UCONN

DEPARTMENT OF MATHEMATICS
Álvaro Lozano-Robledo

MATH 3094: Mathematics of Encryption (Fall 2023)

Course Description:

Title: Mathematics of Encryption

Description:

Modern cryptography lies at the intersection of mathematics and computer science, involving number theory, algebra, algorithmic complexity, and potentially quantum mechanics. Many people think of codes in terms of spies, but in the information age, highly mathematical codes are used every day by almost everyone, whether at the bank ATM, at the supermarket, or when you send a text or purchase products online. Here is the same message encrypted in four different ways:

GUVF PBHEFR VF NJRFBZR (Caesar cipher)

DLGC GMEVQO MQ KACCSKO (Vigenère cipher)

OPGN NKLT KCBA BUSD ZDO (Enigma machine)

1062 338 184 774 649 324 350 693 1022 774 797 649 184 774 649 1002 812 797 774 350 21 797 (RSA, public key [1073, 5])

This course will provide a historical and mathematical tour of cryptography, from classical ciphers to quantum cryptography. The topics will include: classical ciphers (e.g., Caesar and Vigenère ciphers) and the attacks on them, the Enigma system, public-key RSA (including a complete mathematical proof that it works), detecting and correcting errors, primality testing and digital signatures, and elliptic curve cryptography (if time permits).

Prerequisites: MATH 3240 (Intro. to Number Theory) or instructor consent to substitute MATH 3240 by CSE 2500 (or a strong grade in 2710). Enrollment requires instructor permission.

Meets: Tuesdays and Thursdays, from 12:30pm – 1:45pm, at MONT 113

About the Instructor: Álvaro Lozano-Robledo

I'm a Professor of Mathematics. You can find out more about me and about my research here.

Office hours: Thursdays 11-12 (in-person at MONT 233) and Fridays 2-3pm (online), or by appointment.



Alvaro Lozano-Robledo in action (Shawn Kornegay/UConn Photo), see this UConn Today's article.

Enrollment:

The enrollment for this class is by permission for undergraduate students. Send me a message if you would like to enroll.

Outline, books, and other resources:

The book for this course is "An Introduction to Mathematical Cryptography", SECOND EDITION, by Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. (Amazon page.)

NOTE: UConn students have **free online access** to this book via the library. Follow **this Springer Link**.

The course will cover the following topics (from the Second Edition):

1. Chapter 1. An Introduction to Cryptography. (Cover all sections, 1.1-1.7.)
2. Chapter 2. Discrete Logarithms and Diffie–Hellman. (Cover 2.1–2.7.)
3. Chapter 3. Integer Factorization and RSA. (Cover 3.1–3.5 and 3.9–3.10.)
4. Chapter 4. Digital Signatures (Cover 4.1-4.3)
5. Chapter 6. Elliptic Curves. (Cover 6.1, 6.2, 6.3, 6.4, 6.6)
6. Chapter 7. Lattices and Cryptography (Cover 7.1-7.5)

Homework, Quizzes:

Homework will be assigned and collected every other week. Homework will be graded on completion only. If you have questions about how to solve a problem, you should talk to me in office hours or ask questions in class. **Homework is due in class on the date listed below. Late homework will not be accepted.**

Homework:

The homework problem sets will be posted here:

1. **Homework set 1** (due Thursday, Sept. 14th):
    - Section 1.1: 1.1, 1.2, 1.3, 1.4, 1.5,
    - Section 1.2: 1.7, 1.8, 1.9, 1.10.,
    - Section 1.3: 1.16, 1.17, 1.18, 1.22, 1.24 (note: in the first edition, the numbering is slightly different, and you should do 1.15, 1.16, 1.17, 1.21, 1.23 instead for Section 1.3)
2. **Homework set 2** (due Thursday, Sept. 28th):
    - Section 1.4: 1.28, 1.30,
    - Section 1.5: 1.32, 1.34, 1.36,
    - Section 1.6: 1.39 OR 1.41,
    - Section 1.7: 1.42, 1.43, 1.44, 1.46.
3. **Homework set 3** (due Thursday, Oct. 12th):
    - Section 2.2: 2.3, 2.4,
    - Section 2.3: 2.6,
    - Section 2.4: 2.8, 2.9, 2.10,
    - Section 2.5: 2.11, 2.12, 2.13, 2.14,
    - Section 2.6: 2.16,
    - Section 2.7: 2.17.
4. **Homework set 4** (due Tuesday, Oct. 31st):
    - Section 3.1: 3.1, 3.5 (part e), 3.6,
    - Section 3.2: 3.7, 3.8, 3.9, 3.10,
    - Section 3.3: 3.12, 3.13,
    - Section 3.4: 3.14, 3.15,
    - Section 3.5: 3.22, 3.23,
    - Section 3.9: 3.39,
    - Section 3.10: 3.42.
5. **Homework set 5** (due Tuesday, Nov. 28th):
    - Section 4.2: 4.1, 4.2, 4.3,
    - Section 4.3: 4.5, 4.6, 4.8, 4.9, 4.10.
6. **Homework set 6** (due Thursday Dec. 7th):
    - Section 6.1: 6.1, 6.2, 6.4,
    - Section 6.2: 6.5, 6.6(a), 6.7,

- Section 6.3: 6.8, 6.11, 6.12
- Section 6.4: 6.14, 6.15, 6.16, 6.20.

Class Grade:

The grade will be computed based on homework performance, class participation, and two exams and a final.

The total grade will be computed as follows: Prelim 1 (100 points), Prelim 2 (125 points), the final exam (175 points) and a lecture grade (150 points). The lecture grade will be based on homework and class participation.

- **MIDTERM 1**: Covers Chapters 1 and 2. In-class, Thursday, October 5th.
  - Highlights from Chapters 1 and 2.
  - Practice Midterm 1.
    - Practice 1 solutions.
  - Midterm 1 – Solutions.
- **MIDTERM 2**: Covers Chapters 3 and 4. In-class, Thursday, November 16th. (Please note new date!)
  - Highlights from Chapters 3 and 4.
  - Practice Midterm 2.
    - Practice 2 solutions.
  - Midterm 2 – Solutions.
- **FINAL EXAM**: Cumulative with emphasis on Chapter 6. (Please find date and time information at the registrar's website!).
  - Highlights from Chapter 6. (Please also review the highlights for chapters 1-4 above.)
  - Practice Final Exam. (This file only contains practice questions for Ch. 6. Please review previous practice exams and exams for material on previous chapters — the final is cumulative!)
    - Solutions and Hints for Practice Final.

Course Outline:

Week	Topics	Notes
1	1.1	
	1.2, 1.3	
2	1.4	

	1.5	
3	1.7	
	2.1, 2.2	Homework set #1 is due
4	2.3	
	2.4	
5	2.5	
	2.6, 2.7	Homework set #2 is due
6	Catch up/Review	
	EXAM 1 – Exact date TBA	
7	3.1	
	3.2, 3.3	Homework set #3 is due
8	3.4, 3.5	
	3.9, 3.10	
9	4.1, 4.2	
	4.3	Homework set #4 is due
10	6.1	
	6.2	
11	Catch up/Review	
	EXAM 2 – Exact date TBA	
12	6.3	
	6.4	Homework set #5 is due
13	6.6	
	7.1, 7.2	
14	7.3, 7.4, 7.5	

Review	Homework set #6 is due

Policy Statements:

Please refer to the Provost's website for the common policies we follow at UConn.

- Absences from Final Examinations
- Class Attendance
- Credit Hour
- People with Disabilities, Policy Statement
- Discrimination, Harassment and Related Interpersonal Violence, Policy Against
- The Student Code
- Academic Misconduct Procedures for Instructors

Policy Against Discrimination, Harassment and Related Interpersonal Violence

The University is committed to maintaining a safe and non-discriminatory learning, living, and working environments for all members of the University community – students, employees, or visitors. Academic and professional excellence can flourish only when each member of our community is assured an atmosphere of mutual respect. All members of the University community are responsible for the maintenance of an academic and work environment in which people are free to learn and work without fear of discrimination or discriminatory harassment. In addition, inappropriate amorous relationships can undermine the University's mission when those in positions of authority abuse or appear to abuse their authority. To that end, and in accordance with federal and state law, the University prohibits discrimination and discriminatory harassment, as well as inappropriate amorous relationships, and such behavior will be met with appropriate disciplinary action, up to and including dismissal from the University. Additionally, to protect the campus community, all responsible employees (including faculty), as outlined in the Policy Against Discrimination, Harassment and Related Interpersonal Violence, are required to report to the Office of Institutional Equity any information that they receive related to sexual assaults, intimate partner violence, and/or stalking involving a student. *An exception to this reporting exists if students disclose information as a part of coursework submitted to an instructor in connection with a course assignment. Even in the absence of such obligation, all Employees are encouraged to contact OIE if they become aware of information that suggests a safety risk to the University community or any member thereof.* The University takes all reports with the utmost seriousness. Please be aware that while the information you provide will remain private, it will not be confidential and will be shared with university officials who can help. More information, including confidential and exempt employee resources available for support and assistance, can be found at equity.uconn.edu and titleix.uconn.edu.

Statement on Absences from Class Due to Religious Observances and Extra-Curricular Activities

Faculty and instructors are expected to reasonably accommodate individual religious practices unless doing so would result in fundamental alteration of class objectives or undue hardship to the University's legitimate business purposes. Such accommodations may include rescheduling an exam or giving a make-up exam, allowing a presentation to be made on a different date or assigning the student appropriate make-up work that is intrinsically no more difficult than the original assignment. Faculty and instructors are strongly encouraged to allow students to complete work missed due to participation in extra-curricular activities that enrich their experience, support their scholarly development, and benefit the university community. Examples include participation in scholarly presentations, performing arts, and intercollegiate sports, when the participation is at the request of, or coordinated by, a University official. Students should be encouraged to review the course syllabus at the beginning of the semester for potential conflicts and promptly notify their instructor of any anticipated accommodation needs. Students are responsible for making arrangements in advance to make up missed work.

For conflicts with final examinations, students should contact the Dean of Students Office. Faculty and instructors are also encouraged to respond when the Counseling Program for Intercollegiate Athletes (CPIA) requests student progress reports. This will enable the counselors to give our students appropriate advice.

Center for Students with Disabilities

The University of Connecticut is committed to protecting the rights of individuals with disabilities and assuring that the learning environment is accessible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, please let me know immediately so that we can discuss options. Students who require accommodations should contact the Center for Students with Disabilities, Wilbur Cross Building Room 204, (860) 486-2020 or http://csd.uconn.edu/.

Office of Emergency Management on Emergency Preparedness

In case of inclement weather, a natural disaster, or a campus emergency, the University communicates through email and text message. Students are encouraged to sign up for alerts through http://alert.uconn.edu. Students should be aware of emergency procedures, and further information is available through the Office of Emergency Management at http://publicsafety.uconn.edu/emergency/.

Back to top

© University of Connecticut Disclaimers, Privacy & Copyright Accessibility Webmaster Login