Math 341 (Discrete Mathematics II)
Spring 2017
TR 3:00-4:20 p.m., DRL 4C2
University of Pennsylvania

Welcome to Math 341! This semester we're going to have a great time studying cryptography and the mathematics behind it.

Instructor: Dr. William Simmons, DRL 4C3, `wsimmo@sas.upenn.edu`.

Office Hours (held in DRL 4C3): Tuesdays 10:30-11:30 a.m.; Wednesdays 1-2 p.m..; others, time permitting, by appointment.

Textbook: (The replacement text) Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, *An introduction to mathematical cryptography*, 2nd ed., Springer.

Note: The first edition is freely available at `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.9999&rep=rep1&type=pdf`. It should be fine if you prefer to use this rather than get access to the second edition; however, we'll have to work around a few differences in exercises, etc.

Other suggested reading: (The original text) Johannes A. Buchmann, *Introduction to Cryptography*, 2nd ed., Springer. (Available in the Math and Astronomy Library here in DRL.)

Important dates:

- Add deadline: Monday, Jan. 30
- Drop deadline: Friday, Feb. 17
- Withdrawal deadline: Friday, Mar. 24
- Last day of classes: Wednesday, Apr. 26

Homework and in-class board work: To learn mathematics you need to think hard about the material over an extended period of time. You also need to ask questions and explain your reasoning. That's why homework and in-class board work form the largest portion of your grade.

Written work: Weekly homework is generally due at the beginning of class on Thursdays; any changes will be announced in class. *Late work will not generally be accepted, so please talk to me ahead of time if you face a legitimate extenuating circumstance.*

Write neatly and show all relevant work needed to understand your thought process. Incomprehensible and/or messy answers may not receive credit. Be sure to use complete sentences and correct grammar in your work.

In-class board work: The idea of the in-class board work is to share insights, solutions to homework or other interesting problems you encounter, and to ask each other questions. Most days during

class we will have a short time (usually not more than 20 minutes) for board work. You should let me know at least two days in advance what you want to present and how much time you need. (Usually 5 or 10 minutes; if it will take less than that, try adding another problem or going deeper. If you need more time, you can split it up or cut out some details, but don't sacrifice the "meat".)

There aren't too many guidelines; just prepare one or more problems (not super-easy, though) or present a concept with examples and calculations. Explain things as best you can and try to answer questions that come up. Don't worry if you don't have all the answers; beyond the basic solutions you prepared, just think of it as leading a brief discussion.

You are required to present at least two times during the semester. Beyond that, each extra presentation will make up for one to two missed homework problems or one-half to one missed wiki contribution, depending on how in-depth the presentation is.

Course wiki: `http://math341sp17.wikidot.com/` I will send you an email invitation to our course wiki. This is an experimental part of the course that I hope will be enjoyable and help you learn together. You will write entries, work examples, and hash things out (both what we cover in class and what you explore outside of class). The idea is to gain greater understanding by writing things down and interacting with others over cryptography and the associated mathematics. The wiki will be private (at least during the semester), so only the class will be able to view and edit it.

Every Tuesday you will send me a brief email with the text of your contribution since the previous Tuesday. (You don't need to make an entry during the week of spring break.) There's no exact formula for how much you need to do each week; something on the order of two significant examples or exercises, with appropriate explanation, would be enough. You should focus on mathematical details, but some weeks you can give exposition of concepts, protocols, and technologies if you wish. It's also great if you can include more elaborate things (e.g., embed a Sage widget or some other utility for making calculations or visualizations that others in the class can then use); if something like this requires more technical effort, you don't have to include so much written content. It's okay if something is a work in progress; just make it clear where things are going if they're not neatly tied up during the current week.

Use this assignment as a chance to map out and record your study of cryptography as well as provide value to your classmates. Explore topics that capture your interest even if we don't go over them in class. You should also go deeper into the things we do cover. If you struggle with some concept or problem for awhile and then become illuminated, that's a good candidate for a contribution. You can certainly work together on some entries or mini-projects you pursue within the wiki, but in your email you should describe what you contributed.

No LaTeX, HTML, or other coding experience is assumed. We will talk about the basics to help you get started. If you do have such experience, a few times during the semester you may volunteer to typeset or program features on behalf of classmates in lieu of a weekly contribution.

More details to come in class and on the wiki itself. Above all, let's make it fun and learn something in the process.

Exams: No exams! Your job this semester is just to work hard, understand the material, and contribute through class discussions and the course wiki. (The wiki assignment takes the place of a final exam.)

Attendance: The success of the class depends significantly on your participation, especially

through board work and the questions you ask and answer. We will take attendance each day, but you have two free absences (whether "excused" or "unexcused").

Grades: Your grade will be determined by the following breakdown:

- 60% homework and in-class board work, 30% wiki, 10% attendance.

Actual letter grades are calculated as follows:

- A: Earned 80% or more of available points
- A−: Earned between 74 and 79% of available points
- B+: Earned between 69 and 73% of available points
- B: Earned between 64 and 68% of available points
- B−: Earned between 59 and 63% of available points
- C+: Earned between 54 and 58% of available points
- C: Earned between 49 and 53% of available points
- C−: Earned between 44 and 48% of available points
- D: Earned between 39 and 43% of available points
- F: Below 39% of available points

Errors in recording and/or grading must be brought up within a week of the assignment being returned. *Grades are fully determined by the numbers, so please don't request exceptions.*

You and Your Work

- (Background knowledge) You don't need to have taken Math 340, but it is helpful to be familiar with very basic combinatorics and probability. (We'll review mathematical prerequisites as we go along.) You should also have some experience with reading and writing basic mathematical arguments, though you will get plenty of practice throughout the semester. Most of all, you need to be curious about mathematics and cryptography and be willing to dive into the material we discuss.
- (Getting help) Study the assigned material before class. Find out what you don't understand, and bring questions! Beyond that, be sure to take full advantage of office hours. Talk to me early when challenges arise so that we can figure out how you will achieve success with the material. Get to know your classmates and work together to figure things out.
- (Academic Honesty) You must write up your own work so that it represents your own understanding. You are encouraged to study together, talk about problems with others, look at math resources online, etc., but you need to write up homework problems and wiki work on your own (i.e., no copying, whether it be another student's solution or something online). You should also not allow your own work to be copied. Infractions will result in loss of credit for the assignment and, depending on the situation, university discipline. For more details, see `www.upenn.edu/academicintegrity`.

- (Accommodations) Please talk to me as soon as possible about accommodations through Student Disabilities Services (Stouffer Commons, 3702 Spruce Street, Suite 300, `http://www.vpul.upenn.edu/lrc/sds/`), scheduling conflicts with religious holidays, athletic events, etc., or working around health issues and other situations.