Math 5405/Cryptography/Spring 2013 Syllabus

Course webpage: www.math.utah.edu/~bertram/5405

Class meets: TH 12:25-1:45 in LCB 225

Instructor: Aaron Bertram Office: JWB 302

Email: bertram@math.utah.edu Phone: 581-6964

Office Hours: TH 11-12, and by appointment.

Materials: One text for the class is online, titled *Numbers, Groups and Cryptography*, available at www.math.utah.edu/~savin/book_08_12.pdf. You may print this, but please do not distribute it. There is another required text available at the bookstore: *Introduction to Cryptography* by Trappe and Washington.

Grading: Grades will be based on homework and exams.

Homework: Problem sets are assigned each Thursday, collected the following Thursday. You are encouraged to discuss the problem sets among yourselves and with me at office hours, but the final write-up must be your own. Each problem set is worth 10 points, and only the top 10 scores will count. There will be at least 12 problem sets. There will also be assigned reading from the Trappe and Washington book, often accompanied with homework problems.

Midterms: There are two midterms, each worth 100 points.

1st Midterm: Thursday, February 14, in class.

2nd Midterm: Thursday, April 4, in class.

Final: Wednesday, May 1, 10:30-12:30 (200 points).

Total: 10 Problem Sets + 2 Midterms + Final = 500 points

Prerequisites: C or better in Math 4400 (Number Theory).

Description: This is a mathematics course on Cryptography. We will discuss various schemes for encryption and decryption of messages as well as hash functions and error correcting codes, but we will also discuss primality testing and elliptic curves, as well as other “advanced” applications of Number Theory.

ADA Statement: The Americans with Disabilities Act requires that reasonable accomodations be provided for every student with physical, sensory, cognitive, systemic, learning, and psychiatric disabilities. Contact me at the beginning of the semester to discuss whether any such accommodations are necessary.