Course Syllabus

MATH 5248 - Cryptology and Number Theory
Spring 2021, University of Minnesota
Section 03

About this course and syllabus

Welcome to MATH 5248, Cryptology and Number Theory. This document contains all the information you need to know about the course. **Your job is to read this document carefully in the first week of class and familiarize yourself with how this course works and maintain that familiarity throughout the semester.** Almost all questions about the course that you might ask can be answered by referencing the syllabus.

Course catalog description: Classical cryptosystems. One-time pads, perfect secrecy. Public key ciphers: RSA, discrete log. Euclidean algorithm, finite fields, quadratic reciprocity. Message digest, hash functions. Protocols: key exchange, secret sharing, zero-knowledge proofs. Probabilistic algorithms: pseudoprimes, prime factorization. Pseudo-random numbers. Elliptic curves. **prereq**: 2 sems soph math

Note: This is a list of *possible* topics, not all topics in the description will be covered this semester.

Course information

- **Meetings:** We meet *T/Th* in *Vincent Hall 1* from 2:30-3:45pm.
- **Instructor:** Kris Hollingsworth, Ph.D., Assistant Professor of Mathematics.
- **Instructor office:** Vincent Hall 8, just down the hall from the classroom.
- **Instructor email:** kgh@umn.edu
- **Office hours:** To be determined by student vote during the first week of classes.
- **Appointments:** You do not need an appointment for office hours; just drop in. If you need a face-to-face meeting outside of office hours, email me to schedule an appointment—I will accommodate as many students as my schedule allows each week.
- **Contacting the instructor:** There are two main ways to reach me outside of office hours or appointments: through email or through the messaging app known as *slack*.
- **Instructor availability: I am generally unavailable after 7pm weekdays and on weekends** in order to devote time to family, rest, and other projects. Messages received during these times will receive attention once I am back online. Otherwise, you can expect to receive a response to your message within 6 working hours, often sooner. If you post questions to Slack, you may receive answers from other students enrolled in the course more quickly.
- **Last updated:** August 28, 2021

Textbook: There is no required textbook for this section of the course, although the following resources may be helpful:

- The companion text for this course is the second edition printing of *An introduction to mathematical cryptography*, by Hoffstein, Pipher, and Silverman. You can download a free PDF copy (legally) provided by the university library. If you prefer a physical copy, you can also purchase a "myCopy" edition directly from the publisher for $25.00. For either option use the link and your UMN login.

- The above textbook gives a good treatment of most of the cryptology topics for the course, but the presentation of number theory can be quite terse. As a supplement, I would recommend Number Theory in Context and Interactive by Karl-Dieter Crisman, which is freely available online.

Technology: The course will use the following technology to promote learning:

- We will be using **Doenet.org** (Distributed Open Education Network), currently in alpha testing and being developed right here at the University of Minnesota's School of Mathematics, for our pre-class assignments. (Unfortunately the University is slow to update our security certifications — which is ironic for our class in particular. You may get warnings about this when following the above link.)
- The **Slack** group collaboration app for discussion and questions between classes. We will also use Slack for all course announcements and communication. Slack is free and can be downloaded as a native app for Windows and macOS as well as on mobile platforms; it can be downloaded from the appropriate app store, or used online at slack.com. You can find the invitation to our slack channel on the Canvas course page or right here.
- Other technologies may include **python3** or **Google sheets** as a means to implement coding projects. No previous coding knowledge is required to be successful in this course.

In addition to the above, the course has a Canvas site where you will submit work on Challenge problems (discussed below). It also hosts the course calendar, syllabus, and other documentation.

What will I learn?

At a high level, after successfully completing this course, you will be able to:

- Define, explain, and relate the key concepts of cryptology and elementary number theory.
- Write about mathematics using complete English sentences and proper mathematical notation.
- Gain comfort in working through problems in which the full solution is not clear when started by either engaging in self-directed learning and experimentation or in synthesizing multiple techniques from the course material.
- Use feedback to understand and learn from mistakes.

Additionally, you will gain greater skill at mathematical proofs, using statistical and probabilistic tools to recognize patterns, and connecting abstract mathematics to real-world applications.

More specifically, see the last page of this document for core skills on which you will be assessed directly through short quizzes.

What is expected of me in this course?

I want you to be successful in this course. I will do my utmost to help you do this by creating and maintaining a learning environment based on challenge and support and giving my highest professional commitment to your success and well-being. **But I cannot create success for you.** This comes from cooperation with me, interaction with your classmates, and diligent effort throughout the course.

To be successful in this course, you need to make sure you are always giving an effort to do the following:

- **Prepare for class** through the *Preclass Guided Practice* (details below).

- **Attend** all class meetings and **participate** actively during class activities.
- **Be proactive in completing course work** and **avoid procrastination** in all things.
- **Take initiative to seek out help** when you are stuck or have a question using office visits, Slack posts, study groups, and whatever else works for you!
- **Maintain a positive attitude** about the class and what you are learning.

By enrolling in this section of MATH 5248, you are agreeing to all of these expectations. During the first week of the course, you will be asked to digitally sign an agreement that states this.

What will I do to learn?

Learning happens by **doing**, not just by listening or watching. To learn the concepts in this course, you'll be doing a wide range of **active learning** tasks both in and outside of class.

- *Outside of class,* you'll work actively to get your first contact with new concepts through structured **Preclass Guided Practice** activities. Then, following class meetings, you'll be working on activities that ask you to extend the basics by solving both theoretical and applied problems called **Challenge Problems** involving, or highly related to, what you learn in class.
- *In class,* you'll be working with your classmates to make sense of concepts and work on creative applications of those basics through group problem-solving sessions, presentations of solutions to the class, discussions based on the Preclass Guided Practice activities, and more.

Basic skills: Learning targets and the Final Exam

The basic skills you will learn in the course are given in a list of 20 **Learning Targets**. The list is appended to the end of this syllabus. During the course, you'll be expected to provide evidence that you can perform the tasks that are given in the Learning Targets by completing **Learning Target Assessments**. The are short quizzes, each of which addresses a single Learning Target. For example, the Learning Target Assessment for Learning Target MA2 ("I will be able to use the *fast power algorithm* to compute high powers of numbers modulo some integer n") may ask you to compute 3-4 such values.

Learning Target Assessments are graded either **Satisfactory** or **Unsatisfactory**. See the section below titled "Revision Process" for information on re-taking Learning Target Assessments that are marked Unsatisfactory.

What constitutes Satisfactory or Unsatisfactory work will be spelled out specifically and will be printed at the bottom of each Learning Target Assessment.

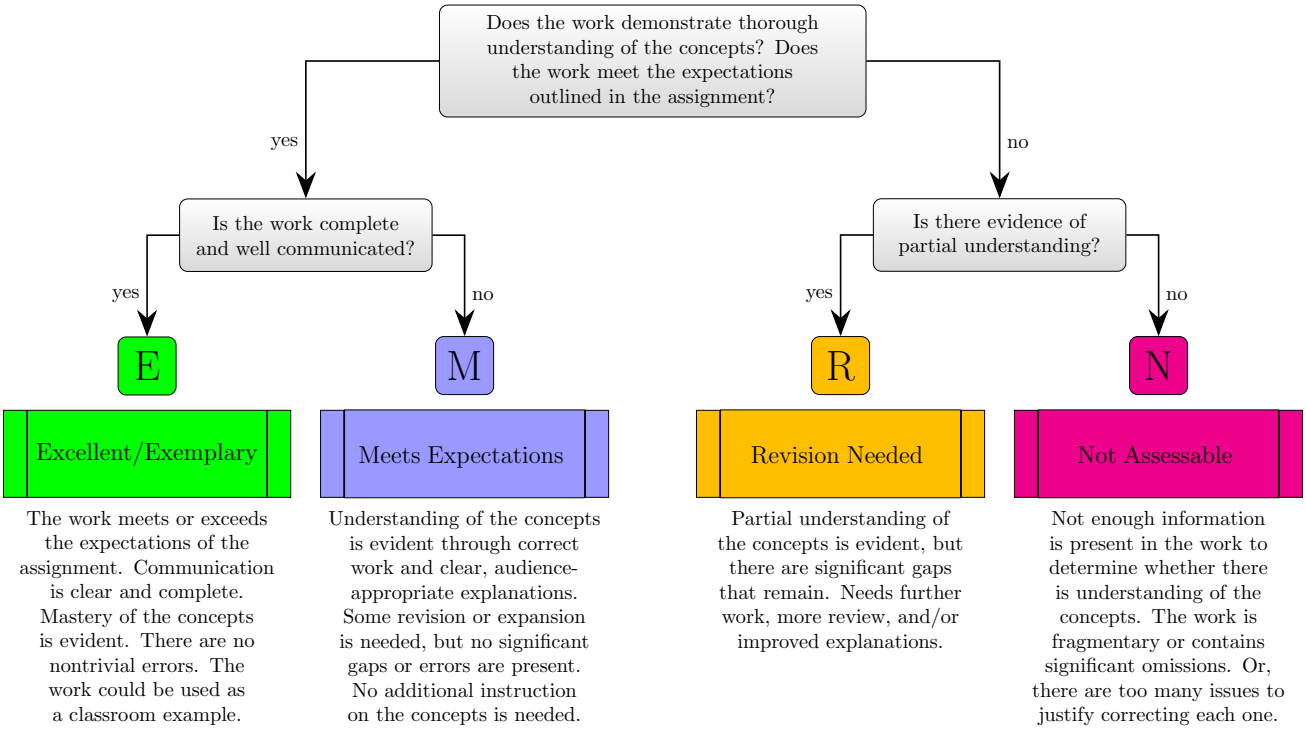
Your mastery of basic skills will be assessed through a **comprehensive final exam** given during finals week. The final exam will consist of ten (10) randomly selected Learning Target Assessments that have already been given in the course as well as a few short response and/or true/false conceptual questions. See the section "Grading System" below for details. The exam period for your section is on Wednesday, December 22 at 10:30 a.m. to 12:30 p.m. (I had absolutely no say in this scheduling).

Applications: Challenge Problems

Your ability to extend the basics to solve challenging problems is measured by completing **Challenge Problems**. Each challenge Problem is a take-home assignment featuring a single chal-

lenging problem to solve. Challenge Problems require not only correct solutions, but clear, correct, persuasive, and well-written solutions presented with professional-looking write-ups.

Each Challenge Problem is graded using the **EMRN rubric** that classifies the work with marks of **E** ("Excellent" or "Exemplary"), **M** ("Meets Expectations"), **R** ("Needs Revision"), or **N** ("Not Assessable"). The visual below shows how these are assigned:



EMRN rubric based on the EMRF rubric, due to Rodney Stutzman and Kimberly Race: https://eric.ed.gov/?id=EJ717675

At least 12 Challenge Problems will be posted during the semester. Here are four things to know about these:

1. **You do not have to do all posted challenges.** Instead, you will choose from among the ones posted and focus only on the ones you think you would enjoy doing.
2. **There are no fixed deadlines on Challenge Problems.** Instead, choose a problem, work on it at your own pace until you believe it is ready to be assessed, then turn it in (see "Revision Process" below for how to turn in your work).
3. **You can revise any Challenge Problem submission if you want to improve your work.** Your submissions will be given extensive written or verbal feedback to draw your attention to any issues that can be corrected or improved, and you can resubmit work repeatedly until you are satisfied with the results. Details in "Revision Process" below.
4. **You may propose your own topics for Challenge Problems.** Given the breadth of possible topics for this course, we will never be able to cover them all in one semester. If there is a topic related to number theory or cryptology you wish was being covered but is not, fear not! You may contact me and we can negotiate a challenge problem to help you begin learning the topic as part of the course through self-directed learning, with all the available support (both myself and your classmates) as additional resources to help in this effort.

Engagement Credits and Preclass Guided Practice *Engagement* in the course means preparing well for class and participating productively both in and outside of class. The more engaged you

are in the class, the better you will learn the material; conversely, students who disengage and try to complete the course from a distance generally have more difficulty succeeding.

Your level of engagement in this course will be measured by earning **Engagement Credits**. An Engagement Credit may be awarded for such accomplishments as participating in a problem presentation or group activity in class, giving a particularly helpful comment in an online discussion in between classes, or even asking an insightful question in office hours. Some engagement credit opportunities may be announced in advance, but many will be unannounced, and you will need to be present in class and present online to earn them (see section on COVID-19 policies for additional information).

The primary means of earning engagement credits is through **Preclass Guided Practice** assignments. Guided Practice provides you with a structured introduction to the basic ideas of new material so that we don't have to spend time in class doing lectures on the material. They provide readings, videos to watch, and other media to help you acquire the new skills we will work with in class, along with exercises to build your basic skill fluency. The exercises are submitted online so that the upcoming class time can be customized based on what students know and do not know.

Preclass Guided Assessments are graded **Satisfactory** or **Unsatisfactory**, and every "Satisfactory" grade earns one engagement credit. Preclass Guided Practice is graded Satisfactory if it meets the following criteria:

1. **The assignment is submitted before the deadline,** which is usually 11:59pm Central time the day before the class meeting. Submissions past this deadline will be automatically marked Unsatisfactory.
2. **Every exercise and question has a response that shows a good-faith effort to be right or complete.** Submissions that have exercises where a good-faith effort is not evident — for example, if the response is "I don't know", "I don't understand", answered with a semantically incorrect statement[1], or answered with a random guess — will be automatically marked Unsatisfactory. If you are truly stuck on a Preclass Guided Practice, you are expected to give yourself enough advance time to ask a question about it in office hours, in group work with others, or on the #guidedpractice channel on Slack.

Please note that *correctness is not factored into the grade*, so you should feel free to give your best effort on each one without fear of being counted off for wrong answers. In fact, misconceptions about the material are part of what Preclass Guided Practice assignments are set up to collect so we can work on them.

Grading system

Your course grade is determined by both the **quality** and **quantity** of the work that you submit in the class. There is a two-step process for determining your grade at the end of the semester.

1. Using your **Learning Target Assessments** and **Challenge Problems** (CPs in the table below), determine your "base grade", which is A, B, C, D, or F.
2. Then, using your **Engagement Credits** and **Final Exam results**, determine if the base grade should have a "plus" or "minus" on it and any other modifications that need to be made to the base grade.

[1] A statement that is *semantically incorrect* is grammatically correct but doesn't make sense and communicates no information. For example, "Purple people eaters palpitate precipitously" is semantically incorrect. So is "I plugged an equation into the problem".

Details on each step of the process are below.

Step 1: Determine the base grade. To help determine the base grade, look up your accomplishments in the following table:

To earn:	Accomplish the following:
A	Earn **Satisfactory** marks on 19 Learning Targets; *and* complete **10 CPs** with an **M** mark or better, including at least 5 **E** marks.
B	Earn **Satisfactory** marks on 17 Learning Targets; *and* complete **7 CPs** with an **M** mark or better, including at least 3 **E** marks.
C	Earn **Satisfactory** marks on 15 Learning Targets; *and* complete **5 CPs** with an **M** mark or better. No **E** marks required.
D	Earn **Satisfactory** marks on 13 Learning Targets. No Challenge Problems required.

Additionally: Students intending to earn an A or B mark in the course *must complete at least two Challenge Problems that are designated as a* ***Theory*** *problem.* Failure to complete this requirement will result in the final grade after modifications (see below) being lowered by one half letter (A to A-, B- to C+, etc.). The Theory requirement *only* applies to base grades of A or B.

Please note that *all* requirements for a base grade must be met in order to earn that grade. The base grade earned is the *highest* grade for which ***all*** requirements are met. Fore example, a student who completes 10 Challenge Problems with all **E** marks, but who earns Satisfactory rating on only 15 Learning Targets, will receive a base grade of "C". A grade of "F" is awarded if the requirements for a "D" are not met.

Step 2: Determine modifications to the base grade. The base grade can be raised by a plus, lowered by a minus, or lowered by an entire letter grade as follows:

- Add a **plus** to the base grade if you earn at least **60** engagement credits *and* earn **at least an 85%** on the final exam.
- Add a **minus** to the base grade if you earn between **30 and 39** engagement credits (inclusively) *or* earn **between 50% and 69%** (inclusively) on the final exam.
- Lower the base grade **one full letter** if you earn **fewer than 30** engagement credits *or* earn **lower than 50%** on the final exam.

(If you end the course with at least 40 engagement credits and earn at least 70% on the final exam, you will incur no penalty on your base grade.)

Note the "and" in the first item and the "or" in the second two. Also, please note that due to potential changes in the schedule and calendar, the amounts of engagement credits above may change. To be safe, always strive to earn as many engagement credits as possible, and note that since around 20 of the engagement credits come from Preclass Guided Practice, **being consistent about completing Guided Practice assignments is the simplest way to maintain or improve your base grade.**

Exceptions to the above rule: UMN does not award grades of A+ or D-. Therefore, the rule for plus grades does not apply to grades of "A", and the rule for minus grades does not apply to grades of "D". However, both A and D grades can be lowered by a full letter, A grades can still receive a minus, while D grades can still earn a plus.

To help you understand this grading system, a flowchart for the system will be provided along with a checklist for keeping track of your class accomplishments. We will take time during class

and on Preclass Guided Practice assignments to practice the system, and progress reports will occasionally be released to you to show you how you are fairing and how much more you need to accomplish to earn the grade you are targeting.

Submitting work and revisions

At the heart of the learning process in MATH 5248 is a system of submission and revision of your work that will allow you to make improvements to your work based on instructor feedback. Most grades on work are not final; you will have the chance on almost every submitted item to revise and resubmit to improve its quality. First, let's detail how to submit your work in the first place.

Submission of work

Submission of **Learning Target assessments** is easy: These are done on paper in class meetings on the days listed on the course Canvas page (see the posted calendar), so you simply turn in your work when done in class. Similarly easy is submission of the **Preclass Guided Practice:** these are done using Doenet that are linked to the assignments in Canvas.

Challenge Problems are a little more involved. Each Challenge Problem is posted to the course Canvas site in the *Challenge Problem* area as an "assignment". At the place where the Challenge Problem is posted, there will be a file to download that contains the tasks to be completed and any special instructions or grading criteria that pertain to it. Your work on the Challenge Problem is to be typed up, saved as a Word or PDF document (PDF preferred), and then uploaded to the place at the "Assignment" where you can upload files. Once uploaded, feedback is left on the submission itself or in the "notes" on Canvas SpeedGrader.

Revision

You can revise any Learning Target assessment and any Challenge Problem as often as you need (with some restrictions; see below) **until you are satisfied with the results.** The process for doing these revisions is different for the two kinds of work.

Revising Learning Target Assessments: All Learning Target Assessments must be attempted during a designated assessment period first. Once this has been done, if the grade is Unsatisfactory, you can retake the Learning Target Assessment in one of two ways.

1. You can retake it during a later assessment period in class by filling out an *Assessment Request Form* (linked on Canvas) prior to the assessment period. A new version of the Learning Target Assessment will be written up and made available to you at that period.
2. You can schedule a 15-minute session during office or appointment hours to retake up to two (2) Learning Target assessments orally. Please note the restriction on both the time (15 minutes) and number of assessments (1 appointment per week, 2 assessments per appointment) that can be done orally. Appointment slots are available on a first-come first served basis.

Please note that oral assessments are *only for retakes*. You must first make a good-faith effort to attempt a Learning Target Assessment on paper in class and receive Unsatisfactory marks on it to be eligible for an oral retake.

Revising Challenge Problems: Challenge Problem submissions can be revised and resubmitted by addressing the issues pointed out in the instructor feedback, then writing up a new draft and submitting to the same location on Canvas as the original submission. The new work will be regraded and given feedback, and you may revise again if needed.

In all retake/revision situations, the *highest grade attained so far* will be the one recorded in the gradebook.

Definition of a "week": For the purposes of this class, **each "week" begins at 12:00am Central time on Mondays and ends at 11:59pm Central time the following Sunday.**

Restrictions: The following restrictions apply to Challenge Problems:

- No more than **two Challenge Problem submissions per week may be made.** This can be two new submissions, a new submission and a revision, or two revisions. A third submission may be made if a token is spent (see below). This restriction is in place to ensure that students don't procrastinate until the end of the course to work on these assignments.
- **A token** (see below) **must be spent to revise any submission of a Challenge Problem that is marked "N"** (Not Assessable). This is in place to ensure students do not submit incomplete or significantly flawed work just to get feedback (rather get feedback through Office Hours, in class, or through Slack).

The following restrictions apply to Learning Target Assessments:

- Requests for in-class retakes of Learning Target Assessments **must be made using the Assessment Request Form by the stated deadline** in order to allow sufficient time to construct and copy the correct batch of assessments. Requests that come in after the deadline will be declined, and *students who attempt an assessment without requesting it will be charged one token per assessment.*
- The oral retake option is only for work that showed a good-faith and complete effort on paper initially but was rated Unsatisfactory. **Assessment work that is incomplete or does not show sufficient effort may require a second attempt on paper before an oral retake is allowed.** If this is the case, a note will be left on the paper assessment saying so. This is to prevent students from intentionally doing Unsatisfactory work in class because they want to do an oral exam instead.
- The oral retake option for Learning Target Assessments may be used **no more than once per week per student** and **must be scheduled at least 24 hours in advance.** Requests for oral retakes with less notice, including drop-in requests, will be declined. Students who are late for appointments may be asked to reschedule at a later date, and repeated issues of not showing up on time for appointments may result in not being allowed to use oral retakes at all in the future.

Finally, there are two important dates for your work:

- No requests for oral retakes of Learning Target Assessments will be accepted after 11:59pm Central time on Tuesday, December 14th. This means that the last round of oral assessments will take place during the last week of classes.
- No further submissions of Challenge problems, either new submissions or revisions, will be accepted after 11:59pm Central time on Sunday, December 19th.

Tokens

Tokens are a "currency" in the course that you can use to purchase exceptions to the course rules, especially the rules for revisions. Each student begins the course with three tokens, and tokens can purchase any of the following:

- One token buys a third Challenge Problem (new submission or revision) during a given week. Further tokens **may not** be spent to obtain fourth, fifth, etc. submissions.
- One token buys a second 15-minute oral retake appointment in a given week. Further tokens **may not** be spent to obtain a third, fourth, etc. appointment. All the rules above regarding scheduling still apply.
- Two tokens may also buy one engagement credit at the end of the semester.

Opportunities to earn more tokens may be made available during the semester.

Academic integrity and collaboration

Academic integrity refers to the concept that **the work that you do for UMN courses should accurately reflect your own efforts and not come significantly from the work of another.** Academic integrity means that your work is "integrated" with your understanding and that you are using personal integrity when doing your work.

If you are encountering so much pressure or stress in your life that you are tempted to break one of these policies, **STOP AND GET HELP from me (the professor).** I am committed to helping you succeed in the course through your legitimate hard work, and I am available and willing to work with you. And **remember that most work in the course can be revised and resubmitted to improve your grade,** which means that academic dishonestly really is not necessary to do well.

The university's student conduct code may be found online at the university's Office of Community Standards' website. Additional guidelines for CSE students may be found with the department's undergraduate academic conduct policy. **Every student has the responsibility of reading and understanding these policies, especially the consequences for engaging in academically dishonest activities.**

In MATH 5248, we will adopt the following specific policies to ensure academic integrity in your work. **It is each student's responsibility to understand these policies and abide by them all semester.**

- For work on **Preclass Guided Practice** assignments, *you may collaborate with others freely on the assignment but you must complete the assignment on your own,* and you may not simply copy from another (not that many computational exercises are randomly generated, making copying impractical anyway). Evidence that copying has taken place will be investigated as an academic integrity policy violation.
- For work on **Learning Target Assessments,** which are done either in class or in the office, and the **final exam**, *no collaboration with another person or resource may take place at all*, and any evidence that this has taken place will be investigated as an academic integrity policy violation.
- For work on **Challenge Problems**, you may collaborate with one or two other students at the level of sharing ideas and strategies for solving the problem. But, you may not collaborate at any level with any other person on the final written solutions that you submit for evaluation. This means that once you have discussed a problem with a collaborator, you must write your final solution independently (and joint writeups are not allowed). Solutions to the same problem from different students, even collaborators, should include differences that reflect each student's individual understanding and writing style. Excessive similarities in submitted solutions will be interpreted as evidence of inappropriate collaboration. Additionally, in your final solution, if you have collaborated in any way with

one or two other students, you must disclose the names of those students and give a short description of what you collaborated on. Any evidence that collaboration has gone farther than the extent described above, or any evidence of collaboration with another student who was not disclosed in your writeup, will be investigated as an academic integrity policy violation.

- Additionally, on Challenge Problems, if outside resources (websites, books, friends not in the class) are used to solve the problem, they must also be cited in the final writeup.

For all work in the class, **you may not look up solutions to any problems on the Internet or in other resources** without prior instructor permission. Any submitted solution that is substantially similar to one that appears on the internet will be considered evidence of academic dishonesty.

On any assignment that bears your name, if there is doubt that you were solely responsible for the final solution (or significantly responsible for the code in a programming problem), **you may be called upon to explain your reasoning on the entire solution to the professor in a one-on-one interview.** In such cases, you are individually responsible for understanding and being able to explain the entire submitted solution without the assistance of others, even if collaboration on the assignment is allowed. If, following the interview, I determine that you have overstepped the boundary for collaboration because you cannot explain the work, it will be taken as a sign of academic dishonesty and will be reported.

Finally, please note that the *minimum* penalty for academic dishonesty is to receive an "N" or "Unsatisfactory" mark on the assignment with no opportunity for future revision, and a report is filed with the Mathematics Department head, the Dean of Students, and the Dean of the College of Science and Engineering. More severe infractions of this policy, or if an infraction is not your first, could result in failure of the course or even suspension from the university.

Where to get help

For general help: The best way to get help in the course is to use the resources that are closest to you and which you have already paid for, name *office hours* and *Slack*. Take a "both/and" approach and seek out help whenever you need it through a combination of these and other resources.

For students with special learning needs: Any student who requires accommodation because of a physical or learning disability must contact the Disability Resource Center at drc.umn.edu or by phone at (612) 626-1333. After you have documented your disability, please make an appointment or contact me by email to discuss your specific needs.

For help with technology: If you encounter any issues with Canvas, your email, or any other technology that is "owned" by UMN, you can contact UMN's IT help desk. They have help by email, online chat, phone, and walk-in service.

If you are encountering issues with any other class technology, please use the #**tech** channel on Slack, search the Internet for help, or both. Make sure to try and resolve the issue yourself before asking others; and please do not simply email me (the professor) because I am often unable to provide tech support. Instead, a public message to the #**tech** channel will be seen not only by me but also your classmates, and this will give you more chances for help as they may have also encountered and already resolved the same issue.

For help with writing: Challenge Problems will often involve a fair amount of writing, and basic writing standards may make the difference between an **E** and **M** grade. But fear not! The university's Center for Writing is available to help you with free face-to-face or online

consultations at all stages of the writing process. Please note that seeking help from the Writing Center does not violate academic integrity policies.

For mental health: Recent times have been exceptionally stressful, which can seriously alter your ability to learn (on physical, mental, and emotional levels). The can stem from strained relationships, increased anxiety (like living through a pandemic), alcohol/drug problems, feeling down, difficulty concentrating and/or lack of motivation. You can learn more about the broad range of confidential mental health services available on campus via the Student Mental Health Website (mentalhealth.umn.edu).

Course schedule and important dates

All date-related information for the course will eventually be housed on Canvas, and summarized in a compact, one-page document available in the "Course Resources" module there. This includes due dates, important university dates, and more.

Course Materials

All course materials (lectures, lecture nots, class activities, challenge problems, learning targets, etc...) are either my intellectual property or borrowed with permission from another instructor who owns the intellectual rights. If you want to post any materials publicly (such as on Chegg or CourseHero) you must have explicit, written permission to do so.

Disclaimer

Changes to this syllabus may occur during the semester. In those cases, the changes will be announced in class and online, and if appropriate, students will be given a voice on how the changes will be implemented. Again, it is your responsibility to attend class and process all the information passed along in course announcements so that you will be aware of any changes that take place.

Last updated: August 28, 2021

Additional Policies:

Any standards not addressed in this document are likely covered by the University's standard policies.

COVID-19 policies

The university's updates on COVID-19 may be found on their COVID-19 Updates page.

The College of Science and Engineering has additional return to campus resources and information which you can find on their website.

Additionally, this course will remain flexible with regards to COVID-19. Per University policy, you will be expected to wear a mask. You are also expected to be respectful of other students in the classroom and create an inclusive, positive learning environment. If you are feeling sick, you are expected to stay home. If you need to miss an assessment day, we will schedule a make-up for the written assessments you would have taken that day. Please be aware, **all course policies will remain flexible as situations change throughout the semester**.

Acknowledgements:

In putting together this syllabus and the course materials, the feedback of Dr. Hannah Burson (UMN) was invaluable, and I thank her for her assitance. The generously shared resources of Dr.

David Clark (a former MathCEP postdoc) and Dr. Robert Talbert, both currently at GVSU were incredibly helpful in the grading design of this course. Additional reference materials were also provided by Dr. Patricia Klein (UMN).

About the instructor

I'm Kris Hollingsworth, and I am an Assistant Professor (MathCEP Postdoc) at the School of Mathematics at the University of Minnesota. I grew up in the Ozark Mountains in North Central Arkansas, and I spent a lot of time outdoors hiking, bicycling, and hammock camping. I don't get a lot of time for hiking or camping these days, but I still commute to campus by bicycle every day.

I started homeschooling after sixth grade, with almost no math curriculum. Consequently, I didn't really start learning mathematics until I started at the community college when I was 25. Before that, I spent 6 years as a (self-taught) computer programmer working primarily on transportation and logistics software for large motor fleet companies, followed by 2 years as a freelance photographer (My favorite CV line item from this time is being published in a magazine titled *Blood & Thunder*!). At school, I started as a business major with a minor in studio art, and the major quickly changed to mathematics. I eventually transfered and graduated from the University of Central Arkansas with a BA in Mathematics and a minor in studio art (mostly printmaking and ceramics). After taking a year off to teach at a community college, I went to the University of Delaware for my Master's and Ph.D. in Pure Mathematics, writing my dissertation on the underlying mathematical framework for high-dimensional signal processing and studying constructions of such schemes. Now, I spend a lot of time crafting materials for the courses I teach while I prepare to go back on the job market for my hopefully forever job.

I live in Saint Paul, MN, with my amazing partner and our dog Gemma. We all enjoy cooking, reading, and bicycling. I enjoy cleaning, although neither of the other two do. You can follow Gemma's personal adventures on her Instagram (@GemmaIsAGoodGirl), which just shows you that my dog is better at social media than I am. However, you can find me online through my website at sites.google.com/view/math-kgh.

Fall 2021, 5248-03 Learning Targets

Modular Arithmetic (MA)

(MA1) I will be able to compute congruences $a \equiv b \mod n$ for any integer values (a, b, n) and any cross-section of $\mathbb{Z}/n\mathbb{Z}$.

(MA2) I will be able to use the *fast power algorithm* to compute high powers of numbers modulo some integer n.

(MA3) I will be able to use the *Euclidean algorithm* to find the inverse of (an equivalence class) of one number modulo another.

(MA4) I will be able to use the *Chinese Remainder Theorem* to solve a linear system of modular Diophantine equations where the moduli are pairwise coprime.

(MA5) I will be able to prove that an equation cannot have integer solutions by showing it does not have solutions modulo some integer.

(MA6) I will be able to use *Fermat's Little Theorem* in a proof or to substantially simplify a computation.

(MA7) I will be able to use *Euler's criterion* to determine if a number is a quadratic residue modulo another number.

Counting and Probability (CP)

(CP1) I will be able to compute the number of possible permutations and combinations that can be made from a given set of characters.

(CP2) I will be able to compute conditional probabilities using tree diagrams and Bayes' formula.

(CP3) I will be able to compute the expected value of a random variable.

Divisibility and Prime Numbers (DP)

(DP1) I will be able to use the definition of primes (given in class) in a proof.

(DP2) I will be able to use the definition of divisibility in a proof.

(DP3) I will be able to compute $\varphi(n)$, the number of positive integers coprime to n.

(DP4) I will be able to use decimal expansions and modular arithmetic to prove small order divisibility tests.

Classical Cryptosystems (CC)

(CC1) I will be able to use a known plaintext attack to determine the key of any of the classical ciphers studied in class.

(CC2) I will be able to identify likely candidates for the cipher used to encrypt some data using information like frequency distributions and index of coincidence.

Modern Cryptosystems (MC)

(MC1) I will be able to use a given subset of Diffie-Hellman values to find other important Diffie-Hellman values.

(MC2) I will be able to use a given subset of El Gamal values to encrypt, decrypt, or find other important El Gamal values.

(MC3) I will be able to use a given subset of RSA values to encrypt, decrypt, or find other important RSA values.