Math 318 – Cryptography (Spring 2023)

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.

Class: TuTh 9:30-10:45am, Craig Lecture Hall (Sci Ctr N292).

Google Drive:

I will post assignments and other material in the course Google Drive folder.

Drop-in help sessions: Come individually, come in groups, come with questions, come to get started on the homework with other students around. Your choice! Showing up to one of these is a great way to find other students to collaborate with.

- Tuesday 12-1:30pm, Math Library (King 203, with me)
- Wednesday 12-1:30pm, Math Library (King 203, with Joe Sangiolo)
- Wednesday 7-8:30pm, Math Library (King 203, with Hannah Babe)

Other Office hours:

- Monday 9:30-10:30am, my office (King 220B)
- Tuesday 3:15-4pm, my office (King 220B)
- Thursday 12-1pm, my office (King 220B)
- If these times don't work, you can make an appointment via email.

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/NP.
- Your grade will be based on **weekly problem sets** and a **final project**. For the most part, you can and should work on the weekly problem sets in groups, but (in lieu of take home exams) there will be a problem or two on each problem set that I expect you to work alone on.
- I will drop the two lowest problem sets. Averaging the rest will determine your numerical grade, and this may be curved up to determine your letter grade. The final project counts as two problem sets and cannot be 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.
- Problem sets will be due approximately every Thursday at 2pm, submitted via gradescope.
- The final project will be a code-breaking challenge, due at the end of our schedule final exam time: Thursday, May 11 at 4pm. It is take-home, and you must work alone on it. There is no in-class final exam.
- Late Work: This is generally **not accepted**, because we have a complicated system of graders, and it is logistically difficult to deal with late work (later that afternoon will generally be ok if you ask in advance and don't make a habit of it). I drop two problem sets because I know that everyone has bad days or weeks, so it is perfectly ok to simply skip that week.
- 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. And there will generally be a clearly marked problem or two that you have to work alone on; treat these like take-home exam problems in typical classes.

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.
- The dedicated tutors! (Hannah Babe and Joe Sangiolo.) They will be holding dedicated drop-in hours to help.
- 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). I am committed to meeting the needs of all students in my class.
- **I want you to succeed, and I want to help you succeed.** Please let me know how I can help!