Class Meetings
TuThu 3:35 pm – 4:50 pm.

Staff
Instructor: Viet Tung Hoang
Email: vhoang@fsu.edu
Office hours: TuThu, 10:30 am–11:30 am

Prerequisites
The official prerequisite is Discrete Math, but if you want to do well in this class, you need to have strong mathematical maturity and a good understanding of probability theory.

Textbooks
The following book is not required, but highly recommended.


What Is This Course About?
This is an introductory course to modern cryptography. Topics include block ciphers, hash functions, pseudorandom functions, symmetric encryption, message authentication, asymmetric encryption, digital signatures, and key distribution.

We adopt a “theory brought to practice” viewpoint, focusing on cryptographic primitives that are used in practice and showing how theory leads to higher-assurance real-world cryptography.
How Will You Be Evaluated?

Scores. The maximum total score is 1000 and its breakdown is shown below. There is no exam in this class.

Grading. Your total score will be converted to letter grade as shown below.

Participation Matters, But How?

In-class Questions. We will typically have many little questions during a lecture. For each question, I will give you a few minutes to think over it, and then one of you will volunteer to give an answer. This may require you to write to a Zoom’s whiteboard, so you should use a computer or tablet to launch Zoom meetings.

Peer Feedback. For each homework, after the deadline, you’ll receive some anonymized papers of your classmates. You need to provide critical feedback for improving the exposition of those papers.

Writing Matters, Too

Bad Writing Hurts. In your homework, 5% of the points will be reserved for the exposition, and that will be judged anonymously by your classmates. See the course website for writing resources.

Writing Workshops. We will occasionally hold a writing workshop to teach you how to write better.

Homework Policy

No Late Submission. In order to provide timely solutions to assignments, I do not accept late homework submissions.

Typesetting. Homework solutions must be typed, and submitted as a PDF file. See the course website for resources on typesetting mathematical writing, as well as a template for homework.

Group Homework. You can form a group of size at most two in each homework. You and your partner should submit a single paper. However, if you work with somebody in one homework, you need to collaborate with somebody else in the next homework.

Skip Class? You Won’t Pass

Attendance is required in this class. If your score is just a bit below the cutoff line, I’ll use your attendance to move you to the better grade. Your Zoom username must be the same as your real name, so that I can check your attendance.
University Attendance Policy

Excused absences include documented illness, deaths in the immediate family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities. Accommodations for these excused absences will be made and will do so in a way that does not penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness.

Academic Honor Policy

FSU Academic Honor Policy (found at http://fda.fsu.edu/Academics/Academic-Honor-Policy):

The Florida State University Academic Honor Policy outlines the University’s expectations for the integrity of students’ academic work, the procedures for resolving alleged violations of those expectations, and the rights and responsibilities of students and faculty members throughout the process. Students are responsible for reading the Academic Honor Policy and for living up to their pledge to “… be honest and truthful and … [to] strive for personal and institutional integrity at Florida State University.”

Americans With Disabilities Act

Students with disabilities needing academic accommodation should: (1) register with and provide documentation to the Student Disability Resource Center; and (2) bring a letter to the instructor indicating the need for accommodation and what type.

This syllabus and other class materials are available in alternative format upon request. For more information about services available to FSU students with disabilities, contact:

Student Disability Resource Center
874 Traditions Way
108 Student Services Building
Florida State University
Tallahassee, FL 32306-4167
(850) 644-9566 (voice)
(850) 644-8504 (TDD)
sdrc@admin.fsu.edu
http://www.disabilitycenter.fsu.edu

Syllabus Change Policy

This syllabus is a guide for the course and is subject to change with advanced notice.