MATH 1025: Introduction to Mathematical Cryptography

Spring 2021

Syllabus

Overview

This course is a one-semester introductory course in mathematical cryptography. It focuses on covering the basic aspects of design of cryptosystems and in analysis of their limitations and vulnerabilities. Students will learn the underlying principles behind cryptosystems and will see how some of these systems are used in real-world applications such as digital signatures and bitcoin. The course places a special emphasis on public-key cryptosystems. Elliptic curve cryptography will be introduced.

Classes

The course meets via Zoom, MWF $115 - 205$.

Prerequisites

Math 430

Texts

[1] J. Hoffstein, J. Pipher, and J. H. Silverman, *An introduction to mathematical cryptography*, 2nd ed., Undergraduate Texts in Mathematics, Springer, New York, 2014.

[2] N. Koblitz, *A course in number theory and cryptography*, 2nd ed., Graduate Texts in Mathematics, vol. 114, Springer-Verlag, New York, 1994.

The entire book [1] is available for free download in pdf format from the University of Pittsburgh library. Be sure to get the second edition. The second edition rearranges chapters and corrects many errors. The second book [2] will serve as an excellent source for supplementary material.

Course website

http://www.pitt.edu/ bdt18/IntrotoCryptography.html

Instructor

Boris Tsvelikhovskiy
email: bdt18 AT pitt.edu

Grading

Your course grade will be based on the following components

(1)	Homework	50%
(2)	Midterm exam	25%
(3)	Final exam	25%

Students with Disabilities

If you have a disability for which you are or may be requesting an accommodation, you are encouraged to contact both your instructor and the Office of Disability Resources and Services, 216 William Pitt Union, 412- 648-7890/412-383-7355 (TTY), as early as possible in the term. That office will verify your disability and determine reasonable accommodations for this course. Academic Integrity Cheating/plagiarism will not be tolerated. Students suspected of violating the University of Pittsburgh Policy on Academic Integrity, from the February 1974 Senate Committee on Tenure and Academic Freedom reported to the Senate Council, will be required to participate in the outlined procedural process as initiated by the instructor. A minimum

sanction of a zero score for the quiz or exam will be imposed. Students are encouraged to study in groups and to discuss homework problems with one another. However, each student is expected to write solutions to homework problems entirely independently, without the use of notes provided by other students or tutors. Solutions should accurately reflect the student's own understanding of the problems.

Email Policy

Each student is issued a University email address upon admittance. This email address may be used by the University for official communication with students. Students are responsible for official communications sent to this address. For the full email communication policy, go to www.bc.pitt.edu/policies/policy/09/09-10-01.html