Math 116, Spring 2021
Mathematical Cryptology

Lecture

Mon, Wed, Fri 9–9:50am in 4645 Geology
Instructor: Hood Chatham
Contact: hood@math.ucla.edu
Office Hours: Thursday, 3pm – 5pm at my office (probably)
Office: Math Sciences 6903

Discussion

Thursday 9–9:50am in Geology 4645
TA: Derek Levinson
Contact: djlevins@math.ucla.edu
Office Hours:
Tuesday 11am – 12am on Zoom ,
Thursday 10am – 11am in MS 3975

Prequisites

- Math 115a or equivalent knowledge of linear algebra
- Knowledge of how to write simple mathematical proofs.

The following are not prerequisites but will make the class easier:

- Prior experience in algebra or number theory
- Some experience using mathematical software for computation is helpful, particularly experience with Sage or Python.

Textbook

Hoffstein, Pipher, Silverman, An Introduction to Mathematical Cryptography, 2nd ed. We will be covering Chapters 1–4 and parts of 6 and 7.
The textbook is freely available for download through SpringerLink from the following link:
https://link.springer.com/content/pdf/10.1007%2F978-1-4939-1711-2.pdf
You need to access the website from within the campus network, or use the UCLA proxy server. If you are having trouble getting access to a digital copy of the book, let me know and I can help.

Learning Goals

- You will learn about public key cryptography and commonly used public key cryptosystems.
- You will learn mathematical concepts used in common public key cryptosystems including modular arithmetic, finite fields, elliptic curves, and lattices.
- You will learn to use mathematical software like SageMath to help with large computations.

Grade

I will assign letter grades based on individual performance relative to the course goals, not based on the class rank. If you deserve an A, then you will receive an A even if 50% of the class performed better. I will compute a numerical score using the grading scheme:

Homework	20%
Midterm	35%
Final Exam	45%

The baseline grade boundaries are as follows:

		A	$\geq 93\%$	A-	$\geq 90\%$
B+	$\geq 87\%$	B	$\geq 83\%$	B-	$\geq 80\%$
C+	$\geq 77\%$	C	$\geq 73\%$	C-	$\geq 70\%$
D+	$\geq 67\%$	D	$\geq 63\%$	D-	$\geq 60\%$
F	$< 60\%$				

A grade of A+ is given only at the discretion of the instructor. Depending on class performance, the grades may be curved up but grades *will not be curved down.* (So for example if your raw score in the class is an 89 you are *guaranteed* at least a B+, but at the discretion of the instructor the grade boundaries *may* be moved down so that you instead earn an A- or A.)

Homework

Homework will be due in class each Friday (starting the second week of class). It will be posted on the course webpage. No late homework will be accepted. Your lowest homework score will be dropped. (If there is an emergency and you let me know ahead of the time, I may allow an extension.)

Please discuss homework problems with other students. You may share solutions, you may even read the answers that other students write. Do NOT look at other students' work when writing your answers. If part of your homework is an exact copy of another student's homework, you may both lose credit. As long as you don't look at other peoples' work while writing your own work, you will be fine.

Homework must be neat and legible. It must be stapled. The staple must be in the corner of the paper, not in the middle of the paper. Leave a bit of margin space at the top and left of the pages. If the paper is torn out of a spiral-bound notebook, the ragged edge of the paper must be removed. The TA may take off points for homework that is illegible or otherwise difficult to grade.

Sage Math

You will need to use Sage to do some of the homework problems. You can use Cocalc which is here: https://cocalc.com. If you wish to install Sage on your computer I wrote some instructions for installing Sage: https://www.math.ucla.edu/~hood/2022-Spring_Math-116/getting-sage.html If you have trouble running sage, please email me with your questions, come to office hours, or ask me after class.

Exams

Midterm
Friday, April 29
9:00 AM - 9:50 AM
In class, 4645 Geology

Final Exam
Thursday, June 9, 2022
11:30 AM - 2:30 PM
Location TBD

All exams will be in person. There is no makeup midterm. If you miss the midterm for an excused reason (injury, illness, other emergency) I will rescale the grading to be 25% homework, 75% final. You must take the final. If you miss the final due to an emergency, you will be able to take a makeup final during the Fall quarter.

Disabilities Requiring Accommodation

If you are already registered with the Center for Accessible Education (CAE), please request your Letter of Accommodation on the Student Portal. If you are seeking registration with the CAE, please submit your request for accommodations via the CAE website. Please note that the CAE does not send accommodations letters to instructors – you must request that I view the letter in the online Faculty Portal. Once you have requested your accommodations via the Student Portal, please notify me immediately so I can view your letter. Students with disabilities requiring academic accommodations should submit their request for accommodations as soon as possible, as it may take up to two weeks to review the request. For more information, please visit the CAE www.cae.ucla.edu.

Schedule of topics

Date	Topic	Textbook section(s)
Monday, March 28	Substitution Ciphers	1.1
Wednesday, March 30	Divisibility and gcd	1.2
Friday, April 1	Modular Arithmetic	1.3
Monday, April 4	Finite Fields	1.4, 1.5
Wednesday, April 6	Symmetric and asymmetric ciphers	1.6,1.7
Friday, April 8	Discrete Log Problems	2.1, 2.2
Monday, April 11	Diffie–Hellman Key Exchange & Elgamal PKC	2.3, 2.4
Wednesday, April 13	Babystep–Giantstep	2.6, 2.7
Friday, April 15	Pohlig–Hellman Algorithm	2.8, 2.9
Monday, April 18	RSA PKC	3.1, 3.2
Wednesday, April 20	Primality Testing	3.4
Friday, April 22	Pollard's $p-1$ method	3.5
Monday, April 25	Quadratic Sieve	3.7.2
Wednesday, April 27	Probabilistic Encryption	3.9,3.10
Friday, April 29	**Midterm Exam**	
Monday, May 2	Digital Signature	4.1, 4.2, 4.3
Wednesday, May 4	Digital Signature continued	4.1, 4.2, 4.3
Friday, May 6	Elliptic Curves	6.1
Monday, May 9	Elliptic Curves over finite fields	6.2
Wednesday, May 11	Elliptic Curve Discrete Log problem	6.3
Friday, May 13	Elliptic Curve cryptography	6.4
Monday, May 16	Elliptic Curve cruptography continued	6.4
Wednesday, May 18	Lenstra's elliptic curve factorization	6.6
Friday, May 20	Lattices	7.3, 7.4
Monday, May 23	Shortest Vector Problem	7.5.1, 7.5.2
Wednesday, May 25	Lattice-based cryptography	7.6, 7.7, 7.8
Friday, May 27	Gaussian Lattice Reduction	7.13.1, 7.13.2
Monday, May 30	No class (Memorial Day)	
Wednesday, June 1	LLL Lattice Reduction	7.13.2
Friday, June 3	Review	