Math/Comp Sci/E C E 435-002: Introduction to Cryptography, Spring 2024

Course Information

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

Credits: 3.

Course Designations and Attributes:
Section Level Com B — False
Level – Advanced
L&S Credit – Counts as Liberal Arts and Science credit in L&S

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

Meeting Time and Location: MWF: 09:55am–10:45am in Sewell Social Sciences Hall, room 6203.

Instructional Modality: Classroom Instruction.

Instructor: Mikhail Ivanov, Teaching Faculty, *Email:* mivanov@wisc.edu

Instructor Office hours: TBA or by Appointment.

Grader: TBA

Course Assistant: TBA

Course Learning Outcomes

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

- Classical cryptosystems such as affine ciphers, substitution ciphers, Vigenére ciphers, and some block ciphers.
- General principles of cryptanalysis and some specific techniques for the classical cryptosystems.
- Modern symmetric key systems such as the Data Encryption Standard and the Advanced Encryption Standard.
- Modern public key techniques such as the RSA algorithm and Diffie–Hellman key exchange.
- The mathematics required for these topics: modular arithmetic, basic prime number theory, factorization theory, and basic probability.
- Issues involved in choice of algorithm and key size; ability to analyze performance of various cryptographic and cryptanalytic algorithms.

How Credit Hours are Met by the Course

This class meets for three 50-minute class periods each week over the fall semester and carries the expectation that students will work on course learning activities (e.g. reading, problem sets, papers, and studying) for about two hours outside of classroom for every class period. The syllabus includes more information about meeting times and expectations for student work.

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 Vigénere 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, ...). 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), ...

Course Website and Digital Instructional Tools

- Our Learning Management System is Canvas. All important course information will be relayed through Canvas. It is your responsibility to read any Canvas announcements.
- We will use Piazza. This page is a forum for you to discuss the material of this class with other students and your TAs and/or instructor. Posts to this page should be confined to questions regarding the material and logistical questions about the class (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.
- We will use Zoom for remote office hours.

Required Textbook, Software and Other Course Materials

- Lecture notes will be provided.
- It is useful to use some computational tools for Homework Assignments.

Exams, Quizzes, Papers, Homework and Other Assignments

Homework. Biweekly homework assignments can be accessed through the Canvas website. Written assignments will be several questions long and will be assigned weekly usually due on Fridays.

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. Any used computational tools should be explicitly described.

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

- Midterm Exam: Tuesday, March 12, 07:30pm–09:30pm.
- Final Exam: Thursday, May 09, 10:05am–12:05pm.

Students must notify the instructor (via email) of any conflicts with any exam during the first three weeks of class.

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	30%
Midterm Exam	35%
Final Exam	35%

Grading Scale. Final grades will be curved.

Academic Policies and Statements

- 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

Mathematica

Mathematica and Wolfram—Alpha Pro are available at no charge to UW Madison students. They are useful for: (a) solving problems, (b) obtaining step-by-step solutions, and (c) writing programs with the assistance of Artificial Intelligence. (AI chat is built in.) To get access, go to www.wolfram.com/siteinfo and enter your University of Wisconsin email. (Here are click-by-click steps if you need them: wolfr.am/UWMadison) Learn how to use Mathematica at www.wolfram.com/wolfram-u/