# Math 441: Cryptography

Spring 2015

## Basic information

**Professor:** Adam Groce, agroce@reed.edu
**Class schedule:** Class meets Monday, Wednesday, and Friday at 3:10 in Physics 122.
**Office hours:** I hold office hours (in Library 390) Monday 1-2, Wednesday 4-5, Thursday 3-4, and Friday 1-2. I can also meet with you by appointment if those times are bad or if you would like to discuss something privately. You are also welcome to stop by other times, but I might be busy.
**Website:** The course website is http://people.reed.edu/~agroce/math441/. Homework and other information will be posted on that website.
**Textbook:** The textbook is *Introduction to Modern Cryptography* by Jonathan Katz and Yehuda Lindell (second edition).

## Course overview

"Cryptography" was historically the art of sending secret messages, but that understanding of the term is now outdated. The cryptography we will be studying in this class has established itself as a fully modern science (or branch of mathematics, depending on your definitions). Unlike the cryptographers of earlier eras, we will be learning formal definitions of security and writing proofs that protocols satisfy those definitions.

Cryptography is also no longer limited to secret messages. It deals generally with all attempts to secure information, computer systems, and protocols against adversarial interference. Nevertheless, we will be starting with sending secret messages, building cryptography from the ground up. As we get later into the course, some more recent cryptographic tools for more complicated tasks will be discussed as well.

Cryptography is incredibly important today. Nations worry about foreign nations using cyber attacks as a threat to national security. Private individuals, corporations, and law enforcement worry about organized crime and large-scale criminal threats and terrorist organizations. Individuals worry about untrustworthy or negligent businesses abusing (or allowing others to abuse) their personal information. Cybersecurity is, in short, a huge concern. Cryptography *is only one part* of cybersecurity, but it is a crucial component, and it is therefore extremely important to learn.

It is important to remember, however, that cryptography is an important branch of theoretical computer science and mathematics and would be even if its practical importance were greatly reduced. Complexity theory studies what problems can be solved efficiently by computers, and cryptography is best understood as a part of complexity theory. We want to know what computers can and cannot do efficiently, and whether it is possible to encrypt a message in such a way that there is no efficient decryption is a natural question to ask. In this class we will be motivated by both practical concerns and theoretical interest.

## Coursework and grading

**Homework:** There will be regular homework assignments throughout the course. Late homework will be accepted, but will be greatly penalized in grading. You are allowed and encouraged to work with others on the homework, but the final result must be your own. Remember, the most important consequence of the homework isn't the grade but rather the learning and understanding that it gives you. If you think working with someone else is reducing your need to struggle through the problems and wrestle with them sufficiently, you will probably be better off working on your own.

**Tests:** There will be two take-home tests during the course and an in-class final. These will be the main determinant of your grade, with the final worth slightly more than each of the other tests.

## Other policies

**Attendance:** I trust you to make decisions regarding attendance for yourself. I think you should attend every class because I think that is important to learning the course material, but it is that learning of the material on which you will be judged, not the attendance directly. I will, however, assume everyone is in class, and if you miss class you should make sure to talk to someone else in the class to find out if you missed any announcements, schedule changes, etc. If you miss a test you will receive no credit unless your absence is excused. Some excuses (such as illness) will require documentation (such as a doctor's note). I expect that if you will be missing class for an excusable but predictable reason (say, a religious holiday) that you inform me before the absence. I will not excuse absences after the fact for reasons that were known about ahead of time.

**Academic integrity:** You are allowed to work with classmates on the homework, but you should write on the homework the names of anyone you collaborated with. You must also write up the actual solutions on your own, and you must actually do the homework together – copying and collaborating are very different things, and I expect you to know the difference. Take-home tests must be done entirely on your own with absolutely no discussion with others, and with no materials aside from those explicitly allowed. I take academic integrity very seriously, and I will not hesitate to report inappropriate behavior.

## Advice

**Don't procrastinate!** The homework and tests will require clever thought and puzzle-solving. That sort of thing takes time. Look at homework and tests immediately, even if you aren't going to put lots of work in them until later. Being able to think things over as you go about the rest of your life is surprisingly helpful. Also remember that it can be tricky to explain what you are doing and make your solutions clear. Allow time to spend getting the writing correct, in addition to the math.

**Ask for help!** This class is not supposed to be easy, and I'm not going to assign tons of homework. I expect you at this point in your academic career to know when you understand something and when you don't. If you are confused (even about something small) it is much better to ask for help right away – it is much harder to back and fix things later.

**Use the textbook!** The textbook for this class is very good, and we'll be following it reasonably closely. I will only *require* reading when it covers material I will not be covering in class, but I highly recommend you read much more than that. It is always good to see multiple explanations of important concepts.

**Have fun!** This class will contain a lot of cool puzzles, ingenious solutions, and useful information. It should be fun and interesting to study. Don't get so caught up in the work that you can't take a step back from time to time and enjoy it.