MATH 295B/395A: CRYPTOGRAPHY

JOHN VOIGHT

Course Info

- **Lectures**: Monday, Wednesday, Friday, 12:50 p.m.–1:40 p.m.
- **Room**: Votey 254
- **Instructor**: John Voight
- **Office**: 16 Colchester Ave, Room 207C
- **E-mail**: `jvoight@gmail.com`
- **Instructor's Office Hours**: Mondays and Wednesdays, 10:45 a.m.–12:15 p.m.; 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.
- **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.

Homework

Homework is due on 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, you must write the solution up on your own.

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.

Computational Resources

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

See the website for links.

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**, 30 Aug (M): Introduction
  - **2**, 1 Sep (W): §1.1: Secure Communications, §2.1: Shift Ciphers
  - **3**, 3 Sep (F): §3.3: Congruences
    6 Sep (M): *No class, Labor Day*
  - **4**, 8 Sep (W): §§3.1–3.2: The Euclidean Algorithm
  - **5**, 10 Sep (F): §§3.1–3.2, Computational Tools
  - **6**, 13 Sep (M): Computation, Big O-Notation, §2.8: Binary Numbers
  - **7**, 15 Sep (W): §2.2: Affine Ciphers
  - **8**, 17 Sep (F): §2.3: The Vigenère Cipher
  - **9**, 20 Sep (M): §2.3
  - **10**, 22 Sep (W): §2.4: Substitution Ciphers
  - **11**, 24 Sep (F): §2.7: Block Ciphers
  - **12**, 27 Sep (M): §3.8: Inverting Matrices Mod n, Determinants
  - **13**, 29 Sep (W): §2.8: ASCII, §2.9: One-Time Pads
- **Chapters 4–5**: Some Modern Ciphers
  - **14**, 1 Oct (F): §2.9: Enigma
  - **15**, 4 Oct (M): §2.9
  - **16**, 6 Oct (W): §2.9
  - **17**, 8 Oct (F): §§4.1–4.2: SDES
  - **18**, 11 Oct (M): §4.4: DES
  - **19**, 13 Oct (W): §5.1: The Basic [Rijndael] Algorithm
  - **20**, 15 Oct (F): Finite Fields
  - **21**, 18 Oct (M): §5.2: The Layers
- **Chapter 6**: RSA
  - **22**, 20 Oct (W): §6.1: The RSA Algorithm, §6.7: The Public Key Concept
  - **23**, 22 Oct (F): §6.1
  - **24**, 25 Oct (M): §6.2: Attacks on RSA
  - **25**, 27 Oct (W): §6.3: Primality Testing
  - **26**, 29 Oct (F): §6.3
  - **27**, 1 Nov (M): §6.4: Factoring
  - **28**, 3 Nov (W): §6.4
  - **29**, 5 Nov (F): §6.4
- **Chapters 7–10**: Discrete Logarithms through Security Protocols
  - **30**, 8 Nov (M): §7.1: Discrete Logarithms
  - **31**, 10 Nov (W): §7.2: Computing Discrete Logs
  - **32**, 12 Nov (F): §7.4: Diffie-Hellman Key Exchange, §7.5: The ElGamal Cryptosystem
  - **33**, 15 Nov (M): Topics from Chapter 8: Hash Functions
  - **34**, 17 Nov (W): Topics from Chapter 9: Digital Signatures
  - **35**, 19 Nov (F): Topics from Chapter 10: Security Protocols
    22–26 Nov (M–F): *No class, Thanksgiving Recess*
- **Chapters 16, 19**: Elliptic Curves and Quantum Cryptography
  - **36**, 29 Nov (M): §16.1: The Addition Law
  - **37**, 1 Dec (W): §16.2: Elliptic Curves Mod p
  - **38**, 3 Dec (F): §16.3: Factoring with Elliptic Curves
  - **39**, 6 Dec (M): §16.5: Elliptic Curve Cryptosystems
  - **40**, 8 Dec (W): Topics from Chapter 19: Quantum Techniques in Cryptography