Math 116 Class Guide - Fall 2015

Yan X Zhang
UC Berkeley

August 21, 2015

For all basic information such as instructor name, textbook, and office hours, see the class **website**: `http://math.berkeley.edu/~yanzhang/classes/math116f15`

1 Should I Take This Class?

Goal of the class: To cover the mathematical side of mathematical cryptography. This is a mathematics class; we focus on the undergraduate-level math that makes it easier to understand cryptography, mostly number theory, but also combinatorics, algebra, etc. and formalize cryptographic protocols in a mathematical way. We occasionally talk about the computer science, implementation, general codebreaking/history, etc., but those are not the core of the course.

Prerequisites / helpful mathematics to already have: the only absolute prerequisite is proofwriting; this is something you will need and will be graded on, but I will not spend class time on it. Everything else I put in the list are things that **I will spend time covering, but faster as compared to the actual cryptography content**.

For each of these, I give some words as a "litmus test," for which if you really know the words, that part of the course will be easier for you. If you recognize most the words, you should be fine (**alternatively: if you haven't seen the words but are currently taking a class that covers those topics, you should be fine too by the end. If you have taken the relevant class and forgotten all the words, I promise that it gets easier the second time!**). If the words are all alien to you, you should **expect a few extra hours on those weeks** when we cover the relevant material, but should be fine.

Here is the list of topics that are either required or will be helpful. I expect most of you to recognize about 1/3 to 1/2 of these words.

- Proofwriting (knowing that you're graded on proof, not just "the answer") and basic proof concepts is the only prerequisite. **The rigor of your proofs (not just the correctness of the ideas) will be part of your grade**, on both homeworks and exams. Having done well in Math 55, and/or having completed a proof-focused course such as Math 104 / 113, would give you adequate prep (litmus test: "for all," "there exists," induction, proof by contradiction, counterexamples, pigeonhole).
- Algebra (litmus test: group, group action, ring, equivalence relation)

- Counting (litmus test: binomial coefficient, Pascal's Triangle, inclusion-exclusion)
- Probability (litmus test: random variable, variance, expectation, independence)
- Basic computer science (litmus test: big-O notation, P, complexity, data type)

Some of you may be surprised that I don't include number theory; this is because that is the main kind of mathematics we see in this course, so I will not be rushing any of the number theory and thus it does not belong in the above list. It obviously helps you, however, if you have seen number theory.

2 Course Content and Style

We will aim to cover material roughly around Chapters 1-4 of HPS (the textbook by Hoffstein, Pipher, Silverman), though I will try to insert some of the main ideas from Chapters 5 and 6 and many ideas not taken directly from the text, such as how a computer scientist or an industry cryptographer may look at cryptography. **Thus, the lectures are *not* restricted to the text, though they "mostly" overlap; please make up material with your classmates (probably through Piazza) if you miss some days of class.**.

This course will include lot of communication during lectures (and also office hours!). As such, there will be a class participation grade.

- The single mantra I will use to decide the participation grade is: **"Is this student actively trying to learn and contributing to a classroom atmosphere where everyone can learn?"**.
- As a guideline, someone who is not distracting / disruptive of others who occasionally asks and answers questions in an earnest attempt to learn (as opposed to, say, showing off), and is reasonably active on Piazza will obtain around 80%.
- I understand some people are quieter than others. However, I cannot see your participation in class if you are not speaking. I hope the other avenues (like Piazza) give you more comfortable options to interact with the class.
- On the other hand, talking too much as to not let your classmates participate, or answering things too quickly (**especially without raising hands**) and not giving time for your more deliberate classmates think, are also examples of disruption.
- Asking questions to the instructor counts for classroom participation (because you are engaging with the material), but only if done in class or through Piazza (because this way everyone benefits). **Piazza participation is a big part of classroom participation, unless you are obviously only posting on Piazza for the sake of posting.**

3 Grading

- Class Participation 20%
- Homework 20%
- Midterm 20%
- Final 40%

The final grade will be curved after averaging. I reserve the right to ignore any questions about grading, especially boundary cases.

A note on classroom participation: people frequently negotiate grades for extreme situations, steady improvement after a rocky start, etc. I think these are legitimate concerns and it is impossible to formalize rules for them. Instead, I think of "Class Participation" as basically the way of turning those murky ideas into points and to tiebreak boundary situations between letter grades. It is still not objective, but I hope it gives you an idea of how much wiggle room you have. (the typical range of class participation for me has been around 10% of the grade)

4 Exams

There will be two exams, a midterm and a final.

Exam dates are **not negotiable**. **If you must miss the midterm, the final exam grade will replace that of the midterm exam.**

As a bonus, **the final exam grade will also replace the midterm exam if you score higher on the final exam.**

5 Homework

Academic dishonesty will not be tolerated. **All homework must start (say in the margin) with a note on from whom/what source you obtained information/help regarding the homework. People and the internet are both sources.** We may disqualify a homework completely if we have sufficient reason to believe that the information you supply is incomplete.

I strongly encourage discussing homework problems with your classmates, but you must write down your own work, in your own words, and cite your classmates. I also encourage having at least one member of your group with some knowledge of computer programming / symbolic manipulation, so you can play with the exercises via a computer. **I hold the right to give problems that *require* a computer to solve. In this case, it is your responsibility to either learn the requisite skills or find classmates (say via Piazza) who have them.**

Homework will be given weekly and given at the beginning of class. Late assignments will not be accepted. Assignments may be slid under the office door (Evans 813) and will count only if I find it before **leaving for class** on the due date, not after class has begun.

There will be no extensions of any kind; in preparation for difficult situations / accidental forgetting of turning in homework / etc., I will remove two of the lowest homework grades. I sympathize with your emergencies and personal problems, but I must separate their consideration from classroom policy.

Most homework will consist of proofs – proofs should be readable, like English prose, so they must be complete sentences when spoken aloud (see the textbook for examples).

6 Other

If you will need special accommodations approved by the Disabled Student's Program, make sure I get notice as soon as possible. **I cannot accomodate last-minute requests.**

Incomplete "I" grades are almost never given. George Bergman has given a clear overview of the system of "I" grades at `http://http://math.berkeley.edu/~gbergman/ug.hndts/I_info.html`.