MCS 425 Codes and Cryptography — MWF 2:00 - 2:50
Spring 2015 — BSB 185

Instructor Bonnie Saunders saunders@math.uic.edu www.math.uic.edu/~saunders
office hours MW 3 - 4 SEO 622 312 413-1417

Course Description

This course will cover a broad selection of cryptography and coding theory topics including classical cryptography, DES and RSA algorithms, discrete logarithms, hash functions and error correcting codes. Topics will be presented from a mathematical point of view. The number theory covered will include modular arithmetic, linear diophantine equations, Fermat and Euler theorems, modular exponentiation and logarithms. Depending on the interest of the students, we may also discuss finite fields (mainly for the AES algorithm) and/or elliptic curve cryptographic.

Requirements

Prerequisite The material should be accessible to mathematically mature students having a little background in number theory and computer programming. Some experience in linear algebra and discrete mathematics will be helpful. Technical prerequisites are C or better in MATH 215 and either MATH 310 or MATH 320.

Required Text *Introduction to Cryptography with Coding Theory* by Wade Trappe & Lawrence C. Washington (second edition), ISBN-10: 0131862391 — ISBN-13: 978-0131862395, Pearson; (July 25, 2005)

Technology The course requires calculations with large integers and programming skills will be useful. In class we will be using the Python Interpretator and doing some programming in that language. Code is provided. Students are responsible for installing Python and appropriate modules on their own computers Python. No previous experience necessary. There will be an opportunity to do more programming for the interested students. See instructor for individual concerns about programming. We will be sharing work on UofIBox. Students can get access to the MCS 425 Spring 2015 folder with an UIC netid, see `http://accc.uic.edu/service/box.`

Grading

Homework [30%] Homework and attendance. Homework assignments are due every other week. Class attendance is mandatory

Presentations [20%] Each student will research and present on an additional topic.

Midterm and Final exams [50%] Midterm and Final exams. Exams will be takehome.

Course Webpage

For more information go to `www.math.uic.edu/~saunders/MCS425_2015`