

Math 592 Topics in Advanced Mathematics for Teaching
Number Theory with Applications to Cryptography
Spring 2014

Wednesday 5:00 - 8:00

600 SEO

Instructor Bonnie Saunders saunders@math.uic.edu www.math.uic.edu/~saunders
office hours Monday 4 - 5 SEO 622 312 413-1417

Course Description

This course presents applications of number theory for teaching cryptography in the middle school or high school mathematics setting. No previous knowledge of number theory or cryptography is necessary. Mathematical topics include prime numbers, GCF, LCM, division algorithm, the Euclidean algorithm and the extended Euclidean algorithm. We will discuss Caesar, affine, and Vigenere ciphers; and RSA encryption. We will be exploring how the schools might expose students to cryptography and number theory.

Requirements

Prerequisite Consent of instructor.

Required Texts

The CryptoClub Cipher Handbook by Janet Beissinger and Bonnie Saunders
This book will be available in class.

Number Theory for Teachers by Bonnie Saunders.
The book is available online, see the course webpage

Recommended Texts The following books will be available in class, but you may want to purchase copies for your own use.

The Cryptoclub: Using Mathematics to Make and Break Secret Codes
by Janet Beissinger and Vera Pless.

Workbook for The Cryptoclub: Using Mathematics to Make and Break Secret Codes
by Janet Beissinger and Vera Pless.

Technology Cryptography demands the use of appropriate technology to encrypt, decrypt and crack secret messages. As well, computational power can facilitate the understanding of number theory. Students without previous experience in cryptography will be learning the classical ciphers online at CryptoClub.org. We will also explore other computer applications that can be used in high school. We will be sharing work on GoogleDocs and UofIBox. Students can get access to the MTH592 Spring 2014 folder with though GoogleApps@UIC. Accounts are free and easy to get at <http://acc.uic.edu/service/googleapps>. Students can get access to UofIBox documents with an UIC netid, see <http://acc.uic.edu/service/box>.

Homework [30%] There will be homework assignments weekly.

Presentations [40%] The course will run as a student seminar. Each student (and the instructor) will research and present aspects of cryptography and/or number theory to the class. Topics will be chosen and assigned according to student interest and previous experiences. It is anticipated that each student will have the opportunity for three presentations.

Midterm and Final exams [30%] Exams will be take-home.

Class attendance is mandatory. If for any reason a class is missed, contact the instructor by phone or e-mail in advance. The student is responsible for finding out what was covered and complete all work on schedule. Missing 2 classes will result in grade reduction and missing 3 or more classes will result in failure.

For more information: www.math.uic.edu/~saunders/MTHT592_Cryptography