Math 1111 Fall 2015

Cryptography

The History and Mathematics of Codes and Ciphers

MWF
12:10-1:00 p.m.
Stevenson Center 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 opinion- and evidence-based arguments

INSTRUCTOR

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

Contact:
derek.bruff@vanderbilt.edu
@derekbruff on Twitter

Office Hours:
Mondays 3-4
Tuesdays 3-4
Thursdays 10:30-11:30
and by appointment

TEXTS

The Code Book by Simon Singh (Anchor, 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. Every other 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).

CRYPTOGRAPHY TIMELINE

http://derekbruff.org/timelines/cryptotimeline.htm

When I offered this course in 2010, my students built an online timeline of the history of cryptography. This semester, we're going to build on their work, making an even better timeline, one that will directly inform your second paper assignment. Details to come.

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.

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

PAPER #1 – REACTION PAPER

In this paper, you'll be asked to read and respond to one of several articles on cryptography that I'll provide for you. You'll need to summarize the thesis and argument of the article you select, then respond by agreeing or disagreeing with the article's thesis and defending your position with your own argument. 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 1,000 words in length. 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 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.

PAPER #2 – LESSONS LEARNED

In this paper, you'll identify one or more lessons about keeping secrets drawn from historical examples of codes and ciphers—examples we've read and discussed, as well as ones we haven't. This paper will give you the chance to practice your descriptive writing, while using examples and stories to support a central argument.

Here's where that timeline will come in handy, by providing leads for examples you could use in your paper. Also potentially useful: the essays on historical codes and ciphers written by students in the 2012 and 2014 offerings of this course, available on the course blog. You'll need to do some original research, too.

Your paper should be between 1,000 and 1,250 words in length. It will be graded primarily on the quality of your examples and how well you connect your examples to your thesis.

PAPER #3 – PRACTICAL CRYPTO

In this paper, you will identify and describe one way that cryptography is (or could be) relevant to the digital life of a college student in 2015. You might address one of the ways that cryptography is embedded in the computer systems we already use (e.g. how credit card information is encrypted by websites) or explain how to better protect one's online privacy by adopting new practices (e.g. sending and receiving encrypted emails). Your chapter will have an expository component, in which you explain cryptographic and/or mathematical processes in ways a fellow student can understand, and an argumentative component, in which you make the case for why a fellow student should care about the topic you've chosen.

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 effectiveness of your technical explanations. The best papers will be posted to the course blog and shared with the Vanderbilt student community.

PAPER #4 – SECURITY VS. PRIVACY

For your final paper, you'll tackle the cryptography question of our time: security 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.

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.

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.

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

WRITING STUDIO

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.

Online Participation	10%
Problem Sets	15%
Math Exam	15%
Paper #1 – Reaction Paper	10%
Paper #2 – Lessons Learned	10%
Paper #3 – Practical Crypto	20%
Paper #4 – Security vs. Privacy	20%

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]