Instructor: Nathan Pflueger (pronounced "fleeger")
email: npflueger@amherst.edu
office: SMUD 401

office hours: (tentative)

Tuesday	1:45-3:15
Wednesday	1:45-3:15
Friday	1:00-2:00
(or by appointment)	

Times and locations:	MWF	11:00-11:50	SMUD 206	
	Tuesday	11:30-12:20	SMUD 206	**Note different Tuesday time!**

What are office hours for? You can come to scheduled office hours for any reason whatsoever. You can bring any questions you have, including vague questions about the big picture. You can also come with no questions; there is a desk in my office and several just outside where you are welcome to work, meet your classmates, or listen to other conversations. Office hours are the best way I have to learn about you and how you're doing in the course and the college, so please visit!

Course webpage: `http://npflueger.people.amherst.edu/252/`

Textbook: *An Introduction to Mathematical Cryptography,* **Second Edition**, by Hoffstein, Pipher, and Silverman. If you are on the Amherst network, you can download the entire book for free, buy a discounted ($25) paperback copy, at the following link. **Buying a copy through SpringerLink is almost certainly cheaper than other sources.**

`https://link.springer.com/book/10.1007/978-1-4939-1711-2`

If you are off-campus, you should first look up "Springerlink" (one word) in the Amherst College library catalog, and follow the link in the catalog entry, to get full access (including the discounted price).

Goals and topics: This course has four main goals.

- Explain the **mathematical details of the most important public-key cryptosystems and related algorithms** in use today, as well as precautions necessary to protect these systems against certain attacks (more specifics below).
- **Introduce and illustrate the main concepts of abstract algebra** in an applied setting. In this course, we'll see examples of groups, rings, and fields, but at less depth and abstraction than in Amherst's core algebra course, Math 350. The course is designed for students who have not yet taken Math 350. However, students who have taken Math 350 will see several new aspects of algebra, especially algorithmic issues.
- **Develop basic programming skills**, and give students practice solving mathematical problems and performing mathematical experiments using code. We will use Python for all coding in the course. No prior experience is necessary; many past students have gained their first programming experience in this course and found in extremely useful in future employment and coursework.
- **Problem solving.** Mathematics is a versatile and useful discipline largely because it trains you to problem-solve in novel situations. Much of the challenge, and satisfaction, of doing mathematics is learning to rely on your own ideas, and placing faith in the soundness of your own reasoning, when solving problems unlike those you've seen before. Therefore I will often challenge you to adapt ideas from class to novel situations to train these skills.

Caution: Math 252 is first and foremost a math course, and there are many aspects of Cryptography (indeed, the majority of it!) that we will not have time to discuss. Students are encouraged to consider the Computer Science department's courses on cryptography and security to see other aspects of the subject. In particular, always remember that **real-world cryptography applications are only as secure as their weakest link, which is usually not the mathematics**! So you should certainly learn about security more broadly, and work in a team with experts from several different backgrounds, before trying any of this in the real world.

Course topics: The unifying theme of the course is the construction of the most commonly-used **public-key** cryptographic algorithms, and certain attacks against them that must be anticipated. We will cover mathematical problems underlying public-key ciphers and digital signatures, as well as algorithms to solve them. Topics include:

1. The discrete logarithm problem and Diffie-Hellman key exchange.
2. Integer factorization and the RSA cryptosystem.
3. Digital signatures.
4. Elliptic curves and related cryptosystems.
5. The NTru lattice-based cryptosystem.

Throughout the course, we will discuss both *cryptography* (encryption and signing algorithms) and *cryptanalysis* (algorithms to break cryptosystems).

Expectations: You are expected to attend class every day, arrive on time, and be respectful. You are expected to know about any announcement I make in class. You should expect to spend at least eight hours studying and working on problem sets outside of class each week. Of that time, I recommend that you spend at least two hours reviewing your notes, the textbook, and previous assignments. Distributing your practice and review throughout the semester will be much more effective than concentrating your review and studying right before exams or due dates.

If you are new to programming, working on that skill will account for a lot of your time (but it will pay very high dividends, as my previous students repeatedly tell me!). Some assigned problems will be quite challenging, and **you do not need to complete all problems to earn a good grade in the course**. However, I recommend attempting all assigned problems.

You will sometimes be expected to take the initiative in looking up information about the tools you need, especially when programming. If you can't find what you're looking for, though, I will of course be happy to help.

The nature of a course like this, which connects to several different disciplines, is that some students may have an easier time with the material than others (e.g. if they already know how to program, or already know some abstract algebra). If it seems like the course is easier for some of your classmates, do not be discouraged! This just means that you have a lot to gain from the course. I hope that by the end of the course all students will reach the same place, and you will all be

versatile and valuable problem-solvers wherever you take your skills from this course.

Prerequisites: A course with proofs, such as Math 220/221 or 271/272, or instructor permission. Prior programming experience is **not** required, nor is prior coursework in abstract algebra.

Structure and grading: There will be weekly homework assignments, two midterm exams, and a final exam. The dates of all exams, and their share of your final grade, are listed below. There is no set curve or grading cutoffs, but most likely the median grade will be around a B.

Written homework	20%	
Programming homework	20%	
Midterm 1	15%	Monday 3/9 in class
Midterm 2	15%	Monday 4/27 in class
Final exam	20%	Date/time TBA
Your best exam	10%	(midterm or final; added to its original weight)

Exam dates: The midterm dates are listed above. **Put them on your calendar now**. The final exam date is set by the registrar, and should be available on the registrar's website partway through the term. The final exam will be sometime in the week of May 11-15. **Do not schedule travel before the end of exam week unless the final exam date has been determined by the registrar**. All students are expected to be present for the final exam.

Homework: Homework will be **due at 10pm**, typically on Wednesdays, via an online system called Gradescope. To allow for technical difficulties or other last-minute issues, Gradescope will allow you submit homework after the deadline, however your score will be reduced by 2% per hour after the deadline (scaled continuously, e.g. being fifteen minutes late results in a 0.5% deduction). Please try to turn in your work by 10pm (I don't want to be responsible for lost sleep!), but don't worry about short delays.

I do not grant extensions for any reason. However, to compensate for illness and other emergencies, your **lowest two homework scores will be dropped**. If you cannot make a due date due to an emergency, my advice is to skip the assignment, but study and understand the problems when you have time, and focus on keeping up with the new material in the course. You do not need to apologize or provide any reasons for skipping an assignment or turning it in unfinished; please choose what is best for your time, health, and well-being.

Missed exams: There are no make-up exams. If you must miss an exam due to a medical or other emergency, your final exam score will be substituted for that exam score in your course grade. If you are ill or an emergency arises near an exam, notify me as soon as possible. Any medical emergencies must be confirmed by your class dean. If you have a time conflict with an exam, notify me as soon as possible, and **at least one week in advance** (exam dates are listed above).

Accommodations: I strive to make this course welcoming to all students. If you would like to discuss your learning needs with me, please schedule a meeting so that we can work together to support your academic success. Anyone who may require an accommodation based on the impact of a disability should contact me to make arrangements. I rely on Accessibility Services for assistance in verifying the need for accommodations and developing accommodation strategies, so you should contact them at `accessibility@amherst.edu` or 413-542-2337. If you require accommodations on exams, please arrange this with me at least one week in advance.

Intellectual responsibility:

- **Homework:** Mathematics is a collaborative subject; open and generous communication is one of its core values. Therefore you are strongly encouraged to work with other students, ask many questions, and learn from as many people as possible. However, you must write up the solution yourself. **All your submitted work must be your work, written in your own words**. Copying solutions from other students, solutions manuals, or online databases is plagiarism; such copying will result in a 0 on the assignment and will be reported to Community Standards. You are also expected to **list each person your worked with** on the front of your homework assignment.

- **Exams:** You will be allowed **one page of notes (front and back)** for each exam. No calculators or other aids are permitted. Cell phones should be stowed out of sight during exams. Use of cell phones or other devices during the exams will be grounds to receive a 0 on the exam. You are bound by the college's honor code, and all work must be entirely your own on exams.

For both homework and exams, I reserve the right to give no credit for any work that appears suspicious.

Tips:

- **Come to office hours!** I am happy to answer your questions and also talk about the course in general. Even if you don't have specific questions, you can come to review material, listen to other students' questions, or just to chat.
- **Review early and often.** You should constantly be looking over your notes and keeping the big picture in mind. Arrive each day in class with a sense for where we are.
- **Keep a positive attitude.** Learning is a long process, and you will struggle often. Remember that struggle and difficulty is how you grow. Don't be afraid to talk to me about whatever difficulty you're facing. I want all of my students to be successful and deepen their mathematical skill and appreciation.
- **Practice, practice, practice.** Start early on homework, and let hard problems simmer in your head. Try unassigned problems in addition to homework. Read the book, and **read actively**, always questioning, summarizing, and interpreting what's on the page.

Resources and additional help: Be sure to take advantage of office hours, and your peers, to answer questions and think through the material. The staff at the **Moss Quantitative Center** in the Science Center will host regular help hours, and are available for individual appointments. We also have a Math Fellow for the course, who will hold regular office hours, host exam review sessions, and be available to help with LaTeX. The schedule of these help hours will be posted on the course website once they are set. Finally, some students may benefit from a peer tutor, if they are already using the available help hours and require additional support. Peer tutoring is a limited resource, so please speak with me about it before requesting tutoring.

email policy: The best way to reach me with course questions (besides office hours) is by email. I generally reply to email within 24 hours. However, **I often do not reply to email on weekends**. I will also reply less quickly on Thursdays, which is the day I devote primarily to research.