Math 318 – Cryptography (Summer 2021)

Instructor: Kevin Woods. Call me Kevin! (he/him)

Contacting me: Kevin.Woods@oberlin.edu or 443-695-1681 (mobile). Email is better for involved or less important questions; texting is better for quick, time-sensitive questions.

Lectures: MWF 1:30-2:20pm, Craig Lecture Hall (Sci Ctr N292).

Google Drive:

I will post assignments and other material in the course Google Drive folder. You will need to have regular access to this and to your Oberlin email.

Office Hours:

- Monday 11:10am-12pm, Tuesday 12:30-2:30pm, Wednesday 2:30-3:30pm, Friday 12:30-1:20pm. Or you can make an appointment via email.
- The **Tuesday 12:30-2:30pm office hours will be in King 203** to encourage lots of students to come and talk to each other. The other office hours are in my office, King 220B. . If you'd like to meet over zoom, I'm happy to: please email me in advance.

Textbook:

- *An Introduction to Mathematical Cryptography*, by Hoffstein, Pipher and Silverman, **2nd edition** (2014). The first edition is fine, but section numbers will be annoyingly different.
- You can download a free pdf of the textbook from SpringerLink, through our library; go to this link, type in your last name and library bar code number, and click the "Download book PDF" link.
- We will cover much of Chapters 1-4 and parts of Chapters 5, 6 and 7. I'll keep you updated about which sections we're currently covering.

Prerequisites:

- MATH 220 (Discrete Mathematics). The most important thing from Discrete is comfort with mathematical proofs and readiness for a 300-level math class. Even though the subject matter is very approachable, **this is a 300-level math class**: there will be challenging proofs, and things will sometimes get very abstract.
- Discrete also includes some basic modular arithmetic and number theory; we'll review everything you need from this, but we'll cover it quickly.
- You should also have some comfort with programming (if/then statements, arrays, loops, writing functions) as you will regularly write short programs for assignments. Prior or concurrent enrollment in CSCI 150 is more than sufficient.

Mathematica:

- I will often expect you to use Mathematica to work on problems. This will include writing short programs. You'll see examples in class, and I am very happy to help with implementation.
- Mathematica is available in every computer lab on campus, you can download a free copy for your own computer from cit, and it is available on both the Mac and Windows Virtual Computer Labs.

Learning Goals:

At the end of this course, students will:

- Have knowledge of a number of modern cryptosystems and a theoretical understanding of how to make and break them,
- Have experience thinking algorithmically about cryptography, including writing short programs.
- Have confidence proving statements and mathematically manipulating examples in number theory and cryptography.
- Have experience working with other students on mathematics (this one is up to you to work on).

Assignments and Grades:

- Your focus should be on **growth**, but grades are a fact of college life. **If I can see that you are working hard and seeking support, you will pass this class.** If you find yourself preoccupied with grades, consider taking it P/NE.
- Problem sets (40%, lowest two dropped).
    - The best way to learn the concepts in this course is to get your hands dirty! I hope you will work in groups on these, though your written solutions must be in your own words. This is also an opportunity to work on writing careful, clear proofs and explanations. Good mathematics is articulate mathematics! Explain things carefully and in complete sentences. Imagine that another student in the class who hasn't done this problem yet will read your solution: they should be able to understand it without having to ask you questions.
    - These problems will be graded strictly for how coherently written they are. Problem sets will be due approximately every Wednesday at 5pm, as a pdf via this google form.
    - Late Work: I generally do not allow you to turn problem sets in late. These go out to a grader, and so late work is logistically challenging.. Your lowest two grades will be dropped at the end of the semester, so if you have a busy week or are sick, it's often best just to skip that week's.
    - Honor Code: I encourage you to work together on the problem sets. Your solutions must be in your own words, however. Work on the problem together, and then go back home and write up your solution. In particular, you should never look at someone else's write-up before it is due.
- Three midterms (40% total, lowest score dropped).
    - The first two midterms will be take home exams, tentatively due Wednesday, June 23 and Wednesday, July 28. These will be open notes, and you'll get several days to work on them. You are not allowed to talk to anyone about these questions.
    - The third midterm will be in-class on Wednesday, August 18. You will be allowed something like a sheet of notes.
    - I want you to succeed, and everybody has bad days or weeks. **I'll drop the lowest exam score, as long as you put in a good-faith effort on all of them**.
- Final project (20%).
    - This will be a code-breaking challenge where you have to decrypt some messages. It is open notes, and you must work alone. It will be due Sunday, August 29 at 11am, via google form submission.

Support:

- You belong at Oberlin and you belong in this class. People arrive here with different experiences and backgrounds in mathematics. Put in the work, seek out support, and focus on self-improvement, and I promise you that **your mathematical skills will grow**. The rest of us are here to help, including:
- Me! Come by office hours, any time.
- Your peers! Working with other students helps everyone improve.
- Yourself! Your skills will improve best if you come at this with a growth mindset: embrace the challenge of this class, persist through difficulty, be inspired (not threatened) by the success of others, seek out support.
- If you have a disability of any sort that may affect your performance in this class, please consult with me and with Student Academic Success Programs (Peters 118). All requests for accommodation must go through that office.

COVID-19 Classroom Safety:

- Students and faculty who are fully vaccinated (two weeks past the final dose) are not required to wear masks in the classroom. It is recommended that unvaccinated students wear masks and maintain distance when possible.
- We are in a large lecture hall, with space to spread out as much or as little as you wish, masked or not (as you wish). I just ask that you respect everyone else's choices as we get used to the new policies.