Instructor: Nathan Pflueger
email: pflueger@math.brown.edu
office: Kassar 219
office hours: Wednesdays 1:30-2:30 (with my dog, Charley)
Thursdays 11:30-12:30

Grader: Daniel Keliher
daniel_keliher@brown.edu

Time and location: MWF 11:00-11:50 Barus & Holley 141
Course webpage: `math.brown.edu/~pflueger/math158`

Course topics: We will focus on the mathematics of public-key cryptography. This subject presents an appealing introduction to several notions from abstract algebra, number theory, and computer science. Topics will include:

1. The discrete logarithm problem and ElGamal cryptosystem.
2. Integer factorization and the RSA cryptosystem.
3. Digital signatures.
4. Elliptic curves and related cryptosystems.
5. Additional topics based on time and student interest.

Throughout the course, we will discuss both *cryptography* (encryption and signing algorithms) and *cryptanalysis* (algorithms to break cryptosystems), in order to illustrate the mistakes that must be avoided in implementing these systems, and the vulnerabilities that may arise as technology improves.

Prerequisites: Linear algebra (Math 52, 54, or equivalent). Prior programming experience is useful but not required.

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. The recommended programming language will be Python 2, which I will use in examples and starter code. Prior programming experience is not required, and I will devote some class time to helping you learn Python and showing how to use it for these assignments. However, I will expect you to take the initiative in learning how to look up information on the tools you need. You are encouraged to ask your classmates for help, and also to bring any questions to office hours.

Homework: Problem sets will be assigned every week and typically due on Fridays at the start of class. Written problems should be either turned in at lecture or emailed to me. Programming assignments will be submitted online by 10:50am on the due date, as described on the first problem set. *Late work will not be accepted for any reason.* However, your lowest two homework scores will be dropped.

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.

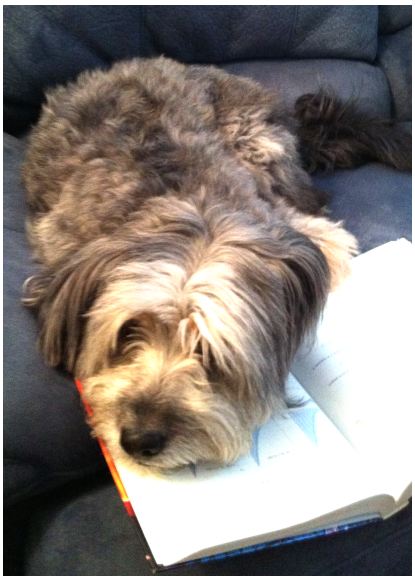
Homework	25%	(includes programming assignments)
Midterm 1	20%	Wednesday 10/7 in class
Midterm 2	20%	Wednesday 11/11 in class
Final exam	35%	Thursday 12/17 2pm-5pm

All exams will be closed-book. Calculators and computers will not be permitted. *Exams cannot be rescheduled for any reason.* If you must miss a midterm for a valid reason, your final exam score will replace that midterm score in your final grade.

Some exam problems will require you to write pseudo-code to solve problems similar to the programming assignments.

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 (tentatively, she will be there on Wednesdays but not on Thursdays). 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. She is very friendly and will certainly like you as long as you aren't a mail carrier.

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.