Math 116, Spring 2021:
Mathematical Cryptology

Mon, Wed, Fri 9-9:50am
on Zoom 957 2104 3583
Lectures and discussion sections are recorded.
Live attendance is not required but recommended.

Prerequisites

- You are expected to know how to write proofs for mathematical statements.
- Some experience of using mathematical softwares for computation will be helpful but not necessary.

Learning Goals

- You will learn mathematical concepts commonly used in cryptography. For example, modular arithmetic, finite fields, and elliptic curves.
- You will also acquire basic knowledge of the public key cryptography, and examples of them.
- You will learn to use mathematical softwares like SageMath to help with heavy computation.

Instructor
Chi-Yun Hsu
Contact: Use Piazza rather than email to contact me, see below.
Office Hour: Mondays 3-3:50pm

Teaching Assistants
Frederick Vu
Section: Tuesdays 9-9:50am

Course website: https://ccle.ucla.edu/course/view/21S-MATH116-1

Textbook: Hoffstein, Pipher, Silverman, *An Introduction to Mathematical Cryptography*, 2nd ed. The textbook is freely available for download through SpringerLink. (You need to access the website from within the campus network, or use the UCLA proxy server.)
We will be covering **Chapter 1–4, 6, and some part of 7**.

Course Discussion Forum on Piazza: http://piazza.com/ucla/spring2021/math116
Please use private post on Piazza, rather than emails, to contact me. Emails can easily get lost or go to my spam folder. You are also encouraged to use Piazza to have online discussion with classmates on course materials, homeworks, or any other questions.

Grade
I will assign letter grades based on individual performance relative to the course goal, rather than based on the class rank. Namely if your performance deserves an A, then you will receive an A even if 50% of the class perform better. In short, I do not grade on a curve.

I will compute a numerical score using the grading scheme:

Homework	20%
Midterm 1	25%
Midterm 2	25%
Final Exam	30%

According to the Departmental policy, your actual letter grade will NOT be below the one converted from the numerical score. The standard conversion is 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%. The grade A+ is optional at the university level. It is given only when there is truly exceptional overall performance, so the grade A+ will be scarce or non-existent.

Homework
I will assign homework problems on the course website on a weekly basis. The homework is **due on Tuesday 11:59pm of the next week**. It is better to do the homework problems after each lecture, rather than rushing to finish at one time.

Please scan your homework and submit to Gradescope. You are responsible for the eligibility of the scan. Even if the TA cannot read the scan, no resubmission will be accepted.

Late homework will NOT be accepted. To accomodate the strict policy, **the lowest homework score will be dropped.** On the other hand, if you are under emergency circumstances such as accident or severe sickness happened well before the deadline so that you cannot possibly have time to do the homework, you can let me know and ask for a deadline extension. However, the deadline extension request is only accepted before the deadline, and will only be granted for emergency circumstances.

I encourage you to discuss homework problems with other students, either form a study group or use online discussion tools such as Piazza mentioned above. However, you must write up the solutions on your own, as writing helps you deepen your understanding. Apart from help from me or the TA, you must acknowledge any collaborators or references at the top of your assignement.

Exams
There will be NO make-ups for missed midterm. You must take the final exam in order to pass the class. Make-ups for the final exam are permitted only under exceptional circumstances.

It is Departmental policy that the Midterms and the Final Exam are designed as 1 and 3 hour exams, respectively, but are all given over a 24-hour period. You are allowed to use any non-human resources including internet, calculators, textbook, notes, lecture videos, etc. You are NOT allowed to seek help from other people, including posting exam questions on online forums.

Tentative exam dates are:

Midterm 1	Apr. 21 (Wed.) 8am - Apr. 22 (Thurs.) 8am	Week 1-3 Material
Midterm 2	May 12 (Wed.) 8am - May 13 (Thurs.) 8am	Week 4-6 Material
Final Exam	June 10 (Thurs.) 8am - June 11 (Fri.) 8am	Week 1-10 Material

Learning Resources

- Your fellow students: You are encouraged to form study groups with your classmates.
- Office hours: You do not need to make an appointment; just show up to ask any questions.

You are encouraged to make good use of these resources. At the same time, don't be too quick to run for help. Learning is challenging and takes time. You should not expect to solve every problem immediately. Try a couple of different approaches before asking for help. Often you learn the most from things you try that don't work!

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.

Center for Accessible Education (CAE)
A255 Murphy Hall
www.cae.ucla.edu
(310) 825-1501

Statement on Sexual Misconduct
Title IX prohibits gender discrimination, including sexual harassment, domestic and dating violence, sexual assault, and stalking. If you have experienced sexual harassment or sexual violence, you can receive confidential support and advocacy at

CARE Advocacy Office for Sexual and Gender-Based Violence
1st Floor Wooden Center West
CAREadvocate@careprogram.ucla.edu
(310) 206-2465

In addition, Counseling and Psychological Services (CAPS) provides confidential counseling to all students and can be reached 24/7 at (310) 825-0768. You can also report sexual violence or sexual harassment directly to

University's Title IX Coordinator
2241 Murphy Hall
titleix@conet.ucla.edu
(310) 206-3417

Reports to law enforcement can be made to UCPD at (310) 825-1491.

Faculty and TAs are required under the UC Policy on Sexual Violence and Sexual Harassment to inform the Title IX Coordinator should they become aware that you or any other student has experienced sexual violence or sexual harassment.

Tentative Calendar

	Monday	Wednesday	Friday
Week 1 (3/29-4/2)	1. Substitution Ciphers (1.1)	2. Divisibility and gcd (1.2)	3. Modular Arithmetic (1.3)
Week 2 (4/5-4/9)	4. Finite Fields (1.4,1.5)	5. Symmetric and asymmetric ciphers (1.6,1.7)	6. Discrete Log Problems (2.1-2.2)
Week 3 (4/12-4/16)	7. Diffie–Hellman Key Exchange & Elgamal PKC (2.3,2.4)	8. Babystep-Giantstep (2.6,2.7)	9. Pohlig–Hellman Algorithm (2.8,2.9)
Week 4 (4/19-4/23)	10. RSA PKC (3.1,3.2)	11. **Midterm 1** on Lec 1-9	12. Primality Testing (3.4)
Week 5 (4/26-4/30)	13. Pollard's $p-1$ method (3.5)	14. Quadratic Sieve (3.7.2)	15. Probabilistic Encryption (3.9,3.10)
Week 6 (5/3-5/7)	16. Digital Signature (4.1-4.3)	17. Digital Signature (cont'd) (4.1-4.3)	18. Elliptic Curves (6.1)
Week 7 (5/10-5/14)	19. Elliptic Curves over finite fields (6.2)	20. **Midterm 2** on Lec 10-18	21. Elliptic Curve DLP (6.3)
Week 8 (5/17-5/21)	22. Elliptic Curve cryptography (6.4)	23. Elliptic Curve cryptography (cont'd) (6.4)	24. Lenstra's Elliptic Curve Factorization (6.6)
Week 9 (5/24-5/28)	25. Lattices (7.3,7.4)	26. Shortest Vector Problem (7.5.1,7.5.2)	27. Lattice Based Cryptography (7.6-7.8)
Week 10 (5/31-6/4)	No class (Memorial Day)	28. Gaussian Lattice Reduction (7.13.1,7.13.2)	29. LLL Lattice Reduction (7.13.2)