Math 318 – Cryptography (Spring 2025)

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: MWF 3:30-4:20pm, Craig Lecture Hall (Sci Ctr N292).

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

Problem 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 this is a great way to find other students to collaborate with. Either I or a dedicated tutor will be there to facilitate group work and give help:

- Sundays 2-4pm, King 327 (with Rosie McKusick)
- Mondays 7-9pm, King 327 (with Eliza Bomfim Guimaraes Giane)
- Tuesdays 2:30-4:30pm, King 203 (Math library, with me)

Other Office Hours:

- Wednesdays 1:30-3:20pm, King 203 (mainly for my other class, but you are welcome to come)
- 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.
- A pdf is freely accessible to Oberlin students, and I have placed a copy in our google drive folder.
- 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, using this google doc.

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 coding (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.
- I recommend installing it on a personal laptop, if at all possible, from CIT. It takes a little time, because you need to get an activation key, etc.
- Mathematica is also available in every computer lab on campus. People have also tried using our Virtual Computer Labs or Wolfram Cloud, though these have their own annoyances.

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**, a late-semester **exam,** and a **final project**.
- 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 midterm counts as one problem set, and the final project counts as two problem sets; neither can 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 Wednesday at 10pm, submitted via gradescope.
- The exam will be in-class on Monday, May 5. You will be allowed a sheet of notes.
- The final project will be a code-breaking challenge, due at the end of our scheduled final exam time: Friday, May 16 at 11am. It is take-home, and you must work alone on it.
- Late Work: I will give you until Thursday 10pm for problem sets, if you ask in advance and don't make a habit of it. After that, late work is generally not accepted, because it needs to go to the graders. 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. You should never go looking for the solution to a specific problem: for example, **don't read someone else's solution, search the internet or a book, or ask reddit/AI/etc**.

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! (Rosie and Eliza.) See the problem session times above.
- 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, communicate and advocate for yourself.
- If you have a disability of any sort that may affect your performance in this class, please consult with me and with the Office for Disability and Access. 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!