MATH 75: MATHEMATICAL CRYPTOGRAPHY
SPRING 2016

JOHN VOIGHT

Course Info

- **Lectures**: Monday, Wednesday, Friday, block 2 (1:45–3:00 p.m.)
- **x-period**: Thursday, 1:00–1:50 p.m.
- **Dates**: 28 March 2016 – 31 May 2016
- **Room**: 028 Haldeman Center
- **Instructor**: John Voight
- **Office**: 341 Kemeny Hall
- **E-mail**: `jvoight@gmail.com`
- **Instructor's Office Hours**: Monday 3:00–4:30 p.m. and Tuesday 10:00–11:30 a.m., or by appointment
- **Course Web Page**: `http://www.math.dartmouth.edu/~m75s16/`
- **Prerequisites**: Math 71, or Math 25 and 31, or instructor permission
- **Required Texts**:
  (1) Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, second edition, 2014.
  (2) Paul Garrett, *Making, Breaking Codes: Introduction to Cryptology*, 2001.
  (3) Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, 2000.
- **Recommended Texts**: None
- **Grading**: Grade will be based on weekly homework (50%) and a final cipher challenge (50%).

Homework

The homework assignments will be posted on the course webpage. Late homework will not be accepted. Standard weekly homework assignments, counting for 50% of the grade, will be typically due on Wednesdays.

Cooperation on homework is permitted (and encouraged), but if you work together, do not take any paper away with you–in other words, you can share your thoughts (say on a blackboard), but you have to walk away with only your understanding. In particular, you must write the solution up on your own. Please acknowledge any cooperative work at the end of each assignment.

Certain problems will be computational in nature and can be solved using a computer algebra package; please print out and attach complete code and output.

Plagiarism, collusion, or other violations of the Academic Honor Principle, after consultation, will be referred to the The Committee on Standards.

Final cipher challenge

A final cipher challenge will be assigned in place of a final exam. Further details will be forthcoming and posted on the course webpage.

Religious observances and accommodation

Some students may wish to take part in religious observances that occur during this academic term. If you have a religious observance that conflicts with your participation in the course, please meet with me before the end of the second week of the term to discuss appropriate accommodations.

Students with disabilities, including "invisible" disabilities such as chronic diseases and learning disabilities, enrolled in this course and who may need disability-related classroom accommodations are encouraged to make an appointment to see me before the end of the second week of the term. All discussions will remain confidential, although the Student Accessibility Services office may be consulted to discuss appropriate implementation of any accommodation requested.

Library

A key to successful research is the use of reliable, high-quality information sources. While some information can be found on the open web, the best place to start your research is at the Librarys Mathematics Research Guide, `http://researchguides.dartmouth.edu/math/`. This research guide has the librarys key mathematics resources organized for easy use. The Kresge Physical Science Library website, `Dartmouth.edu/~library/Kresge/`, also has information on useful research tools and services. In addition to the online information, Katie Harding, the Mathematics Librarian, has been assigned to this class to answer research questions and to help you find appropriate resources. Katie can be reached at `katie.harding@dartmouth.edu`.

Syllabus

We live an information age, with technology increasingly integrated into our daily lives. As a result, the security of our information is of the utmost concern, even as the interconnectedness of the Internet makes our data more vulnerable to attack. The ability to encrypt secrets and to conduct a trusted exchange of digital information, once a subject of interest primarily to governments and the military, is now a matter of necessity for us all.

At the end of the day, the foundation of modern cryptography relies upon the difficulty of solving certain mathematical problems; this course is intended to address them from both a mathematical and algorithmic point of view. We will cover some subset of the following topics: conventional encryption techniques, the Hill cipher, DES and SDES, RSA, the Rijndael cipher, discrete logarithms and the Diffie-Hellman key exchange, and elliptic curve cryptography.

All mathematical objects will be defined, so the essential prerequisite is familiarity with abstract algebra and a healthy mathematical and computational appetite. Some experience with number theory would also be helpful. We will also be writing some simple computer programs in Python.

A full schedule is available on the course webpage.