, 1996