MATH/CS 295: MATHEMATICAL CRYPTOGRAPHY FALL 2012

JOHN VOIGHT

Course Info

- **Lectures**: Monday, Wednesday, Friday, 12:50 p.m.–1:40 p.m.
- **Dates**: 27 August 2012–5 December 2012
- **Room**: Votey 209
- **Course Record Number (CRN)**: 93918 (Math), 94628 (CS)

- **Instructor**: John Voight
- **Office**: 16 Colchester Ave, Room 207C
- **Phone**: (802) 656-2271
- **E-mail**: `jvoight@gmail.com`
- **Instructor's Office Hours**: Mondays and Wednesdays, 2:00–3:30 p.m.; or just make an appointment!
- **Course Web Page**: `http://www.cems.uvm.edu/~jvoight/295/`
- **Instructor's Web Page**: `http://www.cems.uvm.edu/~jvoight/`

- **Prerequisites**: Math 52 (or Math 54) and Math 124 and one of the following: Math 251, Math 255, or permission. To get permission, all you need is some advanced coursework and a healthy dose of curiosity!
- **Required Texts**: Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman, *An Introduction to Mathematical Cryptography*, 2010.
  Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, 2000.
- **Grading**: Weekly homework will count for 55% of the grade. Class participation and preparedness will count for 5% of the grade. A final cipher challenge will count for 40% of the grade.

Homework

The homework assignments are posted on the course webpage. Late homework will not be accepted. Standard weekly homework assignments, counting for 55% of the grade, will be typically due on Wednesdays (sometimes Fridays).

Be sure to show your work and explain how you got your answer. Correct but incomplete answers will only receive partial credit. Part of the beauty of mathematics is in the elegance of its proofs, and one goal of this course is for you to learn to write mathematics excellently.

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, write the solution up on your own. Please write on your assignment the names of any other collaborators you worked with.

Certain problems will be computational in nature and the use of computer algebra packages is encouraged. Please print out and attach your work.

Plagiarism, collusion, or other violations of the Code of Academic Integrity

(see `http://www.uvm.edu/policies/student/acadintegrity.pdf`)

will be referred to the The Center for Student Ethics and Standards.

Class participation and preparedness

You are expected to read the section before we cover it in class. Come with good questions! Your participation and preparedness in class is essential for your success and will be assessed accordingly.

As a requirement for class participation, you must come to my office at least once before Thanksgiving break. A short visit suffices; if you cannot come during office hours, please email me to set up an appointment.

Accommodation

Appropriate and fair accommodations will be provided for students with documented special needs; please contact the ACCESS office (`http://www.uvm.edu/~access/`) directly and early in the semester.

Students have the right to practice the religion of their choice. Each semester students should submit in writing by the end of the second full week of classes their documented religious holiday schedule for the semester.

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.