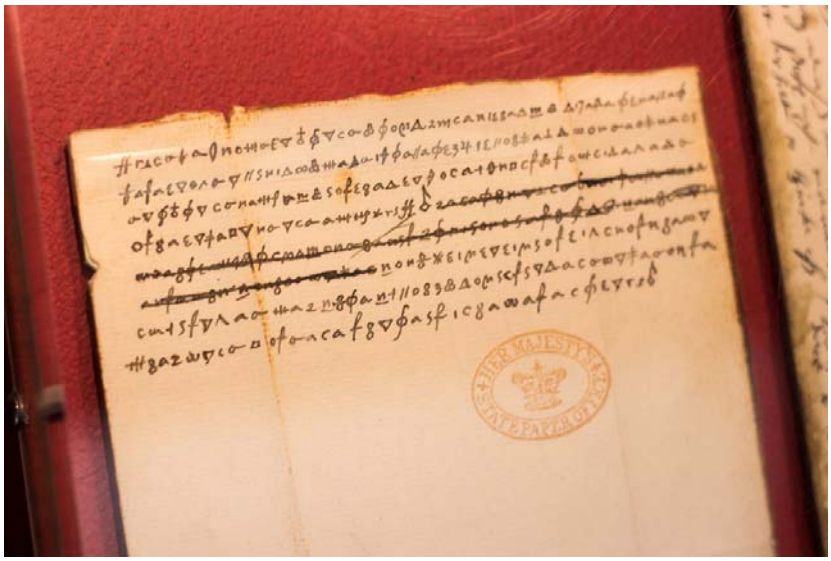


Math 1111 Fall 2018

Cryptography

The History and Mathematics of Codes and Ciphers

MWF
12:10-1:00 p.m.
Stevenson 1313

INTRODUCTION

Mathematics has long played key roles in both sides of the cryptography "arms race," helping cryptographers devise ever more complex cipher systems while also providing tools to cryptanalysts for breaking those ciphers. During World War Two, this battle between code makers and code breakers led to the construction of the first digital computers, which in turn ushered in an information age where cryptography makes information security possible—but not certain, given surveillance efforts by governments and others. This course will provide an understanding and appreciation of the ways codes and code breaking have affected history, technology, and privacy—and continue to do so.

COURSE GOALS

- To gain proficiency in creating and breaking simple codes and ciphers
- 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 evidence-based arguments

INSTRUCTOR

Derek Bruff, PhD
Director, Center for Teaching
Principal Sr. Lecturer, Mathematics

Contact:
derek.bruff@vanderbilt.edu
@derekbruff on Twitter
931-442-5114 on Signal

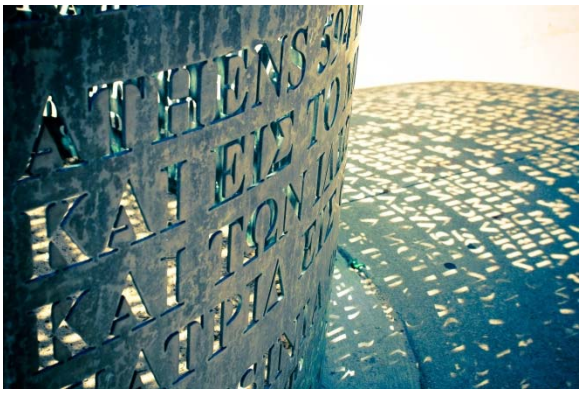
Office Hours:
Mondays 2-3
Wednesdays 3-4
Thursdays 11-12
and by appointment

TEXTS

The Code Book by Simon Singh (Anchor, 1999)

Little Brother by Cory Doctorow (Tor, 2008)

Photo: "Her Majesty's State Paper Office," Derek Bruff, Flickr (CC BY-NC)



Iacto by Jim Sanborn
University of Iowa campus

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. Every week or so, I'll give you a blogging assignment, asking you to respond to questions about a reading assignment (before we discuss it in class) or write about some other topic.

Your blog contributions will be "lightly" graded. 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 1111: Cryptography" I've set up. I'll ask you to seek, find, and bookmark online resources relevant to the course—particularly the current events portion of the course—and save them to the Diigo group so we can all access them easily.

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).

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

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.

Enigma Machine
International Spy Museum, DC

PAPER #1 – LITTLE BROTHER

In this paper, you'll be asked to make an argument based on your reading of *Little Brother* by Cory Doctorow. You'll have to decide what argument you want to make. You might make an argument about security or privacy, responding to such arguments made by characters in the novel. You might question the use of the terms security, privacy, and surveillance. You might critique the actions of one of the main characters in the novel, or the rhetorical approach of the author. Or you might go in some other direction that interests you.

Your paper should be between 750 and 1,000 words in length. This essay will be graded on both content (including the relevance and complexity of your argument) 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 grade on this assignment will be the grade given to your revised paper—which will be no more than one letter grade away from the grade on your first draft.

PODCAST – HISTORICAL CRYPTO

https://soundcloud.com/user-302864534

In this audio project, 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 project 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 an audience beyond the course.

Your project will take the form of a 10-to-15-minute episode of a class podcast on the history of cryptography, *One-Time Pod*. Your podcast episode should be interesting and accessible to a general audience, which means you'll need to find ways to engage your audience and to explain the mechanics of your chosen code or cipher (enciphering, deciphering, decryption) in ways your audience can understand.

You'll be asked to submit a full script for feedback prior to recording your episode, as well as show notes and a producer's statement for your finished episode.

PAPER #2 – SURVEILLANCE VS. PRIVACY

For your final paper, you'll tackle the cryptography question of our time: surveillance vs. privacy. Should our government be given wide latitude to use electronic surveillance in the interests of national security, even if that means citizens' privacy is not always respected?

This is a question we've explored in every offering of this course. Thanks to Edward Snowden's 2013 revelations about the National Security Agency, it's now part of our national dialogue. We will explore this question from many angles this semester. This paper is your opportunity to spend time thinking critically about the question and crafting a well-supported answer.

Your paper should be between 1,500 and 2,000 words in length, and it will be graded on the strength and clarity of your arguments, as well as the quality of your sources. As with the first paper assignment, you will be required to submit your paper for a grade and feedback, then revise and resubmit your paper. Your grade on this assignment will be the grade given to your revised paper—which will be no more than one letter grade away from the grade on your first draft.

Photo: "Mystery Patch," Derek Bruff, Flickr (CC BY-NC)

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. 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.

ACCESSIBILITY

This class respects and welcomes students of all backgrounds, identities, and abilities. If there are circumstances that make our learning environment and activities difficult, or if you have medical information that you need to share with me, please let me know. I am committed to creating an effective learning environment for all students, but I can only do so if you discuss your needs with me as early as possible. I promise to maintain the confidentiality of these discussions. If appropriate, also contact Vanderbilt's Student Access Services to get more information about specific accommodations.

PRIVACY

The Family Educational Rights and Privacy Act (FERPA) is a federal law designated to protect the privacy of a student's education records and academic work. In this course, we will be working with third party applications online (i.e. blogs, social bookmarking services, podcast platforms). It will be your responsibility to read the privacy documentation at each site. You will be allowed to use a pseudonym or alias in order to maintain your privacy as long as you notify me of that username. The online component is required as part of this course. I will take your continued enrollment in this course as consent regarding this policy. If you still have concerns, please contact me as soon as possible to discuss your options.

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're also welcome to email me any questions you have. Please allow for up to 24 hours for a response. You might get a quicker response if you contact me through twitter, where I'm @derekbruff.

GRADING

Your assignments in this course will be weighted according to the following chart.

Online Participation	10%
Problem Sets	15%
Math Exam	20%
Paper #1 – Little Brother	10%
Podcast – Historical Crypto	20%
Paper #2 – Security vs. Privacy	25%

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