MCS 425: Codes and Cryptography (Fall 2018)

Lectures: M–W–F 9:00 - 9:50 am in LH 101 (Lincoln Hall)
CRN number: 39218 (undergraduate) 39219 (graduate)

Instructor: Will Perkins
Email: willp@uic.edu
Office hours: 626 SEO building, Wednesdays 12pm-2pm, or by appointment

Course webpage: `http://willperkins.org/MCS425-2018.html`

Course description This course is about coding theory and cryptography, the two pillars of the science of communication. We will learn the general principles of coding and cryptography, then learn about important cryoptographic systems like AES and RSA and the mathematical principles underlying them. We will also learn about the theory and practice of error-correcting codes.
Course prerequisites: Grade of C or better in MATH 215; and Grade of C or better in MATH 310 or Grade of C or better in MATH 320; or consent of the instructor.

Required textbook *Introduction to Cryptography with Coding Theory*, second edition, W. Trappe and L. Washington, Pearson Prentice Hall. ISBN:0-13-198199-4

Syllabus

- Principles of communication theory and cryptography
- Classical cryptosystems
- Number theory for cryptography
- AES and DES
- The RSA algorithm
- Error-correcting codes
- Security protocols: key distribution, digital signatures, Bitcoin

Grading

The course is assessed by homework, one midterm, a course project, and a final examination.

(1) **Homework** (30%): we will have written homework due once a week. Points will be given only for fully correct answers, but I will return the initial submissions with comments and corrections and you will have the chance to correct and resubmit the homework for full points. No late homework will be accepted.
(2) **Midterm** (20%): we will have one midterm test (date TBA).
(3) **Course project** (20%): you will complete a course project of your own choosing and prepare a report and a presentation. The project is an opportunity to explore in depth a topic that we did not cover in class.
(4) **Final exam** (30%): the final exam will cover all the material from the course (date and time TBA).

Grades will be determined by the following scale:

$85-100\%$	**A**
$75-84\%$	**B**
$65-74\%$	**C**
$50-64\%$	**D**
$0-49\%$	**F**

Graduate students taking the course may be assigned additional homework problems.

Course Policies

Each student must turn in their own homework but you are encouraged to discuss the homework with other students and to read each others work. You must indicate clearly on your homework which students you worked with.

Class discussion, working in groups, and communicating with the instructor are all essential elements of the course. I expect all of us to treat each other with respect and courtesy in all of our interactions.

Late homework will not be accepted in general. Exceptions may be requested with good reason and advance notice.

Academic honesty

Issues of academic honesty will be taken very seriously in the this class. As an academic community, UIC is committed to providing an environment in which research, learning, and scholarship can flourish and in which all endeavors are guided by academic and professional integrity. All members of the campus community – students, staff, faculty, and administrators – share the responsibility of insuring that these standards are upheld so that such an environment exists. Instances of academic misconduct by students will be handled pursuant to theStudent Disciplinary Policy: `https://dos.uic.edu/docs/Guidelines%20for%20Academic%20Integrity.pdf`

Disability policy Students with disabilities who require accommodations for access and participation in this course must be registered with the Office of Disability Services (ODS). Please contact ODS at 312–413–2183 (voice) or 312–413–0123 (TTY).

Academic deadlines Please see `http://grad.uic.edu/cms/?pid=1000222`

Religious holidays

Students who wish to observe their religious holidays shall notify the faculty member by the tenth day of the semester of the date when they will be absent unless the religious holiday is observed on or before the tenth day of the semester. In such cases, the student shall notify the faculty member at least five days in advance of the date when he/she will be absent. The faculty member will make every reasonable effort to honor the request. `http://oae.uic.edu/docs/ReligiousHolidaysFY20152017.pdf`