MATH 165 FS CRYPTOGRAPHY AND SOCIETY
Fall 2020

INSTRUCTOR

Prof. L. B. Pierce, Mathematics Department, Duke University, pierce@math.duke.edu

CLASS MEETINGS

8:30am–9:45am Monday and Wednesday for lecture/discussions

OFFICE HOURS

further details arranged with the class

TEXTBOOK

The Mathematics of Encryption, An Elementary Introduction, Margaret Cozzens, Steven J. Miller

ADDITIONAL READINGS AND DISCUSSION MATERIAL

Supplementary reading material: items on philosophical concepts and items from current media sources will be distributed by the instructor and also by students, periodically throughout the semester.

FORMAL DESCRIPTION

Introduction to topics in mathematical cryptography, and the role of cryptography within society, in both historic and modern contexts. Cryptographic systems studied will include: early historical ciphers; the Enigma machines of WWII; modern public channel cryptography. Students will learn: to encode/decode using each system; to quantify the complexity, strength, and weaknesses of each system; to use elementary techniques from combinatorics, graph theory, abstract algebra, and number theory; about the role cryptography plays in human society.

LEARNING ACTIVITIES FOR SKILL DEVELOPMENT

The main lecture/discussions will be focused on mathematics, but will be consistently interspersed with discussions on historical, philosophical, and societal topics. Students will develop skills through three main interlocking types of assignments.

Mathematics-focused assignments will include problem sets and reading assignments in the primary textbook, which includes mathematical exposition, mathematical exercises, and historical discussions. The problem sets and readings will develop knowledge of concepts, fluency in manipulating concepts, and proof techniques. These will be solidified in discussions taking place during class meetings, with peers, and with the instructor.

Writing-focused assignments will consistently develop two kinds of writing: (A) technical writing that rigorously documents mathematical processes—a necessary skill for success in higher level math courses; (B) writing that communicates technical topics, and analyzes their societal impacts, for a lay audience. Technical writing skills will be developed via (1) problem sets that are rigorously graded for their written presentation as well as mathematical correctness; (2) evaluating each other's problem sets for presentation; (3) collaborating in groups to write rigorous mathematical solutions. Non-technical writing will be developed by (1) performing close readings of exemplar articles written for a lay audience; (2) writing short essay responses; (3) evaluating and discussing each other's writing; (4) the semester-long development of a final paper.

In addition to mathematics-focused assignments and writing-focused assignments, we'll also be using oral activities. Oral expression activities will take place during lecture/discussions, during meetings with peers and the instructor, and in the development of group projects. These oral activities will provide further chances to solidify learning, deepen understanding, and improve fluency. Talking about what we are learning is itself a way to learn!

ORGANIZATIONAL MATTERS

INTERACTION AND PARTICIPATION

Interaction: Students will have many opportunities to engage with the professor and with the class group within the context of each type of activity. Interaction will occur in lecture/discussions, question and answer sessions, formal written assignments, short oral student presentations, short written assignments, peer-feedback interactions, online office hours, chat groups, an online "forum," email, and more.

Participation: active participation is the best way to learn the most, and to enjoy any university course! During a pandemic, participation may sometimes mean something different than it normally would. The best way to participate is still to join in the lecture/discussions when they are occurring, and to ask questions and participate in the discussion. Some assignments (such as short oral presentations) will also naturally work best if you can present them live at the online lecture/discussions.

However, we understand that there can be circumstances this semester that prevent this. If synchronous participation is absolutely impossible, either long-term or short-term, please contact the professor right away and we will discuss appropriate alternatives. If the problem is short-term, email the professor before the lecture/discussion occurs. If the problem is long-term, you'll also need to contact your dean as soon as possible.

MODE OF LECTURE/DISCUSSIONS

The lecture/discussions will take place online (via Zoom, accessed in Sakai) at the appointed class times. It is preferred that students participate "live" (synchronously) with these lecture/discussions each class session. (Under normal circumstances, attendance would be "mandatory.") If this is not possible, email the professor before the lecture/discussion.

Certain lecture/discussions may be recorded, stored for up to 2 weeks, and accessed with a password set by the professor. Certain lecture/discussions which feature student discussions may not be recorded, for reasons of privacy and to encourage students to feel free to talk about complex subjects. An ongoing recording can also be paused. You may ask the professor about this at any time.

In all cases, it is against the course code of conduct to download any videos of the lecture/discussions.

MODES OF COMMUNICATION

Lecture/Discussions: Students are always welcome to ask questions during the lecture/discussions. The lecture/discussions take place on Zoom via Sakai at the appointed class times.

Office hours: Each week there will (typically) be a virtual office hour with Prof. Pierce, at a time to be announced. This will be held on Zoom via Sakai. There will be a sign-up page to sign up for a time in advance, so that we can gauge the level of attendance in advance. Office hours are typically more stimulating if multiple people attend and ask questions—we learn from each other's questions. But any student can also request a portion of the office hour for a private chat if needed.

Chat on Sakai: students are welcome to use the Chat feature on Sakai to ask questions to the class, at any time. The Chat is viewable by all members of the class, and class members are welcome to answer anyone's question.

Forum on Sakai: this is a better organized way to chat. You can start a conversation thread, such as "Problem Set 1." This can be a good place to get help from peers on problem sets or with practical information. Please make sure this remains a welcoming and respectful space for all.

Asynchronous office hours: In addition, there will be a forum called "Asynchronous Office Hour." You can put a question here. Prof. Pierce will check for outstanding questions at fixed times each week that will be announced by email.

Email: If all of the above methods haven't provided an answer, students can email the instructor directly. All emails should include the words Math 165FS in the subject line.

TYPES OF LEARNING ACTIVITIES

PROBLEM SETS
The goal of problem sets is to help students achieve a solid understanding of mathematical concepts, to gain fluency in manipulating those concepts, and to gain proficiency in formal mathematical writing and proof methods.

Problem sets will be made available on Sakai (typically each Wednesday), and completed problem sets must be submitted to dropbox on Sakai before the beginning of lecture period on the due date. The due date will (typically) be the following Wednesday.

Problem sets may be hand-written and submitted as a scanned PDF document (note: one document, not a series of pictures as separate files), or typed in LaTeX and submitted as a PDF. In either case, the file must be named PSn_LastName.pdf, with "n" replaced by the number of the problem set, and "LastName" replaced by your last name. For example, if the professor were submitting problem set 3, the file name would be PS3_Pierce.pdf.

We *encourage* students in this course to discuss their work on the problem sets in groups, for example via Zoom meetings in Sakai, or via Chat Room or Forum in Sakai. However, each student must present a complete written solution to each problem, in their own words, without reference to the written solution of any other person. *On each student's written problem set, the student must name the students or other people with whom the student had significant discussions about the problems.* Written sources (such as books and online sources other than the course textbook) that contributed significantly to the student's understanding of the problem should also be cited.

Unless otherwise noted on a particular assignment, it is acceptable to verify your work on problem sets with a computational aid.

ORAL ACTIVITIES
The goal of oral activities is to help students use the oral modality to solidify the understanding of mathematical, historical, philosophical, and social topics addressed in the course, and to gain proficiency in communicating those topics spontaneously in discussions.

These activities can include the following synchronous activities: participation via questions/answers in lecture/discussions, online office hours, brief oral presentations to the class on mathematical, historical, philosophical, and social topics, brief oral assessments of mathematical concepts, and discussions in groups with peers.

Brief oral assessments of mathematical concepts will be scheduled in advance and will take place online in a 1-to-1 meeting with the instructor.

If synchronous participation in a specific activity is absolutely impossible, please contact the professor as soon as possible to discuss possible substitutes for each specific assignment.

SHORT WRITTEN ACTIVITIES
The goal of short written activities is to help students use the written modality to formulate questions about complex ideas, to solidify the understanding of mathematical, historical, philosophical, and social topics addressed in the course, and to gain proficiency in communicating in a nontechnical way to a "lay audience."

These activities can include writing short responses or formulating short questions about reading material that the professor provides, reading material that the student is asked to collect from the media, or discussions that have occurred in lecture/discussions. This can also include plans or drafts of longer projects.

GROUP PROJECTS
The goal of group projects is to deepen the learning process through communicating with learning partners. Both asking questions and answering questions with peers shows us what we know, solidifies

what we know, and helps us learn what we don't know. In addition, working in groups helps to form community bonds, which in turn enable us to have deeper discussions and to tackle harder problems.

Group projects can include: peer assessments of technical written work (such as a problem set), peer assessments of drafts of the final paper, collaborative work on challenge problems, and the development of a code-breaking treasure hunt for a selected grade (elementary or middle school).

FINAL PAPER

The goal of the final paper is to help the student synthesize all of the material of the course, and all of the modes of thinking developed through the learning activities, into one body of work.

The final paper (10–12 pages single spaced excluding bibliography, 12 point Times New Roman font, 1 inch margins) will be on a topic that involves all three of (a) mathematics, (b) cryptography, and (c) modern society. A successful final paper will explain a mathematical topic in a way that is appropriate to a lay audience; explain a cryptographic system which uses that mathematical topic; situate the development of that particular cryptographic system historically; explore the interaction of that cryptographic system with modern society; include philosophical approaches encountered in class.

A one-page bullet-point outline of the paper and drafts of certain sections of the paper will be due at certain points throughout the semester, and will receive both student and instructor feedback. Detailed instructions will be made available early in the semester.

RESOURCES

THE ACADEMIC RESOURCE CENTER
The Academic Resource Center (ARC) offers free services to all students during their undergraduate careers at Duke. Services include Learning Consultations, Peer Tutoring, Learning Communities, ADHD/LD Coaching, Outreach Workshops, GRE/MCAT Prep, Study Connect, and more. The ARC writes: "Because learning is a process unique to every individual, the ARC works with each student to discover and develop their own academic strategy for success at Duke." Find out more here: ARC or write to arc.duke.edu.

THE WRITING STUDIO
At the Writing Studio, students will find a place beyond the classroom to work collaboratively with an attentive, non-evaluative reader. Students can visit at any stage in the writing process, including before starting to write. Visit their website Writing Studio to schedule an online appointment and to learn more about Studio resources. This may be useful for the Final Paper.

DUKE LIBRARIES
Duke Libraries has special services for First Year Students. Learn how to get the most out of the extensive libraries, and to find and cite the resources you need. Find out more here: Library services for First Year Students.

REGULATIONS

ATTENDANCE
Students are expected to participate synchronously whenever possible.

ASSIGNMENTS
Students are expected to submit all assignments on time.

LATE OR MISSED WORK, SHORT-TERM OR LONG-TERM CHALLENGES
However, we understand that this semester may throw us many unexpected challenges, and even the semester we expect to have is already challenging. The key will be good communication. If you expect that you cannot participate in the agreed way, or circumstances mean that you need more help than you can find on your own, or that you cannot turn in an assignment because of a significant life-affecting event, it is better to inform the professor as soon as possible. If this is a short-term problem, email the professor immediately, and preferably *before* the lecture/discussion or deadline you are about to miss.

If something extraordinary occurs that will drastically affect your participation in the long-term, please contact both the professor and your academic dean by email as soon as possible. If at all possible, we will try to make arrangements to work with you so that you can complete the course.

Any challenges that affect your participation and potential success can be discussed with your dean, and with the professor. We have experience with helping students succeed in courses even with incredible and unexpected external challenges. *But this always requires good, open, honest communication and documentation, preferably ahead of time.* Starting earlier with this is much, much better than coming to us after the fact.

To say it again... What's the big message: If you are facing a sincere challenge, the instructor and the university resource offices and administrators will work with you to get you through. Get in touch sooner rather than later!

ETHICS
Students are expected to adhere to the Duke Community Standard.

It is acceptable to seek out clarifications of concepts and definitions by consulting other textbooks or online sources, and asking your classmates and the professor. However it is not acceptable to intentionally seek out and copy solutions to the precise problems on the problem set, either in other texts, materials from previous semesters, or online sources. Doing so is an infraction of the Duke Community Standard. You can always ask the professor for clarification on this policy if you have a question.

If a student is responsible for academic dishonesty on a graded item in this course, then the student will have an opportunity to admit the infraction and, if approved by the Office of Student Conduct, resolve it directly through a faculty-student resolution agreement; the terms of that agreement would then dictate the consequences.

If the student is found responsible through the Office of Student Conduct and the infraction is not resolved by a faculty-student resolution agreement, then the student will receive a score of zero for that assignment, and the instructor reserves the right to further reduce the final grade for the course by one or more letter grades—possibly to a failing grade—at the discretion of the instructor.

In addition, students are expected to adhere to a Course Community Standard, which the class will develop at the beginning of the semester.

GRADING

GRADING

The following percentages are approximate:
Problem sets: 15%
Participation and oral assignments: this can include participation in lecture/discussions, office hours, oral presentations, oral assessments of mathematical concepts, group discussions, contributions on chat/forum, or appropriate substitutes arranged by the professor if synchronous participation is impossible; this also includes upholding the community standard in all aspects of engagement with the course: 20%
Shorter written assignments: this can include short responses to readings and prompts, drafts of longer assignments, etc. 15%
Group projects: this can include group work on challenge problems, peer feedback assignments, and other collaborative projects such as the "treasure hunt": 20%
Final paper: 30%

An outline of key assignment due dates will be made available early in the semester.

THE COURSE GRADE

This course will assign either the grade S (Satisfactory) or the grade U (Unsatisfactory).

The above percentages will be used to calculate a final score for the course. This score will be used to determine a final grade, which will either be S or U. An S grade corresponds to a score that would be on the level of a letter grade equivalent to a C− or better. A U grade corresponds to a score that would be on the level of a letter grade equivalent to a D+ or worse.