MATH 343L, FALL 2017
APPLIED NUMBER THEORY

ANDREW J. BLUMBERG

1. Syllabus

- **Text:** An introduction to mathematical cryptography, by Pipher, Hoffstein, and Silverman.
- **Instructor:** Andrew J. Blumberg
  RLM 10.160
  blumberg@math.utexas.edu
- **Office hours:** Monday 4-5, Friday 3-4.
- **Overview:** The goal of the class is to introduce students to modern cryptography. We will cover a number of the most important public key cryptosystems and signature protocols, starting with RSA. We will discuss the number-theoretic underpinnings of these protocols, with a dual focus on explaining how to implement these cryptosystems efficiently and how to think about why breaking them is believed to be infeasible.
- **Prerequisites:** 343K or 328K. But mostly, mathematical maturity and a willingness to work hard.
- **Grading policy:** The final grade will be determined based on:
  (i) Quizzes, 5%,
  (ii) Homework, 15%,
  (iii) two midterm exams, 40%,
  (iv) and the final paper 40%.
  Plus/minus letter grades will be assigned.
- **Homework policies:** Homework will be assigned on Tuesdays, and due by 5 pm the following Tuesday. Late homeworks will not be accepted without prior permission. Some homework will involve programming exercises.

  I encourage working in groups to solve the homework problems. However, do not write down anything that you do not understand. A good rule of thumb is that if your homework was destroyed by fire, it should be easy for you to rewrite it without help from anyone else.
- **Attendance:** I expect that students will attend all classes.
- **Midterm:** There will be two in-class midterm exams during the semester. The exams will be held Thursday, October 5th and Thursday, November 16th.

- **Final project:** The final project will involve implementation of a cryptosystem from a recent research paper. The final project will be due on Monday, December 18th, at 5 pm.
- **Class web site:** Handouts, homework, and other miscellaneous announcements will be posted to the class website at:
`http://math.utexas.edu/ blumberg/343.html`
- **Students with disabilities:** The University of Texas at Austin provides upon request appropriate academic accommodations for qualified students with disabilities. For more information, contact the Office of the Dean of Students at 471-6259, 471-6441 TTY.

RLM 10.160
E-mail address: `blumberg@math.utexas.edu`