Math 493
Mathematics of Cryptography: an Introduction
George Mason University, Fall 2018
`http://lukyanenko.net/teaching/2018/493/`

Instructor:
Anton Lukyanenko
alukyane@gmu.edu

Office Hours:
Thursdays 4:30-5:55pm & by appointment
4113 Exploratory Hall

Class:
Mondays-Wednesdays 10:30-11:45
4301 Exploratory Hall

Thursdays 10:30-11:45
4307 Exploratory Hall

Course content. 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.

In this class, we will see how cryptography works first-hand. We will start with classical ciphers (Atbash and Caesar ciphers) and develop our mathematical techniques and programming abilities until we are able to implement RSA from scratch.

Topics covered in the course lead into the following majors: mathematics, computer science, electrical engineering, and cyber security engineering.

Workflow and assignments. The course is teamwork-based, with discussion guided by worksheets (in the classroom) and labs (in the computer lab).

In the classroom, we will develop mathematical theory in small groups. Once enough problems on a worksheet are solved, a group will present them on the board. Once the entire worksheet is completed (however long that takes), it is written up carefully at home and becomes part of the final textbook. The homework (supplementary exercises) listed at the end of each worksheet is due a week after the worksheet is completed.

In the computer lab, we will implement the theory we develop in class and explore some additional topics. Computer lab assignments are turned in once they are completed and do not contain any further homework.

Grade breakdown. For the final grade, assignments will be weighed as follows:

Homework: 35%
Class participation: 25%
Labs: 20%
Final textbook: 20%

Letter grades will be based on the usual breakdown (90-93.3 for A-, 93.4-96.6 for A, 96.7-100 for A+, etc).

Worksheets There are 13 worksheets, which build up the mathematical theory we need to verify that the RSA algorithm works as desired:

1. Codes
2. Numbers
3. Modular addition
4. Shift ciphers
5. Remainders
6. Modular multiplication
7. Multiplicative inverses
8. Affine ciphers
9. The Euclidean algorithm
10. The extended Euclidean algorithm
11. RSA encryption
12. Prime numbers
13. Fermat's and Euler's Little Theorems

Labs There 8 lab assignments, which implement the things we develop in the classroom and explore some additional topics. All labwork uses Mathematica, and you are encouraged to search online and in documentation for ways to solve the problems. However, no additional software is allowed (no python, perl, etc.).

1. Cracking codes
2. Modular arithmetic
3. Frequency analysis
4. Kid Krypto
5. Base-26
6. Recursive functions
7. MyPowerMod
8. Putting RSA Together

Final textbook. At the end of the course (on **December 19**), students will turn in a 'textbook' consisting of their solutions to all problems from in-class worksheets. On the following dates, students will submit writeups of all worksheets (1) not submitted previously and (2) completed by the Wednesday prior to the due date:

September 21 October 5 October 26 November 16

Worksheets will be graded on correctness and clarity of exposition. Students are encouraged to type up their solutions in LaTeX for easier editing, but neat handwritten copies will also be accepted.

Each of the above blocks will count 5% toward the final textbook grade. The final project, complete solutions to all worksheets that incorporate previous comments, counts the remaining 80% and is due in class on **December 19**.

Legalities and resources. Hopefully, everyone in the class will have a good time and learn a lot. The policies below exist to encourage these two goals.

Participation and attendance. The participation grade will include attendance, effort, and collegiality. Both contributing to the team and helping others contribute are essential to the course.

In particular, coming to class is extremely important in this course for both the student and their team.

Serial Absenteeism Clause. A student is allowed at most three unexcused absences from class. The instructor will decide what is an acceptable absence on a case-by-case basis, and all absences due to illness require a note from University Health Service. For every unexcused absence beyond the third, the student's final grade will be reduced by one letter grade. For example, a student with four unexcused absences and a final grade of A will receive a B, and a student with a final grade of A and five unexcused absences will receive a C.

Groupwork vs. cheating. Groupwork is critical to the format of the class, and students are encouraged to work in groups on all homework. That said, all submitted work must be the student's own.

Any copying (especially verbatim) is unacceptable, and will result in a zero for the entire assignment. A second instance of cheating on homework will result in automatic failure of the course. Late homework will not be accepted, except in grave emergencies, and will count zero.

Conducive environment. A pleasant and accommodating environment for all students is critical for learning. In particular, the instructor is happy to provide individualized support during both reguarly scheduled and additional office hours; while the university provides support services for a variety of ongoing conditions and emergencies.

Any violations to the above standard are taken very seriously by the university. In particular, any cases of discrimination, harassment, or violence involving students are investigated by the Dean of Students and can lead to expulsion from the university and/or criminal charges.

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

- College of Science Adivisng: `https://cos.gmu.edu/uaa/advising/`
- Department of Mathematics Major Information: `http://math.gmu.edu/undergrad-student-resources.php`
- Department of Mathematics Advising and Contacts: `http://math.gmu.edu/contacts.php`
- Disability Services: `https://ds.gmu.edu/`
- Counseling and Psychology Services `https://caps.gmu.edu/`