Introduction to mathematical cryptography (Math 1025)

Spring 2025

Time:	MWF 10:00 am – 10:50 am
Place:	627 Thackeray Hall (6th floor)
Course Page:	https://canvas.pitt.edu/courses/310300

Instructor: My name is Mohamed Moakher, and you're welcome to call me "Mohamed". I am originally from Tunis, Tunisia. I completed my PhD in number theory in Paris, and I have just begun a postdoctoral position here at Pitt.

How to contact me: You can email me at mom224@pitt.edu, and you are welcome to set up a meeting with me at my office, 518 Thackeray Hall.

Office Hours: Will be at the lounge on the 7th floor of Thackeray Hall, *initially* scheduled from 2pm to 3:30pm on Wednesdays.

Course description: This is an introductory course on mathematical cryptography. The course explores how mathematics is applied both to the design of cryptosystems and to the analysis of their limitations and vulnerabilities. Students will gain an understanding of the principles underlying public-key cryptography, as well as the mathematical foundations essential to the subject. The course also includes an introduction to elliptic curve cryptography.

Main References: The main textbook thatI plan to reference is

- *An introduction to Mathematical Cryptography*, by 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.

Both references can be downloaded from the course webpage. I highly recommend reviewing the textbook and familiarizing yourselves with the material before and after class. Understanding mathematical concepts requires time, repetition, and personal effort. You shouldn't expect to grasp everything just by attending lectures.

Problem sets: There will be frequent problem sets that you should submit through Canvas.

Use of LaTeX is strongly encouraged. Problem sets completed using LaTeX, which is the standard typesetting package in mathematics and many other fields, will receive a 5% bonus. LaTeXis free and can be downloaded to your computer. You can use a free online version such as Overleaf to compile documents in LaTeX.

Late problem sets will not be accepted, unless you seek approval of an extension from me *at least 24 hours in advance*. Any problem set not turned in by the deadline receives a grade of zero.

Collaboration Policy: You may collaborate with fellow students on the problem sets, provided that you

- write up your explanations independently, and
- list the names of those that you collaborated with on your written assignment.

Grading Policy: Problem sets (40%) (lowest score will be dropped), Midterm (25%), Final (35%).

Disability Resource Services: 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, 140 William Pitt Union, 412-648-7890, as early as possible in the term. Disability Resources and Services ("DRS") will verify your disability and determine reasonable accommodations for this course. More information may be found at http://www.studentaffairs.pitt.edu/drs/.

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 problem set or exam will be imposed (In particular, this includes following the collaboration policy described above).