Syllabus

MATH 134 – Cryptography

Summer 2025 • MWF: 5:00 – 7:15 PM

Instructor: Deewang Bhamidipati
(Please address me by my first name, pronounced thee-waang. Pronouns: he/him/his.)

Office Hours: Wednesdays 10 – 11 AM & Thursdays 3 – 4 PM
(This is when you come and talk to me if you have any questions, or otherwise.)

Teaching Assistant: Brian Ma

TA Office Hours: Mondays 3 – 4 PM & Tuesdays 10 – 11 AM

Canvas: I will be using Canvas primarily as a course repository. It will also be a place where you will receive course announcements, access homework etc.
(Log in at `https://canvas.ucsc.edu` using your CruzID and Gold password.)

Ed Discussion: We will be using Ed Discussion as a discussion forum for anything and everything course related. It will be checked frequently and unresolved questions will be answered. You're highly encouraged to collaborate with each other and answer each other's questions; engaging in such discussions amongst yourselves is an incredibly invaluable part of succeeding in this course. You can access it by navigating to it from the Canvas menu on the left on our Canvas course page.

Gradescope: Any assessment (see below) that needs to be turned in will have to be uploaded to Gradescope; links and more details will be available on Canvas.

Learning Outcomes:
- You will be able to analyse the security of classical ciphers, such as shift and substitution ciphers, and apply fundamental cryptographic principles to implement them.
- You will be able to perform key exchanges with Diffie-Hellman and to encrypt and decrypt with RSA, and you will understand how the security of these systems relies on difficult mathematical problems like factoring large numbers.
- You will be able to explain the mathematical operations behind Elliptic Curve Cryptography (the "group law") and use them to perform a key exchange.

References: Lectures will be self-contained, they will largely be based on:

- ***An Introduction to Mathematical Cryptography*** by J. Hoffstein, J. Pipher, J.H. Silverman
- ***Cryptography*** by Simon Rubinstein-Salzedo

You are **not** expected to buy copies of these books.

Assessment Distribution: Our course will have the following assessment components, please read them carefully. More information on them will be available on Canvas.

- IN-CLASS WORK (30%)

  During class time you will be given opportunities to engage with the material directly by working on activities in groups, with support from the teaching team.

- HOMEWORKS (45%)

  There will be (three) homeworks, due in Wednesdays of Weeks 2 – 4.

- EXPLORATION WORKSHEETS (25%)

  In Week 5 you will be given worksheets during class time to explore topics that are natural sequels to the material we covered in the course. You will work on them in groups and each worksheet will end with a short presentation prompt and you will give a short presentation on Wednesday of Week 5. Further instructions and details will be available on Canvas by Week 3, so will a non-exhaustive list of possible topics.

Grading Scale: Passing grade is **C** or above.

A+	$\geqslant 95\%$	**B+**	80 – 84%	**C+**	65 – 69%	**D**	40 – 54%
A	85 – 94%	**B**	70 – 79%	**C**	55 – 64%	**F**	$< 40\%$

Course Schedule: Find below a tentative list of topics that will be covered each week.

WEEK 1	
DAY 1 (07/28)	*Shift & Substitution Ciphers*
DAY 2 (07/30)	*Number Theory I & Vigenere Cipher*
DAY 3 (08/01)	*Introduction to Modern Cryptosystems*
WEEK 2	
DAY 4 (08/04)	*Some Abstract Algebra*
DAY 5 (08/06)	*Number Theory II*
DAY 6 (08/08)	*Discrete Logarithms and Diffie-Hellman*
WEEK 3	
DAY 7 (08/11)	*The RSA Cryptosystem & Primality Testing*
DAY 8 (08/13)	*Elliptic Curves and Cryptography I*
DAY 9 (08/15)	*Elliptic Curves and Cryptography II*
WEEK 4	
DAY 10 (08/18)	*Elliptic Curves and Cryptography III*

Day 11 (08/20)	*Elliptic Curves and Cryptography IV*
Day 12 (08/22)	*Exploration Script*
Week 5	
Day 13 (08/25)	*Exploration Script*
Day 14 (08/27)	*Exploration Presentations*
Day 15 (08/29)	No Class

Guidelines:

- Homeworks (and other assignments)
  - ▷ Please turn in the homework on the due date.
    Extension Policy. If you need an extension, please ask, but make sure you ask before the due date. You can ask for, and will be awarded when asked, at most a two day extension.
  - ▷ Discuss the homework with your peers on Ed Discussion. (I insist on this.)
  - ▷ Write your work, **individually**, using LaTeX.
  - ▷ Pay close attention to the presentation and clarity of your reasoning in your answers.
  - ▷ Cite resources you have used while solving the homework.
  - ▷ Name your peers with whom you have discussed the homework.
  - ▷ Only a portion of the problems will be graded, chosen at the grader's discretion.

- Communication
  - ▷ Please contact me or Brian by email (at dbhamidi@ucsc.edu or bma82@ucsc.edu resp.) if you wish to chat with me about anything! If your question is math-related, I insist that you ask it on Ed Discussion, directly or anonymously.
  - ▷ Please make sure you give me as much information as you possibly can about the subject you intend to discuss when you contact me.
  - ▷ You are more than welcome to contact me at any time, you will get a response from me promptly between 9 AM - 6 PM, Monday to Friday.
  - ▷ **Never hesitate to reach out, I always want to hear from you.**

practice, discuss, ask

practice problems

discuss problems with your peers

ask me questions; more importantly: ask ***follow-up*** questions

SUBSEQUENT ADDENDUMS, IF ANY, TO ABOVE WILL BE MADE VIA CANVAS.
I RESERVE THE RIGHT TO CHANGE ANY PARTICULAR OF THE SYLLABUS ABOVE.
(ANY CHANGES WILL BE TO YOUR ADVANTAGE, AND YOU WILL BE INFORMED OF THEM PROMPTLY VIA CANVAS.)

Other Important Information

Summer Deadlines:

- (Session 2) Drop: **Monday, August 4**; Request for "W": **Sunday, August 17**;

Land Acknowledgement: The land on which we gather is the unceded territory of the Awaswas-speaking Uypi Tribe. The Amah Mutsun Tribal Band, comprised of the descendants of indigenous people taken to missions Santa Cruz and San Juan Bautista during Spanish colonization of the Central Coast, is today working hard to restore traditional stewardship practices on these lands and heal from historical trauma.

DRC (Remote) Accommodations: The Disability Resources Center (DRC) reduces barriers to inclusion and full participation for students with disabilities by providing support to individually determine reasonable academic accommodations. Operations continue via remote appointments. If you have questions or concerns about exam accommodations or any other disability-related matter, email the DRC Schedulers at drc@ucsc.edu for an appointment; you can also visit their website at http://drc.ucsc.edu.

CAPS (Counseling and Psychological Services): This is a stressful time, so if you are in distress, managing heightened stress and anxiety, or want to get more support and a counselors perspective on something you're going through, CAPS provides a variety of services for your needs, please visit their website for more information https://caps.ucsc.edu.

Title IX: The university cherishes the free and open exchange of ideas and enlargement of knowledge. To maintain this freedom and openness requires objectivity, mutual trust, and confidence; it requires the absence of coercion, intimidation, or exploitation. The principal responsibility for maintaining these conditions must rest upon those members of the university community who exercise most authority and leadership: faculty, managers, and supervisors.

The university has therefore instituted a number of measures designed to protect its community from sex discrimination, sexual harassment, sexual violence, and other related prohibited conduct. Information about the Title IX Office, the online reporting link, applicable campus resources, reporting responsibilities, the UC Policy on Sexual Violence and Sexual Harassment, and the UC Santa Cruz Procedures for Reporting and Responding to Reports of Sexual Violence and Sexual Harassment can be found at titleix.ucsc.edu.

The Title IX Office is actively responding to reports and requests for consultation. If you are not currently working with someone in the office and want to make a report/request a consult, you can expect the fastest response by using our online reporting link. For more information please visit the Title IX Operations under Covid-19 page.

Report an Incident of Hate or Bias: UC Santa Cruz is committed to maintaining an objective, civil, diverse and supportive community, free of coercion, bias, hate, intimidation, dehumanization or exploitation. The Hate/Bias Response Team is a group of administrators who support and guide students seeking assistance in determining how to handle a bias incident involving another student, a staff member, or a faculty member. To report an incident of hate or bias, please use the Hate/Bias Reporting Form.

Religious Accommodations: UC Santa Cruz welcomes diversity of religious beliefs and practices, recognizing the contributions differing experiences and viewpoints can bring to the community. There may be times when an academic requirement conflicts with religious observances and practices. If that happens, students may request the reasonable accommodation for religious practices. The instructor will review the situation in an effort to provide a reasonable accommodation without penalty. You should first discuss the conflict and your requested accommodation with your instructor early in the term. You or your instructor may also seek assistance from the Dean of Students office.

Small Group Tutoring: Small Group Tutoring (SGT) supports students academically to advance educational equity by designing inclusive learning environments outside of the classroom. In SGT, you can expect the Tutor to facilitate cooperative group activities designed to have students work together on the course content and develop study skills for the course, please visit their website for more information `https://lss.ucsc.edu`.

Academic Integrity: Academic integrity is the cornerstone of a university education. Academic dishonesty diminishesvthe university as an institution and all members of the university community. It tarnishes the value of a UCSC degree. All members of the UCSC community have an explicit responsibility to foster an environment of trust, honesty, fairness, respect, and responsibility. All members of the university community are expected to present as their original work only that which is truly their own. All members of the community are expected to report observed instances of cheating, plagiarism, and other forms of academic dishonesty in order to ensure that the integrity of scholarship is valued and preserved at UCSC. For the full policy and disciplinary procedures on academic dishonesty, students and instructors should refer to the Academic Integrity page at the Division of Undergraduate Education.