Advanced Topics in Undergraduate Mathematics: Cryptography
Math 480 A; Spring 2017

Lecture: MWF 3:30 - 4:20pm, More Hall (MOR) 221
Instructor: Prof. Bianca Viray
Office: Padelford C-525
e-mail: bviray+480@uw.edu (Include `[Math 480]` in the subject of all emails)
Course Website: http://www.math.washington.edu/∼bviray/Crypto_Spring2017.html
Office Hours: Monday 2:00–2:50pm, Friday 9:30–10:20am, or by appt. in PDL C-525
Text:
An Introduction to Mathematical Cryptography by J. Hoffstein, J. Pipher, and J. Silverman. This book is available for download through SpringerLink. You can also order a softbound MyCopy through the SpringerLink website for $25.

Classroom expectations: I expect that you will come to class on time and prepared to learn, that you will treat me and your classmates with respect, and that you will practice high standards of *academic and professional honesty and integrity as per the student code of conduct*. Conversely, you can expect that I will come to class prepared, start and end class on time, treat all of you with respect, and do my best to help you succeed in this class. More generally, I expect our behavior to be guided by the following:

Let the teacher teach and the students learn.

Grading: Your grade will consist of:

Homework	20%
Exam	25%
Project proposal	10%
Project progress report	10%
Final project	25%
Self-assessment and group assessment	
Progress report	5%
Final project	5%

Homework: Homework assignments will be collected at the *beginning* of class the day it is due. The homework will be posted on the course website at least a week ahead of time, with the exception of the first week. You may discuss the homework with your classmates. In fact, I encourage you to do so! However, the assignment **must** be written up on your own, and for each problem, you must list the names of everyone with whom you worked.

Homework assignments will be worth 25 points each. 2 of the assigned problems will be graded; the possible scores on each are 0,1,5, 9, or 10. The remaining 5 points will be allocated based on the completeness of the remaining problems.

Project: Detailed information about the project will be provided in a separate document.

Exams: Calculators, other electronic devices (e.g. cell phones, laptops, etc.), notes, and books will **not** be allowed during exams. Your exam will be **Wednesday, May 17** in class.

Make-Ups: Extensions and extra submissions on homework will not be given under any circumstances. In the case of observance of religious holidays or participation in university sponsored activities, such as class field trips or athletics, arrangements must be made at

least one week in advance for exams. You will be required to provide documentation for your absence.

If you miss the exam due to unavoidable, compelling, and well-documented circumstances (e.g., illness, transportation emergency), your exam may be replaced by an oral examination. **Contact Prof. Viray immediately if one of these circumstances arises.**

Resources for Students with Disabilities:

The University of Washington is committed to providing access, equal opportunity and reasonable accommodation in its services, programs, activities, education and employment for individuals with disabilities. To request disability accommodation contact the Disability Resources for Students at least ten days in advance at: 206-543-8924/V, 206-543-8925/TTY, 206-685-8379 (FAX), or uwdrs@uw.edu.

Tips for success

- **Practice, practice, practice:** Learning mathematics is in many ways similar to learning a foreign language or sports: the way to learn and improve is by **doing**! This means solving more problems than you are assigned, working on many different types of problems, explaining what you did to your classmates, and challenging your classmates to explain the reasoning behind every step.
- **Do the homework assignment without looking at the textbook or your notes:** You should use the homework assignments to check whether you have really digested the material presented in class. However, if you constantly reference your notes or books when solving the problem, you are really only checking if you can follow the material when it's being presented. This is different from internalizing the material.

  I suggest first attempting the assignment with your book and notes *closed*. You will probably struggle at first. When you have made as much progress as you think you can, then put away the homework, reread your notes and book and/or come to office hours, and work through some other examples. Then you should go back to the assignment (again with your notes and book closed!) and try again, possibly repeating the process multiple times.

  This will probably take longer, but you will have gained a much better understanding of the material, and it will be much better preparation for the exams.
- **Start your homework assignment early:** This is a consequence of the last tip, but is important so bears repeating.
- **Come to office hours:** If you are confused in class or on a problem, come to office hours and ask! Even if you aren't confused, come to office hours – we can talk about something else or you can help clarify things for another student. Nothing solidifies your understanding as well as explaining it to someone else does.