MATH 116: CRYPTOGRAPHY

INSTRUCTOR: TONY FENG

Class venue: MWF 11:10am-noon in Wheeler 204. Attendance is encouraged but not mandatory, except for the last two weeks of class, when it will become mandatory. *Please do not come to class if you feel sick.*

Office Hours: Fridays 4pm in Evans 891. Additionally, Zoom office hours Tuesdays 5pm at `https://berkeley.zoom.us/j/8047543587`. Office hours will commence on Wednesday, January 29.

The Zoom office hours are introduced to accommodate sick/quarantining students.*Please do not come to in-person office hours if you feel sick.*

E-mail: fengt@berkeley.edu. Please begin the subject line with "[Math 116]". I aim to respond within one business day.

Course website: bCourses, `https://bcourses.berkeley.edu/courses/1533302`.

Zoom room: `https://berkeley.zoom.us/j/8047543587`.

Course description. This will be a somewhat idiosyncratic course about mathematical aspects of cryptography, the study of secure communication.

The first part of the course will be cover classical cryptosystems of historical significance, including the Lorenz cipher and Enigma machine. In order to understand them, we will learn the mathematical foundations of probability theory, information theory, and statistical inference.

The second part of the course will cover more modern developments in public key cryptography, such as such Diffie–Hellman and RSA, and their attendant foundations in abstract algebra.

A detailed weekly list of material to be covered can be found in the "Schedule.pdf" document.

Textbook. The main reference will be lecture notes distributed by the instructor. There is no required textbook, but the following resources may be useful:

- Hoffstein, Pipher, Silverman, "An Introduction to Mathematical Cryptography".
- McKay, "Information theory, Inference, and Learning Algorithms"
- Vaudenay, "A Classical Introduction to Cryptography".

Specific references for each topic can be found in the "Schedule.pdf" file. I encourage using electronic copies of books, which can be found online via the usual methods. (See the instructor if further clarification is needed.)

Remote lectures. If class cannot be held in-person for whatever reason, lectures will be given remotely over Zoom at `https://berkeley.zoom.us/j/8047543587`. The same applies to office hours. I will provide as much advance notice as possible if this becomes necessary.

Pre-requisites. The official pre-requisite is Discrete Mathematics at the level of Math 55. The course will draw on combinatorial analysis, probability theory, and abstract algebra, which will be reviewed in class.

Grading. Grades are based on the following division:

- 25% from homework. Problem sets will be due Fridays at 11:59pm, on Gradescope. The two lowest grades will be dropped. *Extensions will not be granted except in truly exceptional cases.*
- 25% each from two midterms.
- 25% from final project. The final project will involve writing a paper and giving a presentation during the last two weeks of the semester (including Reading Week). Projects can be done jointly in teams of up to 4 people.

Grades will be curved upwards if necessary, in accordance with historical grade distributions for this class, so that the median grade is *at least* an A-. **Note that there is no final exam.**

Policies.

- Students are expected to adhere to Berkeley's academic integrity policy. Examples of cheating include copying off of your classmates, or other resources (possibly online). This class will implement a "two strike" policy:
  - The first strike will result in an automatic failure of the assignment in question.
  - The second strike will result in an automatic failure of the course, and a formal report to the university.
- Problem sets must be submitted on Gradescope. *Late assignments will not be accepted under any circumstances.*
- You are encouraged to discuss problem sets with your classmates, but *you must write up solutions by yourself.* This means that you may not look at anybody else's solutions as you write your own. You are free to use the course references or other outside sources, *as long as you acknowledge them properly.*
- Exams are in-class and closed-book. Notes, cheat sheets, and electronic devices will not be allowed in exams.
- Eating or using cell phones in class will not be tolerated. Laptops, iPads, etc. may be used *for note-taking purposes only.* If you come to class, please do so on time and stay for the whole period.
- AI: you may use tools such as ChatGPT to help your learning. However, be warned that such tools are currently quite unreliable. Furthermore, *copy-pasting homework answers from such tools will be considered plagiarism.*

Schedule. Please see "schedule.pdf" for a detailed schedule of topics that will be covered in class. Important dates are highlighted here.

- March 7 – Midterm 1.
- Marc 21 – Deadline for submitting final project proposal, teammates, and references.
- April 2 – No class.
- April 23 – Midterm 2.
- April 28 – Final presentations begin.
- May 9 – Final projects due.

If a personal or medical issue is interfering with your studies:

- Contact your medical provider if you need medical attention.
- Please do not come to class if you are sick. Instead, read the lecture notes or textbook for the sections you missed.
- Email me.

If you need disability accommodations: If you need disability-related accommodations in this class, if you have emergency medical information you wish to share with me, or if you need special arrangements in case the building must be evacuated, please inform me as soon as possible. Also, please make an appointment with the DSP office to discuss the appropriate procedures. More information is available on their website: `http://dsp.berkeley.edu`.

Tutoring. For tutoring and finding study groups, please visit `https://slc.berkeley.edu/mathematics-and-statistics`.