Math 125-H01 Discrete Mathematics with Cybersecurity

George Mason University

Spring 2022 Syllabus

Course Description

Every day, 143,000 terabytes of data are transferred across the internet, including financial transactions, medical records, and sensitive client data. Half of this traffic is secured through encryption, relying on mathematical algorithms such as RSA to encode the data in a way that only the recipient can decode. We will take a deep look at the components of this process. We will start with classical ciphers and networking, then develop number theory and programming skills needed to implement RSA from scratch.

Learning Objectives: Math 125 introduces ideas of discrete mathematics and combinatorial proof techniques including mathematical induction, sets, graphs, trees, recursion, and enumeration. In Math 125H we will address these topics while discovering and implementing the mathematics of cybersecurity, building up to understanding and using the RSA cryptosystem. We will also develop general mathematical skills including problem solving, critical thinking, and oral and written technical communication.

Prerequisite: Completion of a calculus course with a B or better.

Textbook: We will not follow a textbook, but *Discrete Mathematics with Graph Theory 3rd ed.* by Goodaire and Parmenter is the textbook for other sections of Math 125 and may be useful as a reference.

Course Meetings: Mondays, Wednesdays, and Thursdays, 3:00-4:15pm. Online and synchronous.

Course Home Page: Blackboard, `https://mymasonportal.gmu.edu/`

Instructor Information

Name: Dr. Kirsch (she/her/hers)

Student Office Hours: By appointment, on Zoom

Email Address: rkirsch4 @ gmu.edu

Anticipated Project List

1. Decryption

2. Graph Theory

3. Semi-Automatic Decryption

4. An Axiomatic Approach

5. Numbers and Basic Arithmetic

6. Advanced Arithmetic

7. Adding in Binary

8. Fast Multiplication

9. Divisibility

10. Modular Equivalence

11. Modular Arithmetic

12. Kid Krypto

13. MyPowerMod

14. RSA

Assessments and Letter Grades

Project Reports:

There will be 14 in-class projects. For each in-class project (except Project 14), you will individually write a brief formal report (about 1 page per class session), contributing toward your own comprehensive set of course notes. Reports should provide a description of the results and takeaways of the project, including any useful examples, definitions, algorithms, or theorems; and should generally follow the same outline as the worksheet.

There will be 3 chances to submit each report via Blackboard: 1 week after the corresponding project is completed in class, 1 week after the first submission is graded, and 1 week after the second submission is graded.

Each report will be graded as Excellent/Good/Incomplete/Unsubmitted, based on the inclusion of relevant results, demonstrated progress toward the learning objectives, and the clarity of the technical communication, including overall style. Extended feedback will be available during student office hours.

Idea Assessments:

The course will be divided into 4 units. For each unit, you will meet one-on-one with Dr. Kirsch for an idea assessment, to demonstrate your understanding of the unit. Dr. Kirsch will first confirm the unit you are being tested for, and then draw three questions at random from the Idea Assessment Question Set. You will be able to skip one question, and need to respond correctly to the other two questions. Dr. Kirsch may ask a follow-up question, e.g. asking for a definition of a term you have used, for details that you skipped over, or for an example of an idea you are explaining. No notes or other assistance may be used during idea assessments.

Idea Assessment Question Sets will be provided in advance. To prepare for idea assessments, you should write out solutions to all questions and practice explaining them during office hours and study sessions.

To be eligible for an assessment you must have at most two unsubmitted or incomplete project reports for that unit. Idea assessments will be graded pass/fail based on demonstrated understanding of the ideas. You may re-attempt them until you pass, at most once per assessment date listed below, as long as you are eligible.

Idea assessments are available on the following 8 dates: February 10, February 24, March 10, March 24, April 7, April 21-22, May 5, May 16 (finals day). If you need an alternative date for an idea assessment, please email Dr. Kirsch as soon as possible, briefly stating the reason and suggesting an alternative date.

Letter Grades:

Letter grades will be assigned at the end of the semester based on the following requirements for project reports and idea assessments. All requirements must be met to earn the grade.

- A+: All 4 idea assessments passed and all reports Excellent.

- A: All 4 idea assessments passed, at least 10 Excellent reports, and at most 1 unsubmitted/incomplete report.

- B: At least 3 idea assessments passed, at least 4 Excellent reports, and at most 2 unsubmitted/incomplete reports.

- C: At least 2 idea assessments passed and at most 4 unsubmitted/incomplete reports.

University Policies

Disability Services: Disability Services at George Mason University is committed to providing equitable access to learning opportunities for all students by upholding the laws that ensure equal treatment of people with disabilities. If you are seeking accommodations for this class, please visit `https://ds.gmu.edu/` for detailed information about the Disability Services registration process. Then please discuss your approved accommodations with me. Disability Services is located in Student Union Building I (SUB I), Suite 2500. Email: ods@gmu.edu. Phone: (703) 993-2474.

Academic Integrity: Students must be responsible for their own work, and students and faculty must take on the responsibility of dealing explicitly with violations. The tenet must be a foundation of our university culture. See Academic Integrity.

Honor Code: Students must adhere to the guidelines of the George Mason University Honor Code. See the Honor Code.

University Policies: Students must follow the university policies. See University Policies.

Responsible Use of Computing: Students must follow the university policy for Responsible Use of Computing. See Responsible Use of Computing.

University Calendar: Details regarding the current Academic Calendars. See the Academic Calendars.

Students are expected to follow courteous Internet etiquette.