MATH 295A/395A: CRYPTOGRAPHY

JOHN VOIGHT

Course Info

- **Lectures**: Monday, Wednesday, Friday, 1:25 p.m.–2:15 p.m.
- **Room**: Lafayette L102
- **Instructor**: John Voight
- **Office**: 16 Colchester Ave, Room 207C
- **E-mail**: `jvoight@gmail.com`
- **Instructor's Office Hours**: Mondays, 11:00 a.m.–12:00 noon and 2:30 p.m.–3:30 p.m.; Wednesdays, 11:00 a.m.–12:00 noon; or please make an appointment!
- **Course Web Page**: `http://www.cems.uvm.edu/~voight/295/`
- **Instructor's Web Page**: `http://www.cems.uvm.edu/~voight/`

- **Prerequisites**: Math 52 (or 54) or 124 or permission.
- **Required Text**: Wade Trappe and Lawrence C. Washington, *Introduction to Cryptography with Coding Theory*, second edition, Prentice Hall, 2005.
- **Recommended Text (295A)**: Johannes Buchmann, *Introduction to Cryptography*, second edition, Springer, 2004.
- **Recommended Text (395A)**: Jeffrey Hoffstein, Jill Pipher, J.H. Silverman, *An Introduction to Mathematical Cryptography* (Undergraduate Texts in Mathematics), Springer, 2008.
- **Grading**: Weekly homework will count for 65% of the grade. There will be a final cipher challenge which will count for 35% of the grade.

I am happy to provide appropriate and fair accommodations for students with documented special needs; early in the semester, please contact the ACCESS office (`http://www.uvm.edu/~access/`) directly. 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.

Synopsis

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.

Homework

Homework is due on Wednesdays. Be sure to show your work and explain how you got your answer. Correct but incomplete answers will only receive partial credit.

Some of the problems may require you to consult the text—this is an intentional effort to encourage you to read the required (and perhaps also the recommended) books throughout the course.

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.

Certain problems will be computational in nature and the use of computer algebra packages such as Mathematica or Sage is encouraged. Please print out and attach your work. The use of computers is permitted on other problems, but should not take the place of practice and conceptual understanding.

Final Cipher Challenge

There will be no exams in the course. In place of a final exam, there will be a final cipher challenge. Further details will be forthcoming.

Syllabus

Although we may deviate from this by adding or skipping topics, the tentative plan for the course is as follows.

- **Chapters 1–2**: Introduction and Basic Number Theoretic Ciphers
  - **1**, 3 Sep (W): §1.1: Secure Communications
  - **2**, 5 Sep (F): §3.3: Congruences, §2.1: Shift Ciphers
  - **3**, 8 Sep (M): §§3.1–3.2: The Euclidean Algorithm
  - **4**, 10 Sep (W): §§3.1–3.2, Computational Tools
  - **5**, 12 Sep (F): Computation, Big O-Notation, §2.8: Binary Numbers
  - **6**, 15 Sep (M): §2.2: Affine Ciphers
  - **7–8**, 17, 19 Sep (W, F): §2.3: The Vignère Cipher
  - **9**, 22 Sep (M): §2.4: Substitution Ciphers
  - **10**, 24 Sep (W): Permutations
  - **11**, 26 Sep (F): §2.7: Block Ciphers
  - **12**, 29 Sep (M): §3.8: Inverting Matrices Mod n, Determinants
  - **13**, 1 Oct (W): §2.8: ASCII, §2.9: One-Time Pads
- **Chapters 4–5**: Some Modern Ciphers
  - **14, 15, 16**, 3, 6, 8 Oct (F, M, W): §2.9: Enigma
  - **17**, 10 Oct (F): §§4.1–4.2: SDES
  - **18**, 13 Oct (F): §4.4: DES
  - **19**, 15 Oct (W): §5.1: The Basic [Rijndael] Algorithm
  - **20**, 17 Oct (F): §5.2: The Layers
  - **21**, 20 Oct (M): §5.3: Decryption
- **Chapter 6**: RSA
  - **22**, 22 Oct (W): §6.1: The RSA Algorithm
  - **23**, 24 Oct (F): §6.2: Attacks on RSA
  - **24**, 27, 29 Oct (M, W): §6.3: Primality Testing
  - **26**, 31 Oct (F); 3, 5 Nov (M, W): §6.4: Factoring
- **Chapters 7, 10**: Discrete Logarithms and Security Protocols
  - **29**, 7 Nov (F): §7.1: Discrete Logarithms
  - **30**, 10 Nov (M): §7.2: Computing Discrete Logs
  - **31**, 12 Nov (W): §7.4: Diffie-Hellman Key Exchange
  - **32**, 14 Nov (F): §7.5: The ElGamal Public Key Cryptosystem
  - **33**, 17 Nov (M): Topics from Chapter 10: Security Protocols
  - **34**, 19 Nov (W): §10.6: Pretty Good Privacy
  - **35**, 21 Nov (F): TBD

    24–28 Nov (M–F): *No class, Thanksgiving Recess*
- **Chapters 16, 19**: Elliptic Curves and Quantum Cryptography
  - **36**, 1 Dec (M): §16.1: The Addition Law
  - **37**, 3 Dec (W): §16.2: Elliptic Curves Mod p
  - **38**, 5 Dec (F): §16.3: Factoring with Elliptic Curves
  - **39**, 8 Dec (M): §16.5: Elliptic Curve Cryptosystems
  - **40**, 10 Dec (W): Topics from Chapter 19: Quantum Techniques in Cryptography