# Introduction to Mathematical Cryptology

## Math 127 KAUST - Spring 2017

**Instructor:** Gabriel Dorfsman-Hopkins

**Office:** Padelford Hall C-008-G

**Email:** gdh2@math.washington.edu

**Website:** `www.math.washington.edu/~gdh2/m127sp19`

**Lectures:** MWF 2:30-3:50 PM, THO 335. Office Hours will be posted on the course website (above). If you would like to meet with me at any other time, please send me an email and we can arrange a time.

**Purpose:** This course is designed to be a gentle introduction the the theory of mathematical cryptography. This is a beautiful and very concrete application of some more abstract and theoretical mathematics. The main goal will be to get an understanding of public key cryptography and RSA. If we have any time left we may explore the geometric enhancement using elliptic curves.

Along the way we will introduce some modern number theory, abstract algebra, and a bit linear algebra of probability theory. We will also spend some time warming up to a theorem-proof style of abstract mathematics. The pace will be relatively gentle, and the goal is to explore some modern mathematics with a very concrete application to guide us.

We will also be using mathematical software to implement some algorithms of our own. I'd reccommend sage, wich is a free add on to python, and can also be run in your browser at cocalc.com.

**Textbook:** The required text is the *An Introduction to Mathematical Cryptography*, 2014 edition, (the 11-12 edition is ok) by Hoffstein, Phipher and Silverman. A free electronic copy is accessible through the UW Library.

**Homework:** Homework will be assigned as problems from the book, and I will collect it weekly on Mondays.

**Quizzes:** There will be a few quizzes throughout the course. They will be mainly for me to measure progress and maintain pace

**Exam:** There will be one exam, given on the last day of the course (May 15th).

**Grades:**

- Homework: 30%
- Quizzes: 30%
- Exam: 30%
- Participation: 10%

**Quiz or Exam absence:** If you miss a midterm or quiz due to some unavoidable, sudden event (such as a sudden illness, a familye emergency, a traffic accident, etc..) you should contact me as soon as possible.

**Disability Services Office:** The University of Washington is committed to providing access, equal opportunity, and reasonable accomodation in its services, programs, activities, education, and employment for individuals with disabilities. To request disability accommodation contact the Disability Services Office at least ten days in advance at: 206-543-6450/V, 206-543-6452/TTY, or dso@u.washington.edu.