Math 116, Winter 2020:
Mathematical Cryptology

Mon, Wed, Fri 9-9:50am
Geology Building 6704

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
Office: Math. Sciences Building 5242
Contact: Use Piazza rather than email to contact me, see below.

Office Hours:

Wed.	10:00-10:30am	at MS 5242
Fri.	1:00-1:30pm	at MS 5242

or by appointment

Teaching Assistants

David Hemminger (MS 6154, dhemminger@math.ucla.edu)
Section: Tuesday 9-9:50am, GEOLOGY 6704

Course website: https://ccle.ucla.edu/course/view/20W-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 aiming at covering **Chapter 1-4 and 6**.

Course Discussion Forum on Piazza: http://piazza.com/ucla/winter2020/math116
Please use Piazza, rather than emails, to contact me. You are also encouraged to use Piazza to have online discussion with classmates on course materials, homeworks, or any other questions.

Grade

I will compute using both grading scheme below and your course score will be the MAX of the two:

Homework	20%
Midterm	30%
Final Exam	50%
Course Evaluation	1% extra

Homework	20%
Final Exam	80%
Course Evaluation	1% extra

The second grading scheme is designed to accomodate the policy that NO make-up midterms will be provided.

I will assign letter grades based on your course score. The basic cutoff is A$-$ $\geq$ 90%, B$-$ $\geq$ 80%, C$-$ $\geq$ 70%, D$-$ $\geq$ 60%, F$<$ 60%. I will only decide the actual cutoff after the Final Exam when

all scores are ready. I might make the cutoffs lower depending on the distribution of scores, but I will not raise the cutoffs.

Homework
I will assign homework problems on the course website on a weekly basis. The homework is **due on Sunday noon (12pm) of the same 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
Please bring a photo ID to every exam. During the exams, you may not use notes, calculators, cell phones, or anything not for writing. There will be NO make-ups for missed midterm. To accomodate this, there is the second grading scheme which only counts one (higher) midterm score (see the **Grade** section above). You must take the final exam in order to pass the class. Make-ups for the final exam are permitted only under exceptional circumstances. Tentative exam dates are:

Midterm	Feb. 12 (Wed.)	9-9:50am	Geology Building 6704
Final Exam	Mar. 20 (Fri.)	3-6pm	TBD

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.
- Tutors: The Math Department maintains a list of UCLA mathematics graduate students who are available for hire as tutors. See http://www.math.ucla.edu/people/tutors.

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.