



Syllabus

Math/Comp Sci/E C E 435: Introduction to Cryptography

Last Updated: 19 January 2026

Course Information

How Credit Hours are Met by the Course This course meets the Traditional Carnegie Definition for how credit hours are met by the course. Students in the course have 2.5 hours/week of direct faculty instruction during class time and are expected to work on course learning activities (reading, writing, problem sets, studying, etc) for a minimum of 2 hours outside of classroom per course credit (i.e. 6 hours/week). The syllabus includes more information about meeting times and expectations for student work.

Official Course Description Cryptography is the art and science of transmitting digital information in a secure manner. Provides an introduction to its technical aspects.

Requisites (MATH 320, 340, 341, or 375) or graduate/professional standing or member of the Pre-Masters Mathematics (Visiting International) Program

Credits hours, Course Designations and Attributes Credit hours – 3, Level – Advanced, L&S Credit – Counts as Liberal Arts and Science credit in L&S

Course Overview

As the course title “Introduction to Cryptography” suggests, Math/Comp Sci/E C E 435 is a first course on the fundamentals of, and the mathematics behind, secure communication. Cryptography generally refers to methods to encrypt messages for secure communication, while cryptanalysis refers to the science of attacking, and finding weaknesses in, methods used to encrypt messages. We shall be concerned with both aspects, that is, with cryptology:

$$\{\text{cryptology}\} = \{\text{cryptography}\} \cup \{\text{cryptanalysis}\}.$$

We will cover both classical and modern cryptography and cryptanalysis. The classical systems, including substitution ciphers, affine ciphers, the Vig'enere cipher, and Feistel ciphers, use elementary mathematics for their construction; analyses to attack and decrypt also use elementary mathematics including some aspects of probability and statistics. DES (Data Encryption Standard), was based on classical methods and was replaced by AES (Advanced Encryption Standard). We shall develop the necessary background to understand both DES and AES. Modern cryptographic systems (public-key systems) are heavily mathematical, employing such mathematical tools as modular arithmetic, prime number theory, factorization theory, group theory, field theory, ldots). As a result we will have to spend considerable time on the underlying mathematics. We will also discuss various cryptographic protocols, pseudo-random sequences (feedback shift registers), ldots.

Learning Outcomes

By the conclusion of this course, students should have a thorough understanding of:

1. Describe and distinguish between perfect secrecy and computational security. Audience: Undergraduate

2. State game-based security definitions – IND-CPA, IND-CCA, MAC unforgeability, and signature unforgeability – in both symmetric- and public-key contexts. Audience: Undergraduate
3. Explain core primitives: pseudorandom functions, block ciphers, and collision-resistant hash functions. Audience: Undergraduate
4. Contrast foundational hardness assumptions: one-way functions, PRFs, Diffie–Hellman, discrete logarithm, and integer factoring. Audience: Undergraduate
5. Construct symmetric and public-key encryption and authentication schemes using these primitives, and prove their security. Audience: Undergraduate
6. Evaluate the security and deployment trade-offs of protocols such as authenticated encryption, key exchange, and digital signatures. Audience: Undergraduate

Meeting and Instructor Information

Instructor Mikhail Ivanov, Teaching Faculty, *Email:* mivanov@wisc.edu, *Office:* Van Vleck Hall B127.

Instructional Modality In-person

Meeting Time and Location

Lecture 2	MoWeFr: 13:20–14:10	Humanities 1131
Lecture 1	MoWeFr: 14:25–15:15	Humanities 1131

Instructor Office hours

W: 15:15–16:00 room TBA

F: 15:15–16:00 room TBA

(please check Canvas page for updates), or by Appointment.

Grader and Course Assistant We will have a grader that has yet to be determined. We will have a course assistant that has yet to be determined. Canvas page will be updated once they are assigned.

Materials

- Lecture notes will be provided.
- Useful resources:
 - Eric Bach Course notes for Introduction to Cryptography, University of Wisconsin-Madison, 2008
 - Jonathan Katz, Yehuda Lindell Introduction to modern cryptography, 3rd edition, 2021
 - Christof Paar, Jan Pelzl, Tim Güneysu Understanding Cryptography, 2nd edition, 2024, [Online through UW Library](#)
 - Simon Rubinstein-Salzedo Cryptography, 2018, [Online through UW Library](#)
 - Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman An introduction to mathematical cryptography, 2008, 2014
- It is useful to use some computational tools for Homework Assignments.
- Canvas (<https://canvas.wisc.edu/courses/498051>) is our Learning Management System. All important course information will be relayed through Canvas. Make sure your Canvas notification setting for “Announcement” is “Notify immediately” so that you receive messages promptly. Notifications settings can be accessed here: <https://canvas.wisc.edu/profile/communication>.

- Zoom (<https://uwmadison.zoom.us>) will be used for remote office hours.
- Gradescope (<https://www.gradescope.com/>) will be used to grade homework and exams. Instructions will be shared later.
- Piazza (<https://piazza.com/wisc/spring2026/sp26math435001002>), the online discussion forum.

Coursework and Grading

Lectures Lectures will be delivered in-person and synchronously three times a week during regular class hours. Lectures will involve some active learning components (e.g., problems and small group work). Attendance and active engagement is expected.

Piazza The online discussion forum, known as Piazza, will be used to discuss ideas or questions outside of class. Piazza can be used to get hints on homework problems, but no one is allowed to post entire solutions to homework assignments. However, feel free to post entire solutions to practice problems. Logistic questions are usually better posted on Piazza rather than emailed to the instructor, so all students can benefit from the answer. (e.g., exam dates and locations). Please do not use email for math questions.

You can use **private** question in Piazza to communicate with Instructor about personal circumstances.

Any posts containing comments (either positive or negative) about the instructors, the class, the students, or anything else, will be deleted. Unprofessional conduct may result in disciplinary action.

Homework Assignments will be posted on Canvas, and they will have to be submitted in Gradescope as a single pdf file. Written assignments will be several questions long and will be assigned weekly usually due roughly every Friday. Please make sure all pages are in the right orientation when you convert them. Do not hand in your rough draft or first attempt. Papers that are unreadable or disorganized cannot be graded. It is a good habit to download your submission every time and check everything is fine.

Collaborating with other students on the homework is encouraged, but you must write up all reasoning and solutions on your own (in other words, no copying). Failure to abide by this guideline could be construed as a form of academic dishonesty.

Each problem should be completed with neat, understandable, detailed solutions and explanations. Your explanations and proofs must be sound and rigorous, paying attention to detail and clarity. Computations without appropriate explanation will not receive credit, even if the final numerical answer is correct.

Late homework will generally not be accepted. Since it is quite likely that during the semester you will either experience a technical difficulty (e.g., missed the deadline, your computer shut down as you were submitting it, internet outage, etc) or a personal emergency (being sick, attending a funeral, etc), the two lowest HW scores will be dropped. You do not need to contact your instructor if such a situation does come up.

Exams The course will have three exams. We will have two evening Midterm Exams and a Final Exam, places to be scheduled by the University. Final Exam will be cumulative.

Midterm Exam 1	Friday, February 27	05:45pm–07:15pm
Midterm Exam 2	Friday, April 10	05:45pm–07:15pm
Final Exam	Wednesday, May 6	07:45am–09:45am

Students with academic or religious conflict with one of the exams should notify the instructor as soon as possible, and no later than the third week of the semester.

Calculator Policy During an exam no books, notes, calculators, cell phones, pagers, or any electronic devices will be allowed.

Grading In this course, you will be evaluated based on components described above with their corresponding percentages:

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

Grade Appeals All grade disputes must be dealt with within 1 week after receiving your grade on Gradescope. You will receive an email alert once your grade has been posted on Gradescope. Grade appeals can be done online through Gradescope, by the ‘regrade request’ option. Your regrade requests will be carefully reconsidered and may lead to raising, unchanging, or even possibly lowering the original score.

Grading Scale The following grade lines are guaranteed in advance. A percentage score in the indicated range guarantees at least the letter grade next to it.

$$A \geq 92\% > AB \geq 90\% > B \geq 80\% > BC \geq 78\% > C \geq 68\% > D \geq 60\% > F$$

Final letter grades are not curved but the grade lines above may be lowered at the end. Class attendance is not part of the grading.

Academic Policies and Statements

Usage of AI You are welcome to use artificial intelligence tools and applications (such as Copilot, DALL-E, etc.) in this class as they support the learning objectives of this course. Please be aware you are responsible for the information you submit based on an AI query (i.e. ensure your professor has allowed you to publicly post course content such as assignment or assessment prompts and that the AI generated results do not contain misinformation or unethical content). Your use of AI tools must be documented and cited to conform to this course’s expectations.

[Academic Calendar and Religious Observances](#)

[Academic Integrity Statement](#)

[Accommodations for Students with Disabilities](#)

[Course Evaluations](#)

[Diversity and Inclusion Statement](#)

[Mental Health and Well-Being Statement](#)

[Privacy of Student Records and the Use of Audio Recorded Lectures Statement](#)

[Students’ Rules, Rights and Responsibilities](#)

[Teaching and Learning Data Transparency Statement](#)