Math 259: Cryptography
Spring 2019

The course website is `https://www.uvm.edu/~cvincen1/math259.html`.

Instructor Information: Professor Christelle Vincent, office 407 in Henry Marcus Lord House (16 Colchester Avenue).

For content (i.e. mathematical) questions, please post your question to Coursewire at `https://campuswire.com/c/GA18BDC44`. For personal matters, please reach me by email at christelle.vincent@uvm.edu.

Course Description and Goals: In Math 259 we will explore together the cutting-edge cryptography currently presented to NIST as part of its PQCrypto challenge. The class is aimed at students with little or no knowledge of abstract algebra, number theory or computer science.

Office Hours: I will have three hours of office hours each week, they are:

- Monday 12-1pm
- Wednesday 3-4:15pm
- Friday 2-3pm

Textbook: We have two recommended textbooks, Rubinstein-Salzedo's *Cryptography* and Trappe and Washington's *Cryptography and Coding Theory*. You should not need to purchase either, although they are great and if you have the money and the inclination you should! Relevant sections will be scanned and posted on **Blackboard**. Parts of other books and papers will be suggested as reading and also posted on Blackboard.

Attendance: You are expected to attend every lecture. If for whatever reason you cannot attend lecture, you are responsible for asking a classmate to tell you what you have missed. You can always send a friend to turn in your homework in class or to my mailbox.

ROTC, military, athletics: If you are a student-athlete or if you are in ROTC or have active military duty and you believe you might need accommodations due to commitments related to these activities, please submit in writing to me by the end of the second full week of classes your planned schedule of athletic competition or your planned schedule of military duties for the semester. For all homework and quizzes, you will be expected to turn in your work on time, or in advance, as necessary, except in very special circumstances.

If you are a student-athlete, the department of Vermont Catamount Athletics has various resources to help you manage your academic load. Do not hesitate to avail yourself of these resources.

Religious accommodations: Students have the right to practice the religion of their choice. If you believe you might need accommodations to take part in religious celebrations, please submit in writing to me by the end of the second full week of classes your religious holiday schedule for the semester. Together we will work on arranging a way to make up any work you might miss. For all homework and quizzes, you will be expected to turn in your work on time, or in advance, as necessary, except in very special circumstances.

SAS: In keeping with University policy, any student with a documented disability interested in utilizing accommodations should contact SAS, the office of Student Accessibility Services (previously ACCESS). Once you have this letter, I will be available to meet with you privately to discuss the accommodations you plan to use in this course.

Grading: Your grade for this class will be based on your performance in the following activities, weighted as follows:

Quizzes: 35%
Homework: 35%
Final Exam: 30%

All of your work will be graded on correctness as well as legibility and clarity. I reserve the right to assign a score of zero to any problem or assignment that is unreasonably difficult to understand or read.

Graduate credit: You may take this class for graduate credit if you are a graduate student or enrolled in the Accelerated Masters Program. If you would like to avail yourself of this option, please let me know today, or by email before Monday January 28. If you do then you will be required to solve the extra problems for graduate credit on the homework, quizzes, and final exam.

Homework: At the end of every chunk of material, and sometimes in the middle, there will be problems assigned as written homework. The homework will be graded and returned to you.

Homework will be due on the announced due date by the end of the class period. You must turn in your homework either to me in class or drop it off in my mailbox. I do not guarantee that I will find, or grade, homework that is turned in anywhere else. If you are sick or otherwise cannot make it to class, there is a hard cut-off to the time you may turn in homework: I leave UVM at 4:30pm every day and any homework that I do not have by then will not be graded.

The homework will be substantial and require thought. Breaking cryptography is hard! For this reason **do not leave your homework to the last minute**.

Your homework *must* be stapled, and have your full name.

For the homework you may use any computer help you need for computations. I recommend using Sage or Python. There will be help to learn how to use Sage, and you should have received an email invitation to Cocalc if you do not want to install Sage on your own computer.

Quizzes: At the end of every chunk of material there will be a substantial in-class quiz, lasting about 30 minutes. The quiz will apply ideas explored on the homework as well as quiz you on the basic facts we have learned.

The current plan is to have approximately five quizzes. There will not be any any make-up quizzes *under any circumstances.* However, if you must miss a quiz for a valid reason you will be excused from the quiz.

For the quizzes you may use a simple calculator, although you should not need one.

Exams: There will be a university-scheduled final exam. The problems on the exams will be similar to the problems on the quizzes. The final exam will be cumulative but probably not cover the whole semester. Plenty of information will be given closer to the day, depending on how things go.

The final exam is on May 6, from 1:30pm to 4:15pm, in Votey 254.

If you have a conflict with our final exam in this class, you must inform me in writing at least one week before the last day of classes.

If an emergency occurs and you need to miss the exam, you must notify me in writing within 24 hours of the exam. Please include the reason and documentation.

Extra credit: There will be an opportunity to earn extra credit by being active on our Campuswire site. So go ahead and ask and answer questions!

Statement on diversity: Mathematics can be learned and enjoyed by everyone, regardless of gender, age, race, sexual orientation, or other personal characteristics. As a group we will work to create a space where we all feel welcomed and encouraged, and any actions or speech that detract from this atmosphere will not be tolerated.

In particular, we will be mindful of encouraging others to let us know if they do not already know something and do everything to support them in their learning. We will not say that things are "trivial." We will offer corrections gently and with the intention of helping the other, as opposed to making ourselves feel good.