Pitt Math 1025 spring 2016

About

Introduction to Mathematical Cryptography

Overview
This course is a one-semester introductory course in mathematical cryptography. Mathematics is used both in the design of cryptosystems and in the 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 web browser security and bitcoin. The course places special emphasis on public-key cryptosystems. Elliptic curve cryptography will be introduced.

Classes
The course meets in G27 Benedum Hall, MWF 1-2.

Prerequisites
Math 430

Text
An introduction to Mathematical Cryptography.
Hoffstein, Pipher, and Silverman, 2nd Edition, 2014.
The entire book 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.

Course website
https://pittmath1025spring2016.wordpress.com/

Instructor
Thomas Hales, Thackeray 416, email: lastname at pitt.edu

Grading
Your course grade will be based on the following components
Weekly homework 1/3
Midterm exam 1/3
Final exam 1/3

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