

A portion of a Caesar cipher

# Mathematical Cryptography

MATH B399-02

## Course info



Tuesday & Thursday



8:25–9:45a



Park Science 328

## Instructor



Professor John Bergdall



Park Science 334



jbergdall@brynmawr.edu



x5356



Office Hrs:  
Mon TBD  
Wed TBD

## Prep. Meetings



Mondays



TBD



Park 334

## Essential statement

We welcome your participation in whatever form it takes, with the hope that you enrich our space with your identities.

We pledge our attention and a sincere approach to your experiences. We ask that you also acknowledge the different identities and experiences of your peers, and you pledge to respect each of them fully.

As a class, we will develop a strong system of norms to observe. If at any point you feel less than empowered in your learning or less than comfortable in the environment, we encourage you to interface with us in order to provide myself, yourself, and your peers an opportunity to recommit and revisit these norms.

## Essential questions

- What history of ideas has led to the current state of encryption?
- How has technology enhanced, or obstructed, secure communication?
- What mathematical problems, big and small, are leveraged in cryptography?

## Overview

This course is a senior experience in mathematics. We will learn, together, the basics of the mathematics that underlies cryptography, and we will work, together, to learn practical skills in computer programming.

Cryptography itself is an ancient art. Secret codes have always played an important role in communication. Modern encryption and decryption, working together to keep sensitive information safe, are important for each of the world's citizens' privacy. The most famous example of this is the means by which anyone can transmit banking and credit information along public channels, having never personally met their partner in communication. The breakthrough that led to our current technology is called *public key cryptography*. It was invented in the 1970's. Its introduction and features will form the scientific heart of this course.

History happily shows us that while encryption is important to understand, it is also crucial to consider the safety of encryption systems. Each new technology presents an opportunity to both improve encryption techniques and, at the same time, make them obsolete. So as we study modern cryptography, we will also devote energy to understanding the constant back and forth between safe and unsafe mechanisms of creating privacy.

We will also learn new skills and reinforce old ones. A major component of this course will be student-driven presentations. You, and your peers, will be responsible for the material we will learn. Alongside theoretical learning, we will also develop a practical understanding of how to make computations and write programs in the programming language python. Python is one of the most agile languages for scientific computing and thus one of the most useful for students to learn.

All of your work during the semester will culminate in a term project that will blend the scientific knowledge of cryptography, the lessons you have drawn from history, and the technical skills you have developed with a computer. With of each of these ingredients, you will take on the ultimate task of developing an independent research project that will let you deeply dive into a single crypto-related topic.

## Learning goals

In MATH B399, you will:

- Trace the history of mathematical ideas alongside emerging technologies.
- Work in a group to understand advanced mathematics.
- Prepare, deliver, and participate in thoughtfully developed presentations.
- Use a computer computationally through the programming language python.
- Propose and develop an independent research project in cryptography.

# Qs

## ? How do we address you?

! If you need to name me, I go by Professor Bergdall or John (not Dr.). If you write me an email, include an appropriate greeting (Dear/Hello...) and closing (Sincerely/Thank you...). If you need to reference me with pronouns, I use he/him/his.

## ? Programming background?

! You do not need a background in programming. The skills you have developed in logical thinking, through your mathematics courses, will serve you well enough. The technical challenge of writing computer programs will be learned through tutorials and student-driven exercises.

## ? Prior knowledge?

! The biggest concept you will want to draw on from your prior experience is your understanding of the modulo relation on the integers. If you are hazy on that, don't worry! We will cover the background we expect you to have, some of it rather quickly.

## ? What are you most excited about?

! eubbr fhmsy ehmlu jrthi wuyhe yuckyw qihrv wuizq ezugm kmuwp mlfrb mrahz mfmhz epvfj marwm jthrp kqeph zmrwq ezugm pmgmw hzrtv zhhzw rtvzb upqra hzmeh irwhu phlmh uekfh zuhdm dekl efytf fbqrh zmwzr imefh zuhqr tdekk ammkm birdm wmlhr mbjwu ymhzm tfmra yrbit hmwfe pqrtw athtw myuwm mwfup lfyem pheae yfhtl emf

## Material

### Texts

- Hoffstein, J., Pipher, J., Silverman, J. *An Introduction to Mathematical Cryptography*. 2nd edition. Springer (2014). ISBN 978-1493917105. Available electronically through library subscriptions (\$0.00). Copy placed on moodle.
- Singh, S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor (1999). ISBN 978-1857028799. Available used from the Bryn Mawr Bookstore (\$9.75).

### Online

- You will need an account at [datacamp.com](http://datacamp.com) for tutorials and practice in python. Use of this site is free (\$0.00). An invite will be sent to your college email address.
- You will need an account at [cocalc.com](http://cocalc.com) for holding your code and making computations. This site will cost a small fee (\$14.00). An invite will be sent to your college email address.

The only thing we will post to moodle is a copy of this syllabus and the textbook.

## Course components

This course will alternate between student-led presentations of the text material on most Thursdays and student-led discussion and exercise sessions on Tuesdays. Your grade will be cut into five components, according to the percentages:

25%	In-class presentations
25%	Discussion and exercises
10%	Python tutorials
30%	Term project and presentation
10%	Daily course contribution

The default grade lines will be *at least as generous* as: >90% earns a 4.0, >85% earns a 3.7, >80% earns a 3.3, >75% earns at 3.0, and so on.

## Academic Integrity

The Bryn Mawr College Honor Code is in effect for all students enrolled in this course. You may work with other students on homework and lecture preparation. You may seek as much help as you want Prof. Bergdall or any of your peers. But, it is never okay to copy work from another student or resource without carefully working through the material yourself. Submitting such work is a violation of the honor code.

## College accessibility policy

Bryn Mawr College is committed to providing equal access to students with a documented disability. Students needing academic accommodations for a disability must first register with Access Services. Students can call 610-526-7516 to make an appointment with the Access Services Director, Deb Alder, or email her the address [dalder@brynmawr.edu](mailto:dalder@brynmawr.edu) to begin this confidential process. Once registered, students should schedule an appointment with the professor as early in the semester as possible to share the verification form and make appropriate arrangements. Please note that accommodations are not retroactive and require advance notice to implement. More information can be obtained at the Access Services website whose URL is <http://www.brynmawr.edu/access-services/>

Any student who has a disability-related need to tape record this class first must speak with the Access Services Director and to me, the instructor. Class members need to be aware that this class may be recorded.

## Course components

### In-class presentations (25%)

Each student is responsible for participating in multiple presentations. The exact number, and the schedule, will be determined once the class roster settles. The presentations will range between 10 and 25 minutes. Some presentations will involve working in a group; others you'll be alone. All presentations will occur on Thursdays. Presentations will start February 6th.

Each presentation will cover a portion of the text by Hoffstein, et. al. with specific instructions on pages and total coverage. The presenter will conference with me before giving the presentation, so they have a chance to ask questions. Presentation conferences will take place on Mondays and they will last 30 minutes.

There is not enough time to go over every detail from the text during presentations, nor is it a practical way to learn something for the first time.

- Presenters: you should read the material, work through the mathematics, and summarize the main points and examples.
- Non-presenters: you should skim/read the material before class and more fully read it afterward.

A portion of the first day will be spent discussing what makes a “good” presentation. We will use our discussion to create a rubric for providing feedback on each presentation. The rubric will be distributed before the first presentations.

Here are some tips, ordered chronologically, for preparing your presentation.

1. On your own, read through the section that contains the material you will be presenting on, even if your presentation focuses on just a portion of the section. It is important to make sure you understand the complete context.
2. If you are working with a partner, meet early to discuss the reading. Compare notes and discuss perspectives.
3. Fill out, together if you have a partner, the “presentation preparation” form in order to prepare your Monday conference.
4. Conference with me. We will discuss your outlook and go through any technical questions you have. We will also dedicate a few minutes to determining questions and exercises that would reinforce your presentation. If you would like, you are welcome to briefly try a small portion of your presentation in front of me.
5. Prepare your presentation carefully. Then, practice! practice! practice! If your practice does not “sound right,” that is normal. Record carefully what you are finding difficult and then seek out advice from either someone in the class or me!
6. Come to class, present, and shine!

### Discussion and exercises (25%)

A major part of learning is discussing and working through ideas with other people. Over half of our class meetings will be devoted to this. Some meetings will center on discussing Singh's text and others will be focused on solving exercises. Every Tuesday, and some early Thursdays, will be dedicated to discussion and exercises.

The discussions of Singh's text will take place on January 28th, February 11th, and February 25th. Ahead of those meetings you will write a brief reflection to help us frame our discussion. Reflections are due by 7:00a on the day of the discussion. (You will turn them in electronically through cocalc.) If you turn in your reflection on time and with effort you will earn 3/3 points. If it is lacking effort, you will earn 1 or 2 points. If you turn it in late, you may earn at most 1 or 2 points, regardless of effort.

Exercise sets will be determined as a class after Thursday presentations, based on advice and recommendations from myself and the presenters. You will turn in your work electronically, through the cocalc website. Exercise solutions will be written in  $\text{\LaTeX}$ . We will provide templates. If you do not know how to typeset in  $\text{\LaTeX}$ , this is a great chance to learn!

Your score on the exercises for each day will be determined by effort and participation. Namely, every exercise day will be given a score of 0-3 points: 1 point for turning something in, a 2nd point for clear effort, and a 3rd point for turning in a significant majority of the work (each week). There is no “due date” for the exercises, but we will collect them Thursday afternoons at 5:00p. If you modify your solutions after that, it is up to you to tell us.

### Python tutorials (10%)

Many of the exercises we do will involve using a computer, either as a computational tool or by programming it. The language we will be using is python. In order to learn python you will work through tutorials on the free website [datacamp.com](https://datacamp.com). We will further supplement these tutorials with in-class demonstrations, so that you have the chance to fully learn the powerful skill of computer programming. If you already know python, please speak to me to see if there is a more useful alternative for you to participate in this portion of the course.

Python does not contain all the libraries that we will want to use in order to understand cryptography. More specialized libraries are available, and we will be using a single system to access them all. This system is known as sage, which is an acronym for “System for Algebra and Geometry Experimentation.” While sage is technically free, we are going to try to streamline our experience by paying for upgraded access (\$14.00 each) through a commercial website, [cocalc.com](https://cocalc.com), related to sage. This will save us from installing (ridiculously large) files on our machines and provide us a way to share files on the cocalc platform.

## Term project and presentation (30%)

The portion of the text we will cover as a class is quite limited. We will only cover Chapters 1 and 4 completely. We will also go through portions of Chapters 2, 3, 5, and 6. This leaves out a significant number of interesting ideas. You will take one of these ideas and independently research it for a term project.

The major component of your project will be a paper. You will type your paper in  $\LaTeX$ ; we will provide a template. It should be 10-15 pages typed, 1.5-space, in 12 point font with 1 inch margins. If you do not know how to use the  $\LaTeX$  system yet, that is okay. You will learn how to use it through your exercise solutions. The paper will be due at 5:00pm on April 30th<sup>1</sup>.

In addition to writing your paper, you will give a brief presentation to the class. The length of the presentation will depend on the number of students enrolled. The presentations will take place during the final week of the semester.

The grading for the term project will be as follows:

- Your presentation will be graded according to the rubric we decide for the other presentations. It will be worth 5 points.
- We will begin deciding term projects before spring break. You need to decide your project, and write a short proposal (1-2 pages) by March 19th at 8:30am<sup>2</sup>. Your proposal should include
  - A discussion (a few paragraphs) of your topic and your interest, including specific questions you will examine.
  - A list of at least 3 sources you will draw from. These could be our textbook, references included there, other technical texts, news articles, reputable internet sites, or other *good* sources.I will give you feedback. It is worth 5 points: 1 point for turning it in, 2 for effort and 2 more for turning it in on time.
- Your final paper will be worth 10 points. The first 5 points will be determined as in the previous section. The second 5 points will be based on the strength of your argument, research, and reasoning.

In order to help you frame your research, I expect you to answer most, if not all, of these following questions:

- What is your topic broadly about and why is it important?
- What is the history of your topic?
- What is the theory behind (or underlying) your topic?
- How is your topic related to cryptography?
- What is a computation related to your topic?
- What are some open questions about your topic?

A major component of this course is using python to make computations. Your project must contain a significant computer-based computation related to your project. That could mean custom code implementation that you wrote, or you could go through a practical usage example. If you are not sure what you want to do, please come ask and we will brainstorm together.

## Daily course contribution (10%)

You will earn these marks *regardless* of vocal participation by engaging the material and actively participating during work time. You will be an audience member during class presentations that you need to follow to learn the mathematics. So, *you are expected to be at class, on time, on a daily basis*. Regularly missing class or arriving late is disruptive, will hinder your learning, and it is rude to your classmates who will be presenting. We are, however, realistic about the frequency at which students miss class for arbitrary reasons. So, while we will track attendance it will be taken into account as follows:

- You begin the semester with 13 points.
- We will deduct 1 point for missing a day. We will deduct  $\frac{1}{2}$  point for missing the start of presentations and discussion, or for missing more than 10 minutes on exercise days. If we are late, everyone will earn a  $\frac{3}{4}$  point.
- Your final score will be out of 10 points, so 3 “free” points account for typical absences.

Students in the Tri-Co have met our expectations when they are clear. This policy clarifies our expectations; it is not meant to punish. You may encounter a situation, or situations, during the semester that stop you from regularly attending lecture on time. If that is the case, it is your responsibility to interface with us so that we have the chance to adapt our expectations to your changing situation. You are welcome to utilize your dean to communicate with us, if appropriate.

## Late Work and Make-up Policy

- Your presentation dates will be known well ahead of time. Because of scheduling logistics, making up a presentation will be a significant task. Your term paper is due the same time as all written work. Should you encounter debilitating obstructions such as overwhelming concerns of wellness or emergency travel, we ask that you interface with us as soon as possible so that we can find an equitable solution. Include your dean if it is appropriate.
- While exercises are due on Thursday afternoons, there is no penalty for turning them in late. That being said, please do not wait forever to complete the exercises. Working hard in discussion/exercise session should get you most of the way there and the exercises are important to propel your learning.
- The project proposal and pre-discussion reflections are more flexible. You’re invited to turn them in late, but you may lose some points based on the discussion above. It may also delay your feedback (for the project proposal).

<sup>1</sup>Or, possibly later during the finals period.

<sup>2</sup>Updated on 2/19/20

## Resources for help

Before going into details, we make an important observation:

Everyone may need help. The amount of help you need will depend wildly on what you are trying to do, your background, and your environment. The amount of help you receive is determined by the amount of help you seek.

The textbook readings, exercises, and, of course, your presentations are all things you are tasked with understanding. Below we list myriad resources for help with any or all of these. Getting help, from any resource, will not result in a “mark against you.” We wish you the best time finding an efficient way to get help!

### Office hours

During office hours you can ask me any question you like, even if it is not about this course. Because of the presentation conference meetings, I am starting the semester with two office hours. We can add more office hours if there is demand.

If you need help with python programming, I am there to help. If you need help with reading Hoffstein, et. al. I am there to help. If you need help figuring out how to get to a restaurant in Philadelphia using SEPTA, I am there to help with that too. If you are hungry, there are typically chocolates in my office. If not, let me know and I'll go buy some.

### In the hallway and around

You will often see me in the hallway, likely getting coffee. You should 100% feel free to ask me a question if you have one. If I am pre-occupied with another task, I will politely let you know and we can set up a different time to talk. Before and after the colloquium lectures are also a good time to chat for a few minutes. I also, like most people, eat lunch near the middle of the day. If you'd like to ask me some questions over lunch, I am more than happy to do that.

### Email

Your questions are important, so if you cannot find the time to ask me something before class, during class, after class, or in office hours, then you should email me. Your questions may concern anything at all, but I especially invite you to ask any questions related to the course atmosphere that you are not comfortable asking about in person. I try very hard to answer my messages, but there is a caveat with email: once the semester gets moving it could be up to 24 hours before I get around to responding (and longer on the weekends). If you sent me a message and I haven't responded, please send it again or remind me in person. Perhaps I had to follow-up somewhere else on campus and I am waiting for more information.

### Appointments

I am more than happy to arrange for an appointment if you feel that it is more suitable than the above options. You can email me, but I must ask for patience in finding a time to meet. In your initial email you should explain (a) what you want to talk about and (b) what times *you* are available. I will then do my best to find a time that works for both of us. The more times you can offer, the more likely we can arrange to meet quickly.

## Notes on studying mathematics (now and later)

Advanced mathematics is highly-tuned toward students studying and mastering material on their own time. For some of you, this will be a novel experience. Our hope is that your experience in this course will provide a model you can use later in your careers, when you may not have your tasks so structured. Here is a rough plan for approaching new material, like our readings and your presentations.

- Quickly browse or skim the material. Try to estimate how long it will take you to read and whether or not the material can be broken down into smaller sections that can be individually read.
- Carefully read highlighted/bolded/emphasized text and determine the main questions being discussed. Write these questions down. Ask another student if they perceive the same thing.
- Work through the examples in the text! (This,  $\times 100$ ). There is no replacement for working through the numbers and theory for yourself. If you come to class having worked through a single example from each assigned reading then you will be in prime position to get the most out of the presentations.

Now, after giving you some of those tips, we find it necessary to affirm something:

Reading mathematics will take *longer* than other reading.

We have included Singh's text as an attempt to help you understand the contrast between typical writing and mathematical writing. In the textbook, it will be normal re-read the same paragraph quite a few times before feeling like you maybe might just a little understand it. A page of text, in an advanced undergraduate text like our own, may take you more than an hour to read if the material is dense. Do not expect to read the text straight through and “get it.” You are welcome to come to office hours and discuss your reading, and how to do it efficiently. My ears are sympathetic.

## Summary of due dates

There are few long term due dates in this course. You have a term project, the reading from Singh, and the tutorials in python. We summarize the basic due dates for you below.

---

### Term project assignment dates

---

Assignment	Date due
Term project proposal	03/19 (8:30a) <sup>3</sup>
Project presentation	04/21-30 (during class) <sup>4</sup>
Project paper	04/30 (5:00p) <sup>5</sup>

---

---

### Reflections on Singh's text "The Code Book"

---

Assignment	Date due
Chapter 1-2	1/28 (7:00a)
Chapter 3-5	2/11 (7:00a)
Chapter 6-7	2/25 (7:00a)

---

---

### Python tutorials

---

Assignment	Date due
Python basics	01/23 (8:25a)
Python lists	01/23 (8:25a)
Functions & packages	01/28 (8:25a)
NumPy	01/30 (8:25a)
Dictionaries & Pandas	02/04 (8:25a)
Logic, control flow, and filtering	02/11 (8:25a)
Loops	02/18 (8:25a)
Writing your own functions	02/25 (8:25a)

---

---

<sup>3</sup>Changed 2/19/20

<sup>4</sup>Change 2/19/20

<sup>5</sup>Subject to change

Please complete the quiz below, and then fill out the check-in information on the back side of this page. As you fill out the quiz/check-in, I will come around and greet your groups.

## Syllabus quiz

### Multiple choice

Choose the best answer to the following questions.

How long will the presentations be?

- less than half an hour       45 minutes       entire class periods

How much of your grade will be determined by in-semester exams and the final exam?

- 0%       20%       30%       50%       100%

If I miss class twice, I am 3 minutes late to the start of Jenny's presentation, and then I am also late by 5 minutes while we are solving exercises, then my daily course contribution score will be:

- 7.5/10       7/10       10/10       10/13       7/13

### True/false

Decide whether each of the following statements is true or false. (The "I" refers to you, the student.)

"I am responsible for reading before my presentations, but not other students' presentations."

- True       False

"It is okay if I do not know how to program a computer at the start this class."

- True       False

"There are strict deadlines for both exercises and the term project."

- True       False

"The term project has components due prior to the final week."

- True       False

"I will need to type my exercise solutions and the final project."

- True       False

## First day check-in

### Some personal details

Preferred name:

Preferred pronouns (if you would like to share — you needn't):

Outside of mathematics, my favorite college courses have been in...

My BiCo username is:

@brynmawr.edu

@haverford.edu

### Logistics

Are you registered for this course, planning to register, or shopping?

Registered

Planning to register

Shopping

Could you attend the senior conference taught by Professor Donnay (MW 1:10-2:30p)?

100% Yes

100% No

It's complicated

I have a significant reason to take this section

Briefly describe your experience with computers, programming, and python specifically:

### Goals

Briefly describe one goal you have for *this* course:

Briefly describe one goal you have for this *semester* (regardless of MATH B399):

### Class formation

In this course, we will be listening to presentations and working in groups *frequently*. Briefly describe one norm you would like the class to observe. (These will be compiled and included in an update to this syllabus. Your answers will be anonymous.)

In the remaining space, if you are comfortable, please indicate anything else you think it is important for us as your professor to know. (If you are not comfortable, or would like more space, please email me or come see me in office hours.)



## Classroom norms

The following is a list of norms anonymously gathered from yours peers:

- Before the presentation, give a facial expression or emoji to express your thoughts about the chapter.
- Eye contact is important. Try not to read off the slide or notes.
- Listen when people are talking. Do not be distracting.
- Try to share anonymized feedback with reach group.
- Be engaged in discussion and listen to presenters. Ask questions after presentations to better understand the presentation.
- Clap after each presentation, and try to have discussions with different people every time so we will know one another better at the end of the semester.
- People should take notes and respect others.
- Be prepared material-wise and be prepared to listen to others.
- Show friendliness and respect others.
- Leave enough time for Q & A sessions and the audience should show respect.
- Go over names within a group each time. (I'm very slow at learning names.)
- If a student should do a presentation, they should not be late for that class.
- After the presentation we could have a "what we learned from the presentation, what questions we have, and suggestions for improvement" time (hopefully written?)
- Be respectful listeners.
- Respect others' work.
- Leave Q & A time for each presentation.

## Rubric for a good presentation

The grading rubric we compiled will be handed out separately and attached on the final pages of the syllabus.

Presenter name(s):

Your name:

Presenter topic:

Instructions: Place one mark in each row. See reverse for longer descriptions of criteria.

<b>Criterion</b>	<b>Way above expectations (Excellent) (4 points)</b>	<b>Above expectations (Good) (3 points)</b>	<b>Meets expectations (Satisfactory) (2 points)</b>	<b>Below expectations (Unsatisfactory) (1 point)</b>
<i>Knowledge</i>				
<i>Clarity</i>				
<i>Questions</i>				
<i>Organization</i>				
<i>Pace</i>				
<i>Preparation</i>				
<i>Audience engagement</i>				
<i>Visual engagement</i>				
<i>Composure</i>				
<i>Style</i>				

What is one question you have about the presentation?

---

What is at least one aspect of the presentation you'd like to affirm was done well?

---

What is at least one suggestion you have for the presenters to improve their presentation next time?

---

There are a number of factors that go into a good presentation. Successful presentations do not follow any one formula. Based on the post-it notes we filled out on the first day of class and our experience, we've described features of good presentations we can look for as an audience.

The bare minimum you need to do when giving a presentation is know what you are talking about. You should know the material you are presenting *and* you should show you understand how to clearly present it. You should also be able to anticipate and react to questions that could arise. You *may* not know the answer, but you should at least understand the question.

Knowledge: Did the presenters show that they had studied the material and knew it?

Clarity: Are words spoken clearly, ideas understandable, and explanations concise?

Question preparation: Did the presenters handle questions that arose?

Once you have knowledge, you need to think about how to construct your presentation. You need to think about what to include, on what medium, and in what order. Do not take up too little or too much time. Show up ready to start. These skills are honed through rehearsal, ideally *with someone else*.

Organization: Was the presentation organized and ordered in a logical manner?

Pace: Did the presentation fit into the time planned?

Preparation: Was the presentation ready to go at its start?

Finally, memorable presentations involve the audience being a part of the presentation and, ideally, having the audience wanting the presentation to go well. The ability to do this is not a skill everyone naturally has, but it is a skill that you can practice and improve on. You should make sure your physical presence and the material you present engages them. You should also take care to present yourself as composed, and you should make sure your presentation uniquely expresses yourself through stylistic choices.

Audience engagement: Eye contact? A loud enough voice? Face the audience?

Visual engagement: Did the presentation visually keep the audience's attention?

Composure: Were the presenters poised, composed, or confident?

Style: Did the presenters let their personalities and identities shine?

## Addendum: Response to COVID-19 and remote instruction

Before we begin, we must provide two caveats.

- We have not, as of writing this document, determined how many students in our class are facing significant hardship related to access to the internet and computing devices. A brief survey will be sent to students along with this page in order to determine computing, temporal, and spatial constraints. We have 16 students in this lecture, which gives us an advantage that accommodations can be made on a case-by-case basis.
- The college has only announced no person-to-person instruction through April 3. The plan below assumes, as is reasonable, that person-to-person instruction will be suspended for the rest of the semester.

### Overview

The following describes alterations to the course and its policies following the decision to go remote-only on March 16, 2020.

There are 5 learning goals in this course. From the first page, they are:

- Trace the history of mathematical ideas alongside emerging technologies.
- Work in a group to understand advanced mathematics.
- Prepare, deliver, and participate in thoughtfully developed presentations.
- Use a computer computationally through the programming language python.
- Propose and develop an independent research project in cryptography.

Of these 5, each student in the course has already accomplished significant progress on the first 4. At the time of the online-only switch, the class was about to finish its in-class presentations and proceed to focus most of our energy on term projects.

We have not taken the decision to lessen the assignments lightly, but in light of the switch to online-only instruction we have chosen to cancel the in-class pair presentations on 3/24 and 4/02. The remainder of the semester will be spent with students focusing completely on final research projects.

Our chief aim in taking this route is, first, to acknowledge the significant amount of bandwidth the current health situation is going to require of each of us and, second, to allow for higher emphasis on interaction as students focus on a singular purpose. By maintaining just a single activity, the students and professor should find it easier to deal with the complications of remote instruction.

### Details on final project

As before, students working through their final project are still expected to:

1. Produce a 1-2 page research proposal for their project. (The due date is now *to be determined*.)
2. Write a 10-15 page research paper.
3. Produce at 10 minute presentation of their research for the class to watch, either live or recorded.

The specifications of the research proposal and the corresponding paper are as before. The presentation, on the other hand, is flexible and we encourage students to be creative in their choices. Presentations could be given in a meeting format, with recording available for students who cannot make specific times, or students can make multi-media presentations and upload them (location to be determined).

### Remaining class meetings

In the coming months, we will need to adjust to a life with less social interaction and less engagement than the BiCo community provides. Being in your final semester, this is especially devastating. For your mental and emotional well-being, we feel it is important for you to continue to engage with your peers and myself during this difficult time. To find a silver lining, let me point out that work is increasingly done online and remotely, even in times of good public health. So, while working remotely may be happening for you earlier than you thought, please consider considering it an opportunity to hone skills that are going to serve you into the future.

One challenge we face is creating a support system with 16 students. There are a number of specifics to implement, but it is difficult to be concrete before we get more data from the students on their temporal and spatial abilities. Roughly, I hope:

- The entire class will meet 0-1 times per week for at most 45 minutes via video/tele-conferencing. This meeting will be a “stand-up” where each of us explains what we have done the week prior and what we plan to do in the coming week.
- Students will be assigned, weekly, to a small group (3-4 students). The group will meet with myself via video/tele conferencing for up to one hour to discuss a specific topic, such as “How is the computing portion of your project coming along?” Your group will be a support group to keep you motivated during the week. Hopefully, groups will rotate.
- On cocalc.com we will provide a “Shared project” where we can host a chat and work on code together, if we need to.
- I will have long periods (3+ hours) of drop-in office hours on multiple days, where I will be available via video/tele-conference. These hours will allow you a chance to pop in and ask questions related to your research project.

## Addendum: Remote instruction, II

We continue, here, specifying how MATH B399-02 will move to remote only instruction. We remind the students that we are focusing completely on final research projects.

In a typical week you are going to have two main interactions with your peers. First, we will have a stand-up meeting early in the week to report our hopes and dreams from last week and the next. Second, we will have support meetings on Thursdays to help you progress with your projects. In total, we are limiting your must-be-scheduled time in this class to less than one hour per week. This is a privilege our course format allows us, and we think it is particularly prudent in light of the disruptions you all have faced. Since you will still be putting in a lot of effort to finish your project, we will also be available for office hours in chat and on video. (Times TBD.)

### Asynchronous stand-ups (due late Monday nights)

A “stand-up meeting” is a meeting intended to summarize the team’s progress and process. The *stand-up* terminology is used because such meetings are typically done standing, literally, so that they do not last long. For the rest of the semester, we are going to have a weekly stand-up where each member of the class will summarize what’s going on with their project.

Due to the varying time zones we’re living in, these meetings will be *asynchronous*, meaning we will each be “standing up” at different times of the day. You will each record a video, roughly 1 minute long, in which you reach out to your fellow classmates, say hello and answer the following questions:

- If you want, how are things going in the world for you?
- For this class, what have you done in the past week?
- For this class, what are you going to do next?
- For your other classes, is there anything big coming up you’d like to share?

Be specific! Think less like “I did some reading for my project” and more like “My project is on hash functions, and last week I read the textbook by J. Smith. It was really interesting to learn...”

Your videos will be uploaded to moodle (see the instructions below) and then I will process them and re-upload them in an easy to watch format. My goal is to share the videos by noon on each Tuesday, so you need to record your stand-up video by Monday night at 11:59pm Philadelphia time (UTC-4:00).

Please be creative and have fun! We are each in a completely different place than we thought we’d be six weeks ago — it will bring smiles to all of our faces to see how you are getting on. And, finally, please also respect your peers. You should not be sharing videos and images of your classmates, or of myself, without their, or my, express consent.

### Weekly support meetings (Thursdays)

As you work on your final projects, you are also going to need the support of your peers and we would like to give you the chance to share your progress as it happens! On Thursdays, we will hold real-time meetings with small-ish groups of students to go over their projects. You are asked to attend one meeting per week.

These meetings will take place using Zoom. A link to join will be provided each week. You should be able to access this through a web browser or by downloading the Zoom app on your phone or tablet. We chose Zoom largely for its compatibility with joining a meeting without necessarily having to download an app.

Support meetings will start at 8:00am and last until the middle of the afternoon. We hope that there will be 4 meetings, limited to 5 students each. We want to be flexible with your schedule, so we’re even willing to hold evening meetings if that works best. For the first week, things will obviously be more chaotic and our meeting times will be:

- 8:00am - 8:45am
- 9:00am - 9:45am
- 12:00pm - 12:45pm
- 1:00pm - 1:45pm.

For the first week, we will not cap the number of students per meeting. After the first week, we will fix 4 specific hours based on your feedback.

With six weeks left in the semester, we will have six support meetings. Here they are summarized week-by-week.

1. Mar 23-27: How is it going? Any last questions before you submit your proposal?
2. Mar 30-Apr 3: How have you adjusted to the feedback on your proposal? What have been your first project steps?
3. Apr 6-10: What are some of the mathematical hurdles you’ve faced in your project? Anything you need further help understanding?
4. Apr 13-17: Have you started thinking about how to include a computational aspect to your project? Is there any python help you might need? Any draft materials you would like to share?
5. Apr 20-24: How is putting together your presentation going? What kind of process or you following?
6. Apr 27-May 1: What are your final thoughts about the paper? Any last minute questions for your peers?

## Remainder of assignments

Let us summarize the remainder of the assigned work for this course.

### Research project proposal (due March 27th)

The research project proposal was originally due March 19th, and that date has been moved to March 27th. The proposal will be submitted via cocalc.com, as other assignments have been. A sample proposal was provided.

### Final multimedia presentation (due April 30th)

Each student is asked to create a presentation describing their research project. These presentations should be no more than 10 minutes each, and they should follow the same guidelines we developed while training with in-personal presentations: you should lay out the goal of your presentations, the main points of your research, and then cover *some* of the details of what you learned. The environment of the presentation is still to be addressed, but we will make it possible for students to record and upload their presentations or for them to be delivered live to whomever can make it. The presentations will all be due on the date that the final in-class presentations should have taken place: Thursday April 30th at 5:00pm.

### Final research paper (due May 7th)

The specifications for the final research paper are the same as before (see the original Syllabus for this course). The due date, as discussed during the final class meeting before the shutdown, is May 7th at 5:00pm. Remember that one portion of your paper should address a computational aspect, and you should be sure to implement, or work through an example, using python.

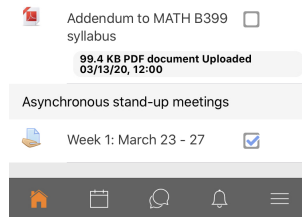
### Soft deadlines for project

At least one student asked me to provide soft deadlines for your research projects. I am writing this in late March, after your project proposals have been turned in already. These are just guidelines. They may start writing sooner than you are used to. Use your experience to adapt this outline to your own style!

- Mar 30 - Apr 3. Early this week you should receive feedback on your proposal. Based on that, you should be able to outline your paper, section by section, and begin to do deeper research into each section.
  - Re-assess plan based on project feedback.
  - Outline paper into sections.
  - Work through the mathematics, taking notes, on at least one section of your outline. Starting writing down some of those details. Try to write 1-2 pages by the end of the week.
- Apr 6 - Apr 10. Math week! With an outline of your paper complete, and some of the mathematics worked out, now is the time to sink into the project. By the end of this week you should know the parts of your paper you'll need help with, and you should plan where to get that help! You should also, if you haven't, begin writing your paper. Choose whichever section you feel strongest about right now. Looking ahead, begin planning out how to include a computational aspect.
  - Study enough of the mathematics to understand where you'll need to confer with a friend or the professor.
  - Begin writing, leaving gaps in the details if necessary. Having 3-4 pages *roughly* done is a good goal.
  - Dedicate time to think about how you are going to involve your python skills in the project.
- Apr 13 - Apr 17. Based on your notes, the math should be nearly all worked out at the end of this week. You should have significant progress on writing. You should dedicate time now to carrying out the computational aspect of your project.
  - Continue writing. Your paper could be 7+ pages at this point, with all the details you've learned in there! If you haven't included any historical portions, that would be a nice change of pace this week.
  - Begin to implement python into your project. By the end of the week, identify any help you think you'll need.
- Apr 20 - Apr 24. Almost there! Your paper still isn't due for 2+ weeks. Enough of it should be written that you are sure you will finish. Now it is time to begin building up your presentation. You are going to want to think about the *main* points of your project and how to build slides around those main points.
  - Finalize your plan to finish the paper. What do you still need to write, and when are you going to write it?
  - Finalize your plan to finish the computational aspect. What problems are you facing? How will you solve them?
  - Begin outlining your presentation. They should end up 5-8 slides long. What is going to go on each slide?
- Apr 27 - May 1. Last week of class! You've put yourself in great position to finish the paper at the start of finals week. The big thing to create this week is your presentation. You should, at the start of the week, have a plan for your slides and you should know how much time it is going to take you to finish them.
  - Create and plan your presentation. Your presentation will be due on April 30th at 5:00pm.
  - Make an absolute final plan for finishing the paper and computational aspects. Having 10+ pages of the paper written is excellent!
- May 4 - May 8. Finals week! With everything you've done so far, you don't have a lot of writing left to do! This week should be focused on putting any final touches on your paper you'd like, and making sure the computational aspect of your project is solid. Remember: done is good, and graduation is around the corner!
  - Finish your paper and your computational component. Turn it in by May 7th.

## Recording your video for asynchronous stand-up

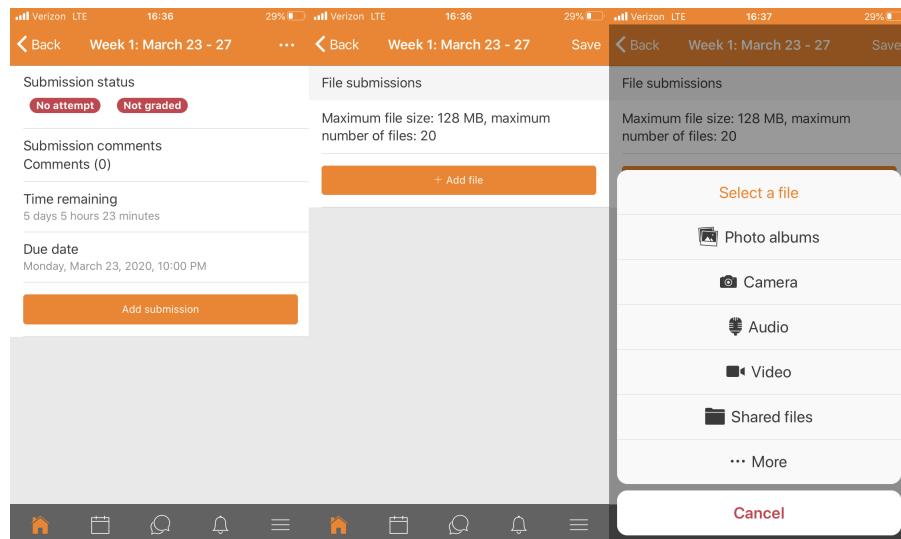
Each week you will be asked to upload a single movie file to moodle. The assignments will be labeled Week 1, Week 2, etc. as you see in the next screenshot, taken from the interface for moodle on the mobile app (iPhone).



The largest file size our system allows is 128 MB. If you record the video via the moodle app, that is plenty large. If you record it on your computer, you will need to make sure to export it in low enough quality to get under that threshold.

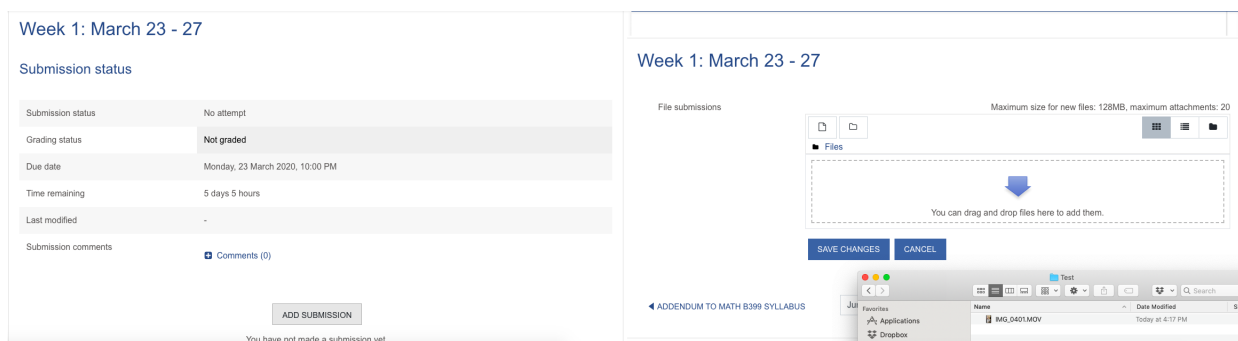
### Uploading via the moodle app

The easiest way to upload a video to moodle is using the smartphone app. Because videos uploaded this way are automatically re-sized to minimize their files size, this is the preferred way of uploading the video. After clicking on the assignment link above, you can hit "Add submission" and then "+ Add file". It will ask you to select a file. Select "Video" and you can record. This is shown in the screenshot(s). (You *should* be able to upload a pre-recorded video, but I personally got errors.)




### Uploading via a web browser

You can also upload from your computer. After clicking on the assignment, hit "Add submission" and then drag/drop the file.



## Signing up for a weekly support meeting

To sign up for a weekly support meeting, navigate to moodle page and look for the Scheduler assignment indicated with a tiny calendar . Once you click that link, it should be straightforward to book a meeting slot. The link to the Zoom meeting will also be provided there. Unfortunately Bryn Mawr's moodle site doesn't support the app for the scheduler. I am going to write to the support at LITS to see what they can do about that.