Math 173B - Introduction to Mathematical Cryptology II
Course Info and Syllabus

Instructor: Maureen Zhang
yuanfz1@uci.edu
Office: Rowland Hall 590

Welcome to Cryptology II!
August 4 – September 8
Lecture: MWF 9:00–10:50 AM, Zoom ID: *935 0154 8575*
Lecturer OH: MW 4:00- 5:00 PM, Zoom ID TBA.
Discussion: MWF 11:00–11:50 AM, Zoom ID TBA.
TA OH: TBA.

Learning Outcomes

- Implement RSA and ElGamal digital signature algorithms.
- Define elliptic curves, including the geometric group law.
- Implement a public key cryptosystem based on the elliptic curve discrete logarithm problem.
- Define lattices and describe cryptographic applications.
- Implement the GGH public key cryptosystem (based on the closest vector problem).
- Explain quantum threats to cryptography.

You're encouraged to make friends in this class!

Staying motivated during a fast-paced summer session can be challenging, so **starting early**, **asking questions**, and **building a community** are key to successful learning. Let's support one another, keep learning, and have some fun along the way!

Textbook

Hoffstein, Pipher, and Silverman, *Introduction to Mathematical Cryptography*, 2nd ed.
Available for free at: `https://link.springer.com/book/10.1007/978-1-4939-1711-2` (if connecting from campus or via VPN).

Tentative Schedule

Week 1: Aug 4–Aug 9 — Review of Diffie-Hellman and RSA, ElGamal digital signatures, and an introduction to elliptic curves (§4.1–4.3, 6.1).
Due: Quiz 1 – Aug 6;

Week 2: Aug 11–Aug 15 — Elliptic curves over finite fields; the elliptic curve discrete logarithm problem (§6.2, 6.3).
Due: Homework 1 – Aug 11; Quiz 2 – Aug 13; Lab 1 – Aug 15

Week 3: Aug 18–Aug 22 — Cryptosystems based on the elliptic curve discrete logarithm problem; Lenstra's elliptic curve factorization algorithm (§6.4, 6.6).
Due: Homework 2 – Aug 18; Quiz 3 – Aug 20

Week 4: Aug 25–Aug 29 — Introduction to lattices and hard lattice problems (§7.4, 7.5).
Due: Midterm – Aug 25; Homework 3 – Aug 25; Lab 2 – Aug 29

Week 5: Sept 1 (Labor Day – no class); Sept 3–5 — Cryptosystems based on hard lattice problems (§7.7, 7.8).
Due: Homework 4 – Sept 3; Quiz 4 – Sept 3; Lab 3 – Sept 5

Week 6: Sept 8 — Review and an introduction to Shor's algorithm and post-quantum cryptography.
Due: Final Exam – Sept 9

Grading

- Homework: 20%
- Quizzes : 10%
- Attendance: 5%
- Midterm: 20%
- Labs: 15%
- Final Exam: 30%

Grades may be adjusted upward if an assessment is unexpectedly difficult.

Homework

Homework is due on Mondays(except Sept 1st) through Gradescope. Collaboration is allowed, but your submission must be written in your own words. The lowest score will be dropped.

Quizzes

Quizzes are due on canvas each Wednesday(except the week of the midterm). Quiz questions are based on each week's textbook sections. The lowest of the scores will be dropped.

Attendance

Attendance will be taken in the form of Canvas quizzes during some lectures.

Labs

Labs are due in Weeks 2, 4, and 5. Submit via Gradescope. You may work in a group of up to 3 students. Each student must submit the same file individually. You are encouraged to use AI creatively. Please explain how and why AI was utilized in your assignments.

Exams

- **Midterm:** Aug 25 — Zoom proctored, PDF upload required.
- **Final Exam:** Sept 9 — Zoom proctored, PDF upload required.

No Make-Up or Late Work Policy

There is a strict no make-up and no late submission policy for this class. To accommodate unforeseen circumstances, the lowest score will be dropped.

Regrading Policy

You may request regrading of up to two midterm problems. To do so, submit:

- A brief explanation of why your original solution was incorrect.
- A paragraph explaining how you arrived at the correct solution.
- A corrected version written in your own words.

Submissions must demonstrate clear understanding. Strict anti-plagiarism standards will be enforced.

Class Meetings

Class meetings are synchronous on Zoom. Lecture recordings will be posted online.

Hardware Requirements

You must be able to connect to Zoom with a webcam during assessments. Use a scanning app (e.g., Camscanner or Adobe Scan) to upload your work.

Disability Services

For accommodations, contact the Disability Services Center: 949-824-7494 or visit `https://dsc.uci.edu/`.

Academic Integrity

You must adhere to UCI's academic integrity policy: `https://aisc.uci.edu/`.
Homework may be collaborative, but quizzes and exams must be completed independently.