Course Policies
Prof. Shahed Sharif

Textbook and other materials. We will be using An Introduction to Mathematical Cryptography by Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman. A good supplementary text is A Course in Number Theory and Cryptography by Neal Koblitz. We will cover chapters 1–3, parts of chapter 4 (time permitting), and chapter 5 of Hoffstein, Pipher, and Silverman, going about one chapter every two and a half weeks. Class work includes use of the Python programming language and the \LaTeX typesetting language. All relevant software is available for free on all computer platforms. However, we will be using the Cocalc platform for Python programming. This site requires a license, which I will purchase for the class in the near future.

Course description. We will cover algorithms for factorization and primality testing, including public key cryptosystems such as RSA, which is widely used for secure transfer of data on the internet. Additional background material (such as the rudiments of elliptic curves) will be introduced as needed. Computer programming will be required, though no prior experience is assumed.

Course objectives. The goal of this course is to understand the theory and practice of cryptography, including related issues such as factoring and primality testing. At the end of this course, you will be able to understand a number of secure cryptosystems, and learn to implement them in the Python programming language. You will also have some understanding of potential weaknesses of common cryptosystems, including how to break a poorly designed cryptosystem. Finally, we’ll learn a range of mathematics predominantly in number theory which relates to cryptography.

Course requirements. The grading scheme is as follows:

20% for homework
20% for code-breaking contests
40% for 2 exams
20% for paper

Homework is announced on my webpage every Friday and is due on Gradescope and/or Cocalc the following Friday.

You must also show all work to receive full credit. You will be graded on your writing! Correct and clear grammar is essential to a correct proof. Of course, your reasoning must also be completely clear for full credit. Rewriting homework before handing it in is highly advisable. You may type your problem sets, but if you do, please use \LaTeX. Homework fulfills this course’s writing requirement.

Some homework problems involve writing computer programs. Programs should be

- written in Python,
- use only allowed commands,
• pass all relevant tests,
• have appropriate documentation strings, and
• be submitted via CoCalc.

Additionally, if required or appropriate, a proof that the program works should be included. You may (and should!) use programs from prior homeworks, in which case you should include the code (with docstrings, but not proofs). Some computational problems also require computer programs. The same guidelines apply.

After homework is handed in, I will be happy to go over complete solutions in office hours. Feel free to also e-mail me questions.

The code-breaking contests will be detailed as they arise. These are competitive group projects which will mainly be conducted outside of class.

The exams are scheduled for March 8 and April 19. There is an optional final exam on Wednesday, May 17, 8:30–10:30 PM; if you take it, the score will replace your lowest midterm score. The replacement will occur regardless of your score on the final.

Your paper is an 8–10 page expository work on a topic of your choice. It is due on April 14, with an optional revision due on May 12. Finished papers will be posted on my web page. This paper may be submitted as part of your Graduate Writing Assessment Requirement (GWAR). Shortly I will circulate a handout giving the details of this assignment. You must prepare your paper using \LaTeX! If you don’t know how to use \LaTeX, I will be happy to assist you.

Late assignment policy. Late homework is not accepted. There are no exceptions! Instead, the lowest two homework scores are dropped.

Make-up exams are not given; see the exam policy above.

Office hours. My office hours are Wednesday, 12:30–1:30 PM and Thursday, 1–3 PM. Drop by the math conference room, Craven Hall 6242, during those times—you don’t need an appointment! If you have a conflict, send me an email and we’ll work out an alternate time. You can also email me any questions that you have. Make sure you include as much relevant detail as possible, and be aware that I may not have the textbook with me when I read your email.

Ethics. You are encouraged to work with others on graded assignments, but, with the exception of the coding projects, the final product should be your own work. In particular, you may not read your classmates’ finished assignments until your own is completed! The same goes for other sources—online, back of the book, or other sources. Avoid looking at these sources, or if you do, take no notes on them. For the code-breaking contests, the same guidelines apply, except replace “you” with “your group”. Failure to follow these guidelines is considered plagiarism, and all involved parties will at a minimum earn a zero on the relevant assignment and have their actions reported to the Dean of Student Affairs.
**Computer use policy.** Our class is in a computer lab, and will occasionally require the use of a computer. Please do not use the computers for personal purposes during class time. It is distracting and disrespectful. If you have an urgent task that requires you to use the computer at some point during class, please let me know ahead of time.

**ADA policy.** Students with disabilities who require reasonable accommodations must be approved for services by providing appropriate and recent documentation to the Office of Disabled Student Services (DSS) in Craven Hall 4300 (ph: (760) 750-4905; TTY: (760) 750-4909). Students authorized by DSS to receive reasonable accommodations should meet with me during my office hours in order to ensure confidentiality.