Time and location: MWF 10:00-10:50 Wilson 309

Instructor: Nathan Pflueger
email: pflueger@math.brown.edu
office: Kassar 219
office hours: Wednesdays 2:45-4:15
Thursdays 12:00-1:30 (with my dog, Charley)

Graders: Daniel Keliher
daniel_keliher@brown.edu
Nathaniel Hanson
nathaniel_hanson@brown.edu

Course webpage: `math.brown.edu/~pflueger/math158`

Course topics: We will cover mathematical problems underlying public-key ciphers and digital signatures, as well as algorithms to solve them. The subject presents an appealing introduction to several notions from number theory, abstract algebra, and algorithms. 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).

Prerequisites: Linear algebra (Math 52, 54, or equivalent). Prior programming experience (in any language) is recommended but not necessary.

Textbook (free to you with your Brown login): *An Introduction to Mathematical Cryptography, Second Edition*, by Hoffstein, Pipher, and Silverman. Your Brown login allows you to download the entire book for free, or to print a cheap paperback copy, at the following link.

http://link.springer.com.revproxy.brown.edu/book/10.1007/978-1-4939-1711-2

Programming: Each homework assignment will include several programming tasks, and some exam problems will require you to write short programs (pseudocode is acceptable on exams). I will use the Python programming language for examples in class, and you will be expected to be able to read and analyze Python code in some homework and exam problems, but you may choose from several languages to use in completing the homework. I will devote some class time to helping you learn Python and showing how to use it to complete the assigned problems. However, I will expect you to take the initiative in looking up information on some of the tools you will need. You are encouraged to ask classmates for help, and also to bring questions to office hours.

Homework: Problem sets will be assigned every week and due on Thursday night (technically Friday morning at 4am is the hard deadline). Each problem set has a written part and a programming part; both must be submitted electronically (see instructions on the course website). Your lowest two homework scores will be dropped. *Late work will not be accepted for any reason.*

Problem sets will typically require between 8 and 12 hours to complete. If you do not have programming background, you should expect to spend more time learning this skill (but past students report that this time spent pays great dividends after the course!).

Some problems will be quite challenging. You do not need to complete them all to earn a good grade, but you should read and understand the posted solutions to problems you could not solve.

Collaboration policy: You are encouraged to work together freely on the homework assignments, but you must write your answers entirely by yourself. In the case of programming assignments, *you must write your code entirely by yourself.*

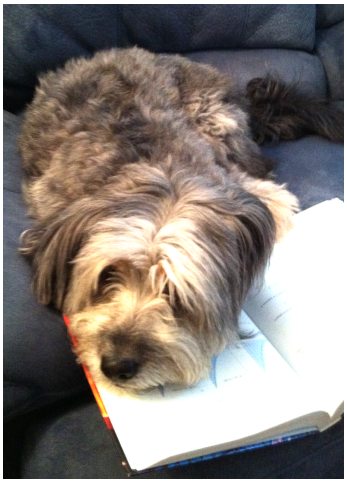
Grades: Your final course grade will be computed as follows.

Homework	25%	(includes programming assignments)
Midterm 1	20%	Wednesday 10/5 in class
Midterm 2	20%	Wednesday 11/9 in class
Final exam	35%	Tuesday 12/20 9am-noon

You will be allowed one page of notes (front and back) for each exam. No calculators or other aids are permitted. *Exams cannot be rescheduled for any reason.* If you must miss a midterm for a valid reason (approved in advance), your final exam score will replace that midterm in your final grade.

Disability support: Please inform me if you have a disability or other condition that might require modification of these procedures. You should also contact the Student and Employee Accessibility Services at 401-863-9588 or SEAS@brown.edu.

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 or listen to other students' questions, or to visit the dog.



Charley the cryptography dog: I will often have my dog Charley (pictured) with me during my office hours (usually she will be there on Thursday, but not on Wednesday). She is available for all your therapy dog needs, and I will not be offended if you come to office hours just to play with her.

I understand that many people are allergic to dogs or just don't like them. *Please tell me if I should leave her at home.* You do not need to tell me a reason.