Math 115F Fall 2012

Cryptography

The History and Mathematics of Codes and Ciphers

Tuesdays & Thursdays
9:35-10:50 a.m.
Stevenson Center 1120

INTRODUCTION

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 affected history, technology, and culture—and continue to do so.

COURSE GOALS

- To understand and appreciate the ways in which codes and code breaking have affected history, technology, and culture
- To understand and apply important concepts and techniques from abstract mathematics used in classic and modern cryptography
- To improve skills in communicating in writing technical information and opinion- and evidence-based arguments
- To gain proficiency in creating and breaking simple codes and ciphers

INSTRUCTOR

Derek Bruff, PhD
Director, Center for Teaching
Senior Lecturer, Mathematics

Contact:
derek.bruff@vanderbilt.edu
@derekbruff (Twitter)
615-322-7290 (Office)

Office Hours:
Mondays 3-4
Wednesdays 4-5
Thursdays 12-1

TEXTS

The Code Book by Simon Singh
(Anchor, 1999)

Cryptonomicon by Neal Stephenson
(Avon, 1999)

Little Brother by Cory Doctorow
(Tor, 2008)

Photo: "The Key of my mind," Daniele Margaroli, Flickr (CC)

COURSE BLOG

http://derekbruff.org/blogs/fywscrypto

The course blog will be the online "home base" for the course. I'll use the blog to post course information and resources. And you'll use the blog to share your thoughts about the course material with each other—and anyone else on the Internet who is interested. Each week I'll give you a blogging assignment, asking you to respond to questions about the week's reading assignment (before we discuss it in class) or write about some other topic.

Your blog contributions will be graded, but mostly on effort. I'm not expecting highly polished pieces of writing on the blog. Instead, the blog is a space where you can play with and test out your ideas about cryptography as they evolve during the course—and learn from your peers as you read and respond to their posts. The ideas and questions you and your peers surface on the blog will likely feed into longer, more formal writing assignments in the course.

SOCIAL BOOKMARKING

http://groups.diigo.com/group/fwyscrypto

You'll need to sign up for an account on the social bookmarking site Diigo and join the group "Math 115F: Cryptography" I've set up. Each week I'll give you a social bookmarking assignment, asking you to seek, find, and bookmark online resources relevant to the course, saving them to the Diigo group so we can all access them easily. Your bookmarks will be graded on effort: If you bookmark a resource that fits the parameters of the assignment by the assignment deadline, you'll get full credit.

I'm asking you to bookmark cryptography resources for two reasons: One is that doing so will give you a chance to make connections between the content of this course and other interests of yours, both academic and personal. The other is that by sharing interesting resources via Diigo, you'll help enrich the learning experience for all of us (including me). I think you'll also find that resources you and your peers share via Diigo will come in handy for the final research assignment in the course.

PROBLEM SETS

In order to learn how to create and break ciphers and to understand the mathematical aspects of cryptography, you'll need to work with ciphers and do some math. To that end, 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. Your work on the problem sets will be graded, and 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. You're also encouraged to ask me for help with problem sets, via email, office hours, or appointment.

MATH EXAM

Yes, there will be a test in this course. It is a math course, after all. I'll give you an exam later in the course covering the mathematical aspects of cryptography discussed in the course. This will give me the chance to evaluate your understanding of the mathematical concepts and techniques you'll be practicing on the problem sets.

**The U-505 Enigma Machine,
Chicago Museum of Science & Industry**

PAPER #1 – REACTION PAPER

In this paper, you'll be asked to respond to one of several articles on cryptography that I'll provide for you closer to the due date. Your paper should draw primarily on your personal experiences and perspectives, supplemented by some fact-checking as appropriate. This paper is an opportunity to surface your opinions about one of the big questions in this course and take some ownership of those opinions. It's also an opportunity for your to practice your argumentation skills without having the added complexity of integrating and responding to multiple sources and references.

Your paper should be between 750 and 1000 words in length, and it should use American Psychological Association (APA) formatting for citations and references. This essay will be graded on both content (including the relevance and complexity of your response) and clarity (including the appropriateness of your writing voice to academic writing). After you submit your paper to me and I've graded it and given you feedback, you'll be required to revise your paper and resubmit it. Your final grade on this paper will be the average of the two grades (before and after revision).

PAPER #2 – EXPOSITORY BLOG POSTS

In this paper, you'll describe the origin, use, influence, and mechanics of a code or cipher of your choice. There are many codes and ciphers we won't have time to explore in detail in this course. This paper will provide you with a chance to explore a piece of the history of cryptography that interests you personally—and to share that exploration with a very big audience.

Your "paper" will take the form of two blog posts: One post, between 450 and 500 words, focusing on the history of your code or cipher will appear on the blog Wonders & Marvels (www.wondersandmarvels.com), a history blog edited by Vanderbilt professor Holly Tucker. A second post, between 750 and 1000 words, describing the mechanics of your code or cipher (enciphering, deciphering, decryption) as well as any associated mathematics, will appear on our course blog. Both blog posts will be graded on content and clarity, with the two grades averaged to yield your final grade on this assignment.

PAPER #3 – "BIG QUESTIONS" PAPER

For your final assignment, you'll be asked to focus on important questions about the ways in which cryptography has affected history, culture, and technology. You'll pose a significant question about the role of cryptography in human affairs, suggest answers to that question, and provide evidence for your answers. In this paper, you'll draw on the argumentation and explanatory skills you practiced in the first two papers, adding to that mix your research skills.

Your paper should be between 3000 and 3500 words in length, and it should use APA formatting for citations and references. The paper will be graded on the strength and clarity of your arguments.

ACADEMIC INTEGRITY

Please familiarize yourself with Vanderbilt's Honor System. I'm encouraging a lot of sharing and collaboration in this course, but your work on your paper assignments should be your own. Please be careful not to plagiarize. The Library has a very helpful guide to understanding plagiarism (http://is.gd/VCoZcq), 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.

Antipodes by Jim Sanborn
Photo by Craig Moe, Flickr (CC)

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. Please allow for up to 24 hours for a response, however, since (a) I'm not on email 24 hours a day and (b) I get a ton of emails. You might get a quicker response if you contact me through Twitter, where my handle is @derekbruff. If you can ask your question in under 140 characters and I can answer it in under 140 characters, chances are, I can respond quickly!

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 this fall 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 (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.

Course Blog	10%
Social Bookmarking	5%
Problem Sets	15%
Math Exam	15%
Paper #1 – Response Paper	10%
Paper #2 – Expository Posts	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

BPQAK TCMTM ILAGW CWVTQ VMBWI BEMMB EPMVG WCZMI LQBGW CTTBP QVSQA VBBPI BVMIB APMIL
NWZBE QBBMZ KWUIV LNQVL IVIUM QBAKQ XPMZM LJMTW EIVIO ZIUQA BPMOI UMWAQ VKMBZ IVAXW
AQBQW VAABC UXUWA BWNGW CNWTS APMZM AIPQV BVBPQ AUQVM ZUQOP BJMIP WIF

AMHAJEBOTLES