MATH 3107: CRYPTOGRAPHY AND CRYPTANALYSIS
SPRING 2024 COURSE INFORMATION

Instructor	Professor Goodson (she/her)
Email	`heidi.goodson@brooklyn.cuny.edu` (I don't often check my email between the hours of 8pm – 8am, so please don't expect a response until the next day.)
Class Times	Monday & Wednesday 11 AM - 12:40 PM in Ingersoll 3146.
Office Hours	Mondays 1 - 2 PM and Wednesdays 9:30 - 10:45 AM in Ingersoll 2313. Please email me to set up a time to meet outside of office hours.
Textbook	"An Introduction to Mathematical Cryptography," by Hoffstein, Pipher, and Silverman (any edition). There is a free copy of the book online through the Brooklyn College library. There may also be some extra readings posted on Blackboard.

Introduction

Welcome to Math 3107! I am very excited to meet you all and to teach in-person this semester! Here are some guiding principles to help us have a great semester together.

- **Be safe:** Please do not come to class if you are not feeling well. Course materials will be available on Blackboard so that you can keep up with the course if/when you need to miss class. I will also not come to class if I am not feeling well and I will find ways to continue teaching you. There is currently no mask mandate on campus, but you are welcome to wear one in class.
- **Arrive on time:** Everyone will be required to show a BC ID when entering campus. Please plan accordingly!
- **Communicate:** Please let me know if you have any concerns about the course, the class, or anything else. I will communicate class changes, campus updates, and anything else that is relevant to our course through announcements on Blackboard.
- **Be persistent:** Mathematics can be both challenging and beautiful. We all get stuck on problems sometimes, but if we are persistent then we will be able to push past our confusion and learn!

Course Content and Goals

We will cover mathematical problems underlying public-key ciphers and digital signatures, as well as algorithms to solve them. Topics include:

- An Introduction to Cryptography (Chapter 1)
- The discrete logarithm problem and Diffie-Hellman key exchange (Chapter 2)
- Integer factorization and the RSA cryptosystem (Chapter 3)
- Digital signatures (Chapter 4)
- Elliptic curves and related cryptosystems (Chapter 6)
- Lattices and cryptography (Chapter 7)

Throughout the course, we will discuss both *cryptography* (encryption and signing algorithms) and *cryptanalysis* (algorithms to break cryptosystems). We will also learn about some historical uses of cryptography.

The mathematical topics we will learn and use largely come from Linear Algebra (matrix operations, vector spaces), Number Theory (modular arithmetic, elliptic curves), and Abstract Algebra (group theory). While you should have a background in Linear Algebra (Math 2101), you are not expected to have a background in the other subject areas. You can think of this course as an opportunity to learn about these mathematical topics in the context of cryptography.

In addition to gaining an understanding and appreciation of an interesting and important area of mathematics, you will also learn to develop and communicate original mathematical ideas, both verbally and in writing. The subject of mathematical writing will be discussed in class, with many suggestions and guidelines for you to use in your work. You will also learn some basic computer programming. Prior programming experience (in any language) is not necessary.

We will strive to approach our study of mathematics with a *growth mindset*: experiences, struggling, making mistakes and learning from them – all of these things cause you to learn and grow your intelligence. Research shows that students who are taught with a growth mindset approach achieve at much higher levels, and that in fact all students can succeed in mathematics. I believe that you can succeed as long as you remain open to being curious and to persevering through mistakes and struggles!

The prerequisite for this course is Linear Algebra (Math 2101). If you are undecided about whether to take the course, please talk to me about it!

Technology for This Course

Blackboard. Course organization (assignments, class notes, pdfs of handouts, etc.) will be on Blackboard. Emails with course announcements will often be sent through Blackboard so please be sure they are not filtered from your inbox.

Gradescope. A website where you upload your assignments to be graded. You will be able to log in and see your grades and my comments on your assessments. Make an account for our course at `www.gradescope.com` using the entry code on Blackboard. You do not need to enter your student ID number.

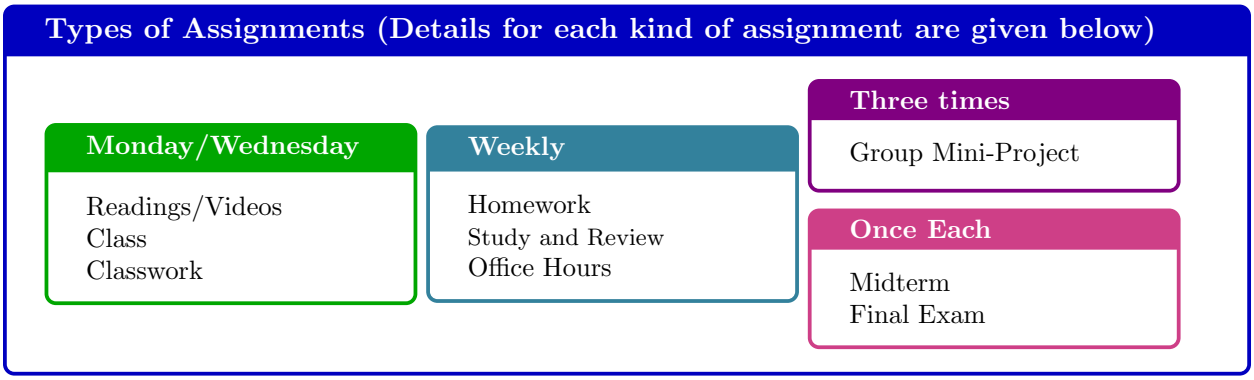
Programming. We will need to write computer programs in order to work on large examples in this course. I will provide resources for getting started in Sage, which is a free open-source mathematics software system, but you are free to use whatever computer software/language you like. Prior programming experience (in any language) is not necessary. We will have several class sessions in a computer lab so that we can learn and practice together (dates will be listed in the course schedule).

Calculators. You will be allowed to use calculators on assignments and exams in this course.

Taking notes in class. You should plan to take notes in every class session. You can do this in a low tech way (pen/pencil and paper) or in high tech way (using a tablet). Some students find it helpful to take photos of the board as a supplement to taking notes. This is allowed, but please do not post the photos publicly online. *Please do not record any video in class without prior permission from the instructor.*

Coursework

> You have to spend some energy and effort to see the beauty of math.
>
> – Maryam Mirzakhani, 2014 Fields Medalist



Reading assignments. Each week, there will be reading assignments and/or videos posted on Blackboard. You are expected to do the reading and/or watching so that you will be prepared for class. During class, I will rely on the fact that you have read the sections/watched the videos, but I will not assume that you have completely absorbed them.

Suggestions for reading math (from Professor Ben Braun at University of Kentucky):

(1) **Understand the story.** Even if you don't understand all the words, you can understand a lot by skimming the expository paragraphs. Is this portion of the text about a specific example? a general phenomenon? Does the author say it is related to something you know about? Does the section contain a lot of theorems and proofs, or mainly a collection of examples? What words are defined in the section?
(2) **Understand the broad ideas.** Read the definitions and theorems. Create small examples and non-examples to illustrate the concepts. Skip all proofs. Summarize the text in your own words.
(3) **Understand the details.** Read the examples and proofs. Create larger examples and non-examples. Create generalizations of the definitions and theorems. Try to prove your generalizations.
(4) **Repeat this cycle.** Read the section again. Create a short summary of the text in your own words. Create a short outline of the text. Explain the material in the section to your study group.

Classwork. In each class session, I will provide you with exercises and problems related to the topics that we are covering. You should aim to finish the exercises and problems (either during class or after class) so that you can practice and learn the topics we are covering.

Classwork is an opportunity to learn math the best way possible – by doing it. In order to encourage you to keep up with the material, I will ask you to submit your work to 2 - 5 problems that I will choose from each week's notes. You will submit your classwork on Gradescope. Classwork will be due on Sundays at 11:59 PM, starting on February 4.

Homework. Homework will be due on Sundays at 11:59 PM, starting on February 11 on Gradescope. All homework assignments will be posted on Blackboard. You will post your solutions on Gradescope. Your homework should be typed or written extremely neatly. The homework consists of problems that enable you to gain a deeper understanding of the class material, to improve your problem-solving skills, and to practice your mathematical writing. The work that you submit should reflect your own understanding of the problem. Homework will be open notes and you may collaborate on the homework, but you should not use the internet to look up answers. Please see the policy on collaboration below.

Homework is graded so that you can practice writing mathematics and receive feedback on your progress. A low score on a homework assignment indicates that in order to stay on track you should get help from me.

I will carefully read and assess some of the problems and will grade others for completion only. Problems will be graded not only on the content of your solutions, but also on the clarity of exposition, with full marks awarded only when the solution is sufficiently clear in terms of both the step-by-step logic and overall organization. Remember: the point of writing your solutions is *communication*. In particular, your solution should be clear enough to communicate all of the important ideas to the grader, and it also should be clear to *you* a few weeks or months later! When writing your homework, use complete sentences and correct grammar.

Computer Labs. We will need to write computer programs in order to work on large examples in this course. I will provide resources for getting started in Sage, which is a free open-source mathematics software system, but you are free to use whatever computer software/language you like. Prior programming experience (in any language) is not necessary. You are encouraged to ask classmates for help, and also to bring questions to office hours. We will have several class sessions in a computer lab so that we can learn and practice together (dates will be listed in the course schedule) and you will submit your work from these computer lab sessions.

Group Mini-Projects. You will work in groups of 2 - 4 on problems that extend our work in the course. You will have at least one week to work on the project and you will submit your work on Gradescope. Your score will be a number from 0 to 10, and everyone in your group will receive the same score. After receiving feedback, your group will have one week to make corrections in order to improve your grade.

Course Engagement. There are many ways to be engaged in this course, including: asking and answering questions in class, working with others both inside and outside of the classroom, attending office hours, and emailing questions. You are expected to come to every class prepared to do mathematics. You should bring paper, pens or pencils, and other equipment you may need. You must be up to date and prepared for class to participate effectively. Attendance and Participation are not a part of your grade, but they are required if you will be successful in the course.

Exams. There will be two exams in this class: one midterm and one final exam. The midterm exam will be during class on **TBD**. The final exam will be during Finals Week on TBD. Please contact me as soon as possible if you have any questions or concerns about this.

No exams missed due to unexcused absences may be made up. Excused absences are granted only in extreme circumstances.

Grade Calculation

Grades are a reflection of your mastery of the material and your ability to communicate through the graded assignments. Grades are not a reflection of your self-worth. Your grade for the course is determined by:

Classwork	10%	**Homework**	20%
Computer Labs	5%	**Group Mini-Project**	15%
Midterm Exam	25%	**Final Exam**	25%

Course grades will be assigned by the following percentage ranges:

90% and above	= A range (A-, A, A+)	80% - 89%	= B range (B-, B, B+)
70% - 79%	= C range (C-, C, C+)	60% - 69%	= D range (D-, D, D+)

Percentages below 60% will not receive a passing grade for the course. Grades of A+, A-, B+, B-, etc will be determined by the instructor based on how close you are to meeting the thresholds for the next letter grade range.

Late Work Policy

There will be set due dates for all assignments to keep you moving through the course material and learning. For most assignments, you will have several days to complete and submit the work. I will accept late submissions of work (not including exams) for 24 hours past the deadline. Late assignments will still get full credit, but try to do stuff in a timely manner. Please do not email me assignments – you can submit them on Gradescope. Please talk to me as soon as possible if you can't keep up with the pace of the course.

Academic Integrity

The faculty and administration of Brooklyn College support an environment free from cheating and plagiarism. Each student is responsible for being aware of what constitutes cheating and plagiarism and for avoiding both.

Submitting the work of another person or persons without proper attribution is considered plagiarism, and will be treated accordingly. Proper attribution requires identifying the source of your work. Failure to do so may result in a charge of plagiarism, and students can be subject to administrative actions, including

- a grade of 0% on the assignment or exam,
- an F grade in the course.

Additional actions may be taken by the College, including admonition, warning, censure, disciplinary probation, restitution, suspension, and expulsion. The complete text of the CUNY Academic Integrity Policy and the Brooklyn College procedure for policy implementation can be found at `brooklyn.cuny.edu/bc/policies`. If a faculty member suspects a violation of academic integrity and, upon investigation, confirms that violation, or if the student admits the violation, the faculty member must report the violation.

If you have any questions about what constitutes plagiarism in this course, please ask me.

Classroom Etiquette

In order to support a flourishing mathematical community, our in-class discussions will focus on dialogue rather than monologue. You will each share your own ideas and ask questions of others. You will listen to each other and carefully consider each other's ideas. In each class discussion, make sure you have heard from everyone in your group! That includes you!

Collaboration

Collaboration on homework is encouraged! However, you need to carefully balance learning with your fellow students and finding your own path through the material. For the written homework, you must follow the collaboration guidelines below.

(1) When solving homework problems, you are not allowed to use outside materials (e.g. from the web) unless I give express permission.
(2) You **must** indicate on your written homework who your collaborators are. (If you collaborate with different people on different problems, say so!)
(3) Work on a problem by yourself until you have your own "idea" about the problem; after that, you may start collaborating. (A valuable idea can be as simple as a sense of why you are stuck!)
(4) Do the actual write-up of your homework without your collaboration notes so as to reflect your own understanding of the problem. If you cannot write the solution without referring to your collaboration notes, then you have not yet understood the solution. In that case, go back to step (3).

So as to ensure productive collaborations, you should not be working in groups larger than four people on any given problem at any given time. Two- or three-person groups are better than four. Large groups of people "working together" are not really working together.

On-campus Resources

Office Hours. Please stop by office hours to ask questions! I have set aside this time specifically to help you learn and be successful in the course. If you are unable to make any of my office hours, please email me to set up an appointment.

Please check this website for updates on services at Brooklyn College, including Personal Counseling, Advising, Financial Aid, Immigrant Student Services, and Internet Access:
`brooklyn.cuny.edu/web/about/offices/studentaffairs/health-wellness/coronavirus/student-resources.php`

Support and Accommodations. Brooklyn College is committed to supporting the learning process for all students. Please contact me as soon as possible if you are having difficulties in the course. There are also many resources on campus available to you as a student, including

Center for Academic Advisement and Student Success
`brooklyn.cuny.edu/web/about/offices/caass.php`

Personal Counseling
`brooklyn.cuny.edu/web/about/offices/studentaffairs/health-wellness/counseling.php`

Student Bereavement Policy
`https://www.brooklyn.edu/policies/bereavement/`

Center for Student Disability Services
`brooklyn.cuny.edu/web/about/offices/studentaffairs/student-support-services/disability.php`

The Center for Student Disability Services (CSDS) will be offering services both in-person and virtually for the fall semester. In order to receive disability-related academic accommodations students must first be registered with CSDS. Students who have a documented disability or suspect they may have a disability are invited to schedule an interview by calling (718) 951-5538 or emailing testingcsds@brooklyn.cuny.edu. If you have already registered with CSDS, email testingcsds@brooklyn.cuny.edu to ensure the accommodation email is sent to your professor.

Immigrant Student Success Office. The mission of the Immigrant Student Success Office is to recruit, enroll, and retain students, with an emphasis on new immigrants, such as students granted Deferred Action for Childhood Arrivals (DACA) who identify with the Development, Relief and Education for Alien Minors Act (DREAMERS), and first-generation students by providing the necessary academic and non-academic support to ensure graduation from Brooklyn College in a timely manner.
`brooklyn.cuny.edu/web/about/offices/studentaffairs/student-support-services/isso.php`

Off-campus Resources.

NYC Well
English: 1-888-NYC-Well (1-888-693-9355), Press 2
Espanol: 1-888-692-9355, Press 3
Text WELL to 65173
Free confidential mental health support for NYC residents:
`https://nycwell.cityofnewyork.us/en/`

Crisis Text Line
Text HOME to 741741
`https://www.crisistextline.org/`