Course Subject, Number and Title
CS/ECE/Math 435, Introduction to Cryptography

Number of Credits
3

Course Designation and Attributes
Breadth – Natural Science,
Level – Advanced,
L&S Credit – Counts as Liberal Arts and Science credit in L&S

Meeting Time and Location
Mondays, Tuesdays, Wednesdays, and Thursdays 2:35 to 3:50 p.m.

Instructional Mode
Online

Credit hours
The three credit hours are met by four 75-minute meetings and about two hours of out of classroom student work per class session for eight weeks.

Instructor
Siddhesh Wagh, Visiting Assistant Professor,
Van Vleck B127,
wagh2@wisc.edu

Allow me 24 hours to answer your email. After that, there is a good chance that I saw your email on my phone, decided to answer when I got to a computer, then forgot because it was marked as read. In that case, please send it again.

Office hours
Monday 4:00 to 5:00 p.m., Tuesday 1:00 to 2:00 p.m., Wednesday 4:00 to 5:00 p.m., Thursday 1:00 to 2:00 p.m., or by appointment.

Official Course Description
Cryptography is the art and science of transmitting digital information in a secure manner. This course will introduce its technical aspects.
Requisites
(MATH 320, 340, 341, or 375) or graduate/professional standing or member of the Pre-Masters Mathematics (Visiting International) Program.

Learning Outcomes
By the end of this course, students should have a thorough understanding of:

• Classical cryptosystems such as affine ciphers, substitution ciphers, Vigen`ere 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.

• Advanced topics such as elliptic curve cryptography, block chains, and cryptographic hashing.

Textbook
Introduction to Modern Cryptography by Katz and Lindell.

Grading
Your course grade will be determined approximately as follows:

• Homework assignments, worth 20% of the final grade.

• 2 Midterm exams, worth 25% of the final grade each.

• Final exam, worth 30% of the final grade.

The following scores correspond to the guaranteed grades in this course. The scores may be lowered at the end of the semester by the instructor.

A ≥ 93% > AB ≥ 89% > B ≥ 82% > BC ≥ 78% > C ≥ 70% ≥ D ≥ 60% > F

Homework
Homework will be due every week on Sunday 11:59 PM and Thursday 11:59 PM, except exam weeks which will have no Sunday homework due on July 5 and July 26. Homework must be submitted to Canvas in PDF format.

Students may discuss the material with others and consult other sources but must specify their collaborators and all sources on each homework, including other textbooks and information found on websites. Failure of doing so is considered academic misconduct.

Exams and Quizzes
The midterm exams will be held during class time on Monday, July 6 and Monday, July 27. The final exam is cumulative and will be held during class time on Thursday, August 6, 2020. There will be alternate timing available for students who cannot give exam these timings.

Barring exceptional circumstances, such as a conflict with an official University-related event, unreasonable time zone issues or a last-minute medical/family emergency, these assessments must be taken at the scheduled date and time.

**Rules, Rights, and Responsibilities**

See the guides to Rules, Rights and Responsibilities at http://guide.wisc.edu/undergraduate/.

**Academic Integrity**

By enrolling in this course, each student assumes the responsibilities of an active participant in UW-Madison's community of scholars in which everyone’s’ academic work and behavior are held to the highest academic integrity standards. Academic misconduct compromises the integrity of the university. Cheating, fabrication, plagiarism, unauthorized collaboration, and helping others commit these acts are examples of academic misconduct, which can result in disciplinary action. This includes but is not limited to failure on the assignment/course, disciplinary probation, or suspension. Substantial or repeated cases of misconduct will be forwarded to the Office of Student Conduct and Community Standards for additional review. For more information, refer to https://conduct.students.wisc.edu/academic-integrity/.

**Accommodations for Students With Disabilities**

The University of Wisconsin-Madison supports the right of all enrolled students to a full and equal educational opportunity.

The Americans with Disabilities Act (ADA), Wisconsin State Statute (36.12), and UW-Madison policy (Faculty Document 1071) require that students with disabilities be reasonably accommodated in instruction and campus life. Reasonable accommodations for students with disabilities is a shared faculty and student responsibility. Students are expected to inform faculty [me] of their need for instructional accommodations by the end of the third week of the semester, or as soon as possible after a disability has been incurred or recognized. Faculty [I], will work either directly with the student [you] or in coordination with the McBurney Center to identify and provide reasonable instructional accommodations. Disability information, including instructional accommodations as part of a student’s educational record, is confidential and protected under FERPA.

**Diversity and Inclusion**

Diversity is a source of strength, creativity, and innovation for UW-Madison. We value the contributions of each person and respect the profound ways their identity, culture, background, experience, status, abilities, and opinion enrich the university community. We commit ourselves to the pursuit of excellence in teaching, research, outreach, and diversity as inextricably linked goals. The University of Wisconsin-Madison fulfills its public mission by creating a welcoming and inclusive community for people from every background—people who as students, faculty, and staff serve Wisconsin and the world.