Cryptography:
The History and Mathematics of Codes and Code Breaking

Basic Information

Days and Times: Tuesdays and Thursdays, 9:35-10:50
Location: Crawford House 208
Course Blog: http://derekbruff.com/site/fywscrypto/

Instructor

Dr. Derek Bruff
Assistant Director, Center for Teaching
Senior Lecturer, Department of Mathematics

Office: Center for Teaching, 1114 19th Ave. S.
Phone: 617-322-3420
Email: derek.bruff@vanderbilt.edu

Office Hours

Mondays	5:00-6:00	
Wednesdays	1:30-2:30	
Thursdays	4:00-5:00	…and by appointment any weekday

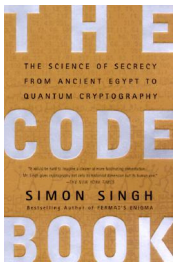
Course Description

Julius Caesar used ciphers to keep his enemies from reading messages he sent to his generals. Sherlock Holmes deciphered a code to solve "The Mystery of the Dancing Men." The defeat of the German Enigma Machine in World War Two by Polish and British cryptanalysts required espionage by Ian Fleming, creator of James Bond, and played an important role in the Battle of the Atlantic and D-Day. It also led to the construction of the first digital computers, which ushered in an information age where cryptography makes information security possible and plays a role in electronic commerce and social justice. This course is designed to provide an understanding and appreciation of the ways in which codes and code breaking have impacted history, technology, and culture. Students will learn concepts and techniques from abstract mathematics used in classical and modern cryptography. Students will also gain proficiency in creating and breaking fun and simple codes and ciphers.

Course Goals

1. To understand and appreciate the ways in which codes and code breaking have impacted history, technology, and culture—and ways they continue to do so
2. To understand and apply important concepts and techniques from abstract mathematics used in classic and modern cryptography
3. To improve skills in communicating in writing technical information and opinion- and evidence-based arguments
4. To gain proficiency in creating and breaking simple codes and ciphers

Textbooks



Required: *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* by Simon Singh (Anchor Books, 1999)

Recommended: *Invitation to Cryptology* by Thomas Barr (Prentice Hall, 2002)

Participation

Your active participation in this course is encouraged since it will benefit your own learning as well as those of your peers. Aside from contributing to discussions during class, there are three primary ways you can participate:

1. Online Discussion – Each week you'll be assigned something to read prior to class, typically a selection from the Singh book. I'll post a few open-ended discussion questions about the reading on the course blog, and you're invited to respond to these questions in writing by leaving comments on the blog. More info: http://is.gd/dYPZV.

2. Social Bookmarking – There are many websites, news articles, and other online resources related to cryptography. To help us all learn about and explore these resources, you are encouraged to sign up for an account on the social bookmarking site Delicious (delicious.com) and start bookmarking websites relevant to the course using the tag *fywscrypto*. You can then visit http://delicious.com/tag/fywscrypto to see the sites we've all tagged in Delicious. More info: http://is.gd/dYQ2t.

3. Collaborative Timeline – Another way to participate will be to contribute items to a cryptography timeline we will construct collaboratively as a class this semester. By dating and describing significant events in the history of cryptography, we will build a timeline that looks like this one: http://is.gd/5UZ6j. This timeline will be useful to all students as they write their final papers. More info: http://is.gd/e66Eu.

I'll monitor your participation in these three areas in order to assign to you a participation grade which will contribute 15% of your overall course grade. Please note that you need not participate in all three areas to obtain a high participation grade. Participating regularly in *at least two* of the three areas is sufficient. I'm providing you these three options so you can participate in a way that suits your personal learning style.

Problem Sets

Since we'll be exploring mathematical aspects of cryptography and since doing mathematics is a much better way to learn mathematics than watching someone else do mathematics, you'll be assigned several problem sets during the semester. Each problem set will feature a few mathematics and/or cryptography problems related to the material recently discussed in the class. Solutions to the problem sets will be discussed in class.

You are encouraged to work on your homework with other students, although copying another student's work is not permitted. If you do work with others on a homework assignment, list your

collaborators' names on your assignment. That way you can give appropriate credit to your collaborators.

Your solutions to each problem set will be graded. Your lowest score will be dropped (allowing you to skip a problem set altogether if you wish) and the remaining scores averaged to contribute 30% of your overall course grade.

Essay #1 – Opinion Paper

In this paper, you'll be asked to share your opinions on one of the following two questions (your pick):

1. Should the public (private citizens, businesses, etc.) have access to advanced encryption techniques, even if that means that law enforcement and national security efforts become more difficult to implement?
2. Why do people find cryptography so interesting (in novels and movies, for instance)? Why do some people enjoy cracking codes themselves (either individually or collaboratively)? Why do some people not enjoy such endeavors?

Your paper should draw primarily on your personal experiences and perspectives. You are not required to do research for this paper, but you should provide references for any significant facts you include in your paper (such as news stories or descriptions of novels or movies). Your paper should be about 3 pages long (typed in 11 or 12 point font, double-spaced) and will be graded primarily on grammar, punctuation, structure, and coherence.

Your opinion paper will contribute 10% of your overall course grade and is due at the start of class on September 28th.

Essay #2 – Expository Paper

In this paper, you'll be asked to explore the origin, use, and decryption of a particular cipher or code (one not explored in depth already in the course) with a focus on clear explanations of the mathematics involved. Your paper should be about 5 pages long (typed in 11 or 12 point font, double-spaced). It should include a list of references and should make clear how you used those references. Your paper will be graded primarily on the quality of your explanations.

All of the expository papers will be shared with the class on the course blog, so keep your audiences (your classmates, as well as the rest of the Internet) in mind as you work. You'll be asked to read and respond to two of your peers' papers on the blog. Sharing the expository papers this way will allow all of us expand the set of ciphers and codes with which we're familiar.

We will spend the class session on September 28th on an introduction to using library resources for researching the literature on cryptography. This will equip you to find and use references for your paper appropriately. We will also have an "essay workshop" in class on October 21st during which you'll read and provide feedback on your peers' draft papers. Your expository paper will contribute 15% of your overall course grade and is due at the start of class on October 26th. You'll also have a chance to revise your expository paper; this revision is due at the start of class on November 11th.

Essay #3 – "Big Questions" Paper

For your final assignment, you'll be asked to focus on "big questions" about the ways in which cryptography has impacted history, culture, and/or technology. Whereas the expository paper focuses on clear explanations, the "big questions" paper focuses on analysis, evaluation, and critical thinking. You'll be asked to pose one or more "big questions" about the role of cryptography in human affairs, suggest answers to those questions, and provide evidence for your answers. The assignment will take the form of a paper about 10 pages long (typed in 11 or 12 point font, double-spaced) with appropriate references and citations. Your paper will be graded on the strength and clarity of your evidence-based arguments.

We will have an "essay workshop" in class on December 2nd during which you'll read and provide feedback on your peers' draft papers. Your "big questions" paper will contribute 30% of your overall course grade and is due at the start of the final class session on December 9th.

Academic Integrity

Please familiarize yourself with Vanderbilt's undergraduate honor policy, http://is.gd/eBvOV. I'm encouraging a lot of sharing and collaboration in this course, but your work on your essay assignments should be your own. Please be careful not to plagiarize. The Undergraduate Honor Council has a very helpful guide to understanding plagiarism, http://is.gd/eBw3O, and the Writing Studio has a great set of resources on working with sources in academic writing, http://is.gd/eBw5Q. We'll spend some class time exploring plagiarism and academic integrity more generally.

If your life is falling apart and you are tempted to plagiarize to save time or get a good grade, please see me instead. I would rather grant you an extension than send you before the Honor Council for plagiarism—but I will send you to the Honor Council if it comes to that.

Getting Help

If you have questions about any aspect of the course, feel free to come by my office and ask me for help. My regular office hours are listed above. You do not need an appointment to see me if you stop by during my office hours. If you cannot make my office hours in a given week, you are free to contact me to schedule an individual appointment. You are also welcome to email me any questions you have.

For help in finding and evaluating the quality of potential resources for your essay assignments, you can ask me or consult with librarian Carlin Sappenfield (http://is.gd/eBweB) in the Stevenson Science and Engineering Library. Carlin will visit our class in late September to orient you to the Vanderbilt Library and its resources.

Also, you're welcome to schedule an appointment at the Writing Studio for additional help. The Writing Studio offers one-to-one assistance with all aspects of writing at any stage in the writing process. I strongly encourage you to make use of this campus resource. See their website, http://www.vanderbilt.edu/writing/, for more information.

Grading

Your assignments in this course will be weighted according to the following chart to yield a numerical score.

Participation	15%
Problem Sets	30%
Essay #1 – Opinion Paper	10%
Essay #2 – Expository Paper	15%
Essay #3 – "Big Questions" Paper	30%

Your numerical score will be converted to a letter grade according to the following scale.

Score	Grade	Score	Grade
93-100	A	73-76	C
90-92	A-	70-72	C-
87-89	B+	67-69	D+
83-86	B	63-66	D
80-82	B-	60-62	D-
77-79	C+	0-59	F