Math 125 H01: Discrete Mathematics and Cybersecurity

George Mason University, Spring 2021
Prof. Anton Lukyanenko, alukyane@gmu.edu

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 the 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.

Overview

We will cover all of the required material of Math125 while also discovering and implementing the mathematics of cybersecurity in a series of small projects. Grades will be assigned based on project reports and idea assessments. Here's a breakdown of the plan for the semester:

Class (MWF 10:30-11:45 via Zoom)

- **Research projects:** most of the course time will be devoted to group-based discovery of the ideas we need, including finding useful definitions, theorems, and proofs.
- **Development projects:** we will implement our ideas and explore new ones using Mathematica.
- **Communication:** when we make significant progress on a project, a group be asked to present their results, with another other group providing friendly feedback.

Studying (groups encouraged)

- **Idea question sets:** towards the end of each of the 5 units, a list of approximately 10 key questions will be provided to help guide studying.
- **Other ideas:** some ideas and definitions will not be covered explicitly in the idea question sets, but will be important to understand and remember; students should review their notes and worksheets to identify these concepts.
- **Book:** the standard book for Math125 is *Discrete Mathematics with Graph Theory 3rd ed.* by Goodaire and Parmenter. We will not use it, but it may be useful as a reference.
- **Office hours:** will be available daily after class, as well as by appointment, and are a great chance to clear up ideas or get feedback on your work.
- **Message board:** available on Blackboard for discussions and questions.

Evaluation (more on this below)

- **Reports:** each project will be written up as a brief formal report (about 1 page per course session), contributing towards a comprehensive set of course notes,
- **Idea assessments:** for each unit, students will demonstrate their understanding of the content by answering questions from the corresponding idea question set, with opportunities for retakes.

Letter grades

Letter grades will be assigned at the end of the semester based on the following requirements. All requirements must be satisfied to get the grade. There will be 5 idea question sets, and approximately 20 project reports.

- A+: 5 idea assessments passed, failing at most once, **and** all reports Excellent.
- A: 5 idea assessments passed, 14 Excellent reports, **and** at most 1 unsubmitted/unsatisfactory report.
- B: 4 idea assessments passed, 6 Excellent reports, **and** at most 2 unsubmitted/unsatisfactory report.
- C: 3 idea assessments passed **and** at most 4 unsubmitted/unsatisfactory reports.

Links

Lectures and office hours: `http://gmu.zoom.us/j/93765774016?pwd=WU5UT29kY2dYOEFZSEE1cEFsd0pYdz09`

Idea assessments: `http://gmu.zoom.us/j/96054506380?pwd=WFhGa3ViR2duK0JKRGZqbmVLTVNCZz09`

Assessment scheduling: `http://calendly.com/alukyane/assessment`

Mathematica: `http://science.gmu.edu/information-technology/software-resources/wolfram-mathematica`

LaTeX: `http://overleaf.com` Whiteboard: `https://awwapp.com/b/uiwkuwgbnjy8g/`

Reports

Individual reports will be submitted for each of the approximately 20 projects (research or development), corresponding to an in-class worksheet. 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. Each in-class day will contribute about 1 page of content to the report. Use of LaTeX is encouraged but not required.

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 one week after the second submission is graded. Late submissions will not be accepted.

Each report will be graded as Excellent/Satisfactory/Unsatisfactory, based on the inclusion of relevant results and overall style. Extended feedback will be available during office hours.

Idea Assessments

During an idea assessment, you will meet one-on-one with Dr. Lukyanenko to demonstrate your understanding of one of the units of the course.

Dr. Lukyanenko will first confirm the unit you are being tested for, and then draw three questions at random from the Idea Question Set. You will be able to skip one question, and need to respond correctly to the other two questions. Dr. Lukyanenko 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.

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 unsatisfactory reports. No notes or other assistance is permissible during idea assessments.

Assessments are available on the following 8 dates: February 4, February 18, March 4, March 18, April 1, April 15, April 29, May 5 (Wednesday, finals day!).

Participation

Active teamwork is critical for learning **and** helping your teammates learn. Three absences will be allowed, after which any unexcused absence will be penalized with a 1/3-letter-grade reduction of the final grade.

Please help make this class good for everyone's learning (including your own!) and generally pleasant, and please bring any problems to the professor's attention as soon as possible. Keep in mind that:

- Math is hard, and consistent work is more impressive than starting off well-prepared.
- It's helpful (and more fun) to work together with others on the reports and idea questions.
- That said, you should contribute substantially to all work and make sure to write your own solutions.
- If you're feeling behind, make sure to speak up in class, find study groups, and come to office hours.
- If you're feeling confident, do help others learn, but make sure you're listening more than talking.

University Resources

The following groups exist to support student learning, with both academic and non-academic issues, so don't hesitate to contact them:

- Mathematics Tutoring Center: `http://math.gmu.edu/tutor-center.php/`
- General Advising: `http://advising.gmu.edu/`
- Student Support and Advocacy Center: `https://ssac.gmu.edu/`
- Disability Services: `http://ds.gmu.edu/`
- Counseling and Psychological Services: `https://caps.gmu.edu/`
- Compliance Diversity and Ethics Office: `https://diversity.gmu.edu/`

Issues affecting learning may also be discussed with the professor. In certain cases, the professor is required to report such issues to appropriate university units.

Accommodations

If you require accommodations, approved by Disability Services, please let Dr. Lukyanenko know as soon as possible. If you think you may need accommodations, please contact one of the relevant University Resources listed above.