First Course Handout, CS670: Cryptographic Techniques for Privacy Preservation (2025, 1st Semester)

Adithya Vadapalli

Assistant Professor

Department of Computer Science and Engineering

Course Organization

Where? KD101

When? Monday, Thursday: 9:00 AM to 10:15 AM

Textbooks There is no textbook for the course. The course will be based on several research papers. All the course material will be shared through the course website.

Office Hours 11:30 AM to 12:30 PM, Mondays, at KD101

Course Structure

The course is divided into the following modules:

1. Module 0: Introduction
2. Module 1: Private Information Retrieval
3. Module 2: Secure Multiparty Computation
4. Module 3: Private Memory Access
5. Module 4: Zero Knowledge Proofs
6. Module 5: Secure Systems

Grading

Students would require a minimum of 50% marks to get a C and a minimum of 40% marks to procure a D+ grade. Anything between 34% and less than 40% would procure a D. The rest of the grading would be relative.

Distribution There will be a quiz and a programming assignment at the end of each module (except module 0 and 5). The distribution of marks for the course is as follows:

1. Quiz 1: 2.5%
2. Quiz 2: 2.5%
3. Quiz 3: 2.5%
4. Quiz 3: 2.5%
5. Programming Assignment 1: 10%
6. Programming Assignment 2: 10%
7. Programming Assignment 3: 10%
8. Programming Assignment 4: 10%
9. Midsem: 25%
10. Endsem: 25%

Quizzes

The quizzes will be closed-book.

Programming Assingments

You can choose any language. You have to submit a Docker container. The assignment must be completed individually.

Midsem and Endsem

One cheatsheet is allowed. It should be handwritten. You can write on both sides of the A4-sized paper.