HONS 195N:
A SOCIAL AND MATHEMATICAL HISTORY OF CRYPTOGRAPHY

JOHN VOIGHT

Course Info

- **Lectures**: Monday, Wednesday, Friday, 12:50–1:40 p.m.
- **Room**: University Heights North Complex 016
- **Instructor**: John Voight
- **Office**: 16 Colchester Ave, Room 207C
- **E-mail**: `jvoight@gmail.com`
- **Instructor's Office Hours**: Mondays, 10:00–11:30 a.m. and 2:00–3:30 p.m.; or please make an appointment!
- **Course Web Page**: `http://www.cems.uvm.edu/~voight/195N/`
- **Instructor's Web Page**: `http://www.cems.uvm.edu/~voight/`

- **Prerequisites**: None.
- **Required Texts**: Simon Singh, *The Code Book*, reprint edition, Anchor, 2000. There is also a coursepack, available at the bookstore.
- **Grading**: Weekly homework will count for 50% of the grade, class participation 10%, and a final paper will count for 40% in place of the final exam.

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.

Homework

Occasional homework will be given roughly on a weekly basis. Some homework assignments may include writing response essays. Others will be mathematical problems; be sure to show your work and explain how you got your answer. Cooperation on these homework problems is permitted (and encouraged), but if you work together, write the solution up on your own.

Class participation

To encourage lively participation, the final grade includes a metric of your preparedness and responsiveness in class.

A Google group for the class has been created. It can be reached at

`http://groups.google.com/group/hons195n`.

On certain days of class discussion, you will be asked to send one or more questions, concerns, points of clarification or interest, etc. to the group concerning the reading on the day before each class. You are encouraged but not required to read the questions of your peers.

Reading

Additional required reading will be posted on the course website; the reading materials themselves can be obtained on Blackboard at `https://bb.uvm.edu/`.

Final paper

A final research paper of 10–15 pages in length will be due at the time of the final exam, Thursday, 17 December 2009, at 3:30 p.m. Details on this paper will be forthcoming.

Exams

There will be no exams in the course.

Syllabus

The Enigma machine was used by the Nazi regime during World War II to encrypt secret governmental and military messages. It used an immensely complex series of electrical wiring and mechanical rotors to encode U-boat locations, governmental orders, and other highly sensitive information into what was thought to be an undecipherable stream of letters. However, a team of British mathematicians at Bletchley Park, led by Alan Turing-building upon work of Polish cryptographers-were able to crack the Enigma machine using a combination of mathematical analysis, computation, luck, and immense cleverness.

This course will discuss the many dimensions of this feat. By way of introduction, we will begin by discussing early (and more basic) cryptosystems, such as the cipher used by Julius Caesar and other simple substitution ciphers. We will then analyze the Enigma machine: we will investigate the history of the machine, its inner workings, and the implications of its use from a political and military perspective. We will then turn to the work of Allied cryptographers, focusing on Bletchley Park (a timely subject as the location is now at risk of closure due to a lack of funding). It is widely believed that the foundations of modern computing came out of these efforts, and in particular we will discuss the life and work of Alan Turing. After the war ended, when it was revealed that he was a homosexual, after years of hormone treatment he committed suicide by cyanide poisoning, which he consumed by taking a bite from a laced apple found beside his bed. The students will consider the role of heterosexism (and other prejudices) when unpacking this episode and looking in to its historical context.

To conclude the course, we will treat some topics in modern cryptography. 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 as with the Enigma machine, is now a matter of necessity for us all. The foundation of modern cryptography relies upon the difficulty of solving certain mathematical problems, in particular, the factorization of integers. We will discuss the RSA cryptosystem and (time permitting) a few other modern cryptosystems, such as the future of quantum cryptography.

The tentative plan for the course is as follows.

- **Basic Cryptography**
  - **1**, 31 Aug (M): Introduction
  - **2**, 2 Sep (W): Shift ciphers and congruences
  - **3**, 4 Sep (F): Substitution ciphers
    7 Sep (M): *No class, Labor Day*
  - **4**, 9 Sep (W): Frequency analysis
  - **5**, 11 Sep (F): The Babington plot
  - **6**, 14 Sep (M): Cribs
  - **7**, 16 Sep (W): Vigenère cipher
  - **8**, 18 Sep (F): Displacement analysis
  - **9**, 21 Sep (M): Kasiski test
  - **10**, 23 Sep (W): Statistical analysis
- **The Enigma Machine: Mathematical Analysis**
  - **11**, 25 Sep (F): Basic functioning of the Enigma machine
  - **12**, 28 Sep (M): Demonstration
  - **13**, 30 Sep (W): Simple Enigmas
  - **14**, 2 Oct (F): Basic principles of counting
  - **15**, 5 Oct (M): Permutations, combinations, and the binomial theorem
  - **16**, 7 Oct (W): The plugboard
    9 Oct (F): *No class, Fall Recess*
  - **17**, 12 Oct (M): The plugboard does not hide all fingerprints
  - **18**, 14 Oct (W): Beautiful Polish females
  - **19**, 16 Oct (F): Passing the torch
  - **20**, 19 Oct (M): The Turing bombes
  - **21**, 21 Oct (W): Bombe and Spider
  - **22**, 23 Oct (F): The bombes at work
  - **23**, 26 Oct (M): The Automatic Computing Engine
- **Cryptology and World War II: Historical Analysis**
  - **24**, 28 Oct (W): The Staff School memory
  - **25**, 30 Oct (F): Historical overview
  - **26**, 2 Nov (M): SHARK
  - **27**, 4 Nov (W): The influence of Ultra in WW2
  - **28**, 6 Nov (F): Hut 6, Hut 8, and naval Enigma
- **The Life and Work of Alan Turing**
  - **29**, 9 Nov (M): Biography of Alan Turing
  - **30**, 11 Nov (W): "Relay Race"
  - **31**, 13 Nov (F): "On the Beach"
  - **32**, 16 Nov (M): Computing machinery and intelligence
  - **33**, 18 Nov (W): The Turing Test
  - **34**, 20 Nov (F): From Turing to the information society
  - **35**, 23 Nov (M): Discussion and wrap-up
    25–27 Nov (W–F): *No class, Thanksgiving Recess*
- **Modern Cryptography**
  - **36**, 30 Nov (M): Public key cryptography
  - **37**, 2 Dec (W): GCDs and modular inverses
  - **38**, 4 Dec (F): Exponentiation and Fermat's little theorem
  - **39**, 7 Dec (M): RSA
  - **40**, 9 Dec (W): Integer factorization