

MATH 5405, MWF 10:45 - 11:35 IN LCB 215

GORDAN SAVIN, OFFICE LCB 205

1. COURSE OVERVIEW

This course is an introduction to mathematical aspects of cryptography. An optional, but highly recommended text is *Introduction to Cryptography with Coding Theory* by Trappe and Washington. This book has some nice stuff, for example, a description of the famous german Enigma machine. Knowledge of material covered in MATH 4400 is necessary to follow this course. However, in the first two weeks we shall review material from MATH 4400 which is needed for this course: Euclidean algorithm, Modular arithmetic, Primitive roots, Discrete logarithm etc. Notes for MATH 4400 and MATH 5405 (one set of notes) are available on my web page:

www.math.utah.edu/~savin

Here is a rough list of topics that we intend to cover:

- (1) Fields.
- (2) Primitive roots.
- (3) Fields of order 2^n .
- (4) Cyphers
- (5) Data Encryption Standard(s).
- (6) Public key ciphers (RSA, El Gamal).
- (7) Primality testing.
- (8) Pseudoprimes.
- (9) Factorization attacks.
- (10) Elliptic curves.
- (11) Factoring using elliptic curves.

2. GRADE AND SYLLABUS

Grade will be based on three exams (contributing 20% each), and homework (40%). Homework assignments will be posted on my web site as we progress. The first exam will be an in-class exam. The last two will be take home exams, because they may involve considerable amount of computations. There is no final exam. Should you need some help with the material or HW, stop by my office. My office hours are MWF, 9:30 - 10:30. (Or after the class.)

3. COURSE LOG

- 01/12 Theorem of Lagrange.
- 01/14 Roots of 1.
- 01/16 Primitive roots.

01/19 Break
01/21 Discrete Logarithm.
01/23 Fields of order p^2 .
01/26 First HW due. Ring of polynomials $F[x]$.
01/28 Fields of order 2^n .
01/30 Quadratic reciprocity I
02/02 Quadratic reciprocity II
02/04 Fermat primes.
02/06 Circle group.
02/09 Second HW due. Mersenne primes
02/11 Review.
02/13 First Exam.
SPRING BREAK 03/16-20.