FYS-146 Cryptography: The Science of Secrecy Fall 2019

Darren Glass
Glatfelter Hall 215A dglass@gettysburg.edu 337-6635

Office Hours: Mondays 1-3, Wednesdays 10-12
I am also available by appointment.

Course Meetings and Information

Tuesdays and Thursdays, 1:10-2:25pm, Glatfelter 203

Course Description and Goals

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that the National Security Agency can frequently find ways around it. - Edward Snowden

For thousands of years, people have been sending secret messages to one another. The ability to communicate secretly has always been important for military and security reasons, and has become even more important in the age of the internet, e-commerce, and electronic voting. In this course, we will look at some of the ways that mathematics has been used to communicate in secret in the past and ways that it may be used in the future ranging from the ancient Egyptians and Romans to World War II to the possibility of quantum computers. We will also discuss the ways that these technological advancements have affected society and vice versa.

More specifically, by the end of the semester you should:

- Understand how abstract mathematics can be used in a very practical setting.
- Understand some of the basic topics of number theory.
- Learn about the role that cryptography plays in today's society as well as the ways in which it has influenced history.
- Strengthen your ability to read and communicate in an effective manner.

This course will help you satisfy two of the college's curricular goals: Science Technology and Society (STS) and Quantitative Inductive and Deductive Reasoning (QIDR).

Course Materials

Textbook: *The Code Book* by Simon Singh
Other readings available through the Moodle course website

Grades

Grades will be determined according to the following table.

Attendance and Participation	20%
Quizzes	10%
Homework	40%
Final Project	30%

Attendance and Class Participation: Attendance in FYS 146 is required. You are expected to actively participate in class by asking questions, making comments, working on the assignments, and sharing your solutions with others. You are also expected to come to class prepared, having done any assigned reading ahead of time.

Quizzes: Most weeks there will be readings that you are assigned to do before class begins. In order to help guide you through the readings (and to encourage you to actually do them) we will typically have short online quizzes that will be administered through the Moodle site. These will be due at noon on the day of class. They will generally be *open book*, but you are *not* allowed to discuss them with any of your classmates before class begins. They are untimed but you are only allowed to submit answers once.

Homework: There will be regular homework assignments which will take a variety of forms. Some of them will be problem sets, some will be short essays, and some will be reading assignments. The written assignments are to be handed in at the beginning of class on the day they are due. Late homework will not be accepted for any reason (though early homework will be).

Unlike quizzes, you are generally encouraged to discuss homework with each other unless specifically told otherwise. However, on all assignments you must turn in your own work and not the work of your co-conspirators. If you aren't sure exactly where the boundary lies, please ask me rather than make assumptions. All work will be graded not only on correctness, but also on how well you communicate and explain your answers.

Final Project: In this course, you will get the opportunity to explore some area which interests you in great depth. The 'product' of this exploration will involve a brief presentation to the class as well as a 12-15 page paper. More details on the project will come in a few weeks

While there will be no final exam in this course, we will use the scheduled Final Exam timeslot (Saturday December 14th from 8:30-11:30am) for a class activity that you must attend, so please make your travel arrangements accordingly.

Some Questions We Will Consider In This Course

- Is it possible for two people across the country from one another to agree on a secret codeword without ever communicating in person?
- Is it possible to prove to your bank that you know your PIN without ever telling it what your PIN is?
- Why do I believe it is safe to send my credit card number to Amazon?
- Is it possible to encrypt music so that a person can decrypt it if they purchase the file but they cannot share the decrypted version with anyone else?
- Can I encrypt a message and send it over the internet in such a way that I can tell if anyone has eavesdropped on the message?
- How can we sign email messages in a way that cannot be forged?
- Should electronic voting machines give voters 'proof' of who they voted for? What would this even mean?
- Is it better (either ethically or in terms of security) to keep your method of encryption a secret or to make the method public and only keep the key a secret?
- What are some of the ways in which cryptography has changed the course of world events?
- Should the government have a 'backdoor' into breaking codes?
- More generally, what *is* the government's role in cryptography?
- Has the advent of computers made secrets easier or harder to keep and communicate?
- Is there a way that your cell phone and your friend's cell phone can figure out if you are close to each other without announcing your location?