MATH 499W: Cryptology Seminar in Mathematics  
Spring 2015

Class Meetings:  
TTh 2:30 – 4:00 PM, Ford 201

Professor:  
Erin McNicholas  
email: emenicho@willamette.edu  
Office: Ford Hall, Room 211  
Phone: 503-370-6590

Class Website:  
Course information, assignments, due dates, and policies are all available on the course website under WISE

Office Hours:  
<table>
<thead>
<tr>
<th>Mondays</th>
<th>Tuesdays</th>
<th>Wednesdays</th>
<th>Thursdays</th>
<th>Fridays</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:00 – 3:30</td>
<td>9:15 – 10:45</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ford 211</td>
<td>Bistro</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If these times do not work for you, please let me know; I’m also available by appointment.

Class Text: The text for this course has not yet been written. You will be given a scaffold of a text that will serve as the basis for the course. The scaffold consists almost entirely of definitions, incomplete examples, and statements of theorems. Almost none of the usual details and proofs are supplied. Your challenge is to discover those missing proofs, filling in all the missing details and explanations.

“In mathematics is not a careful march down a well-cleared highway, but a journey into a strange wilderness, where the explorers often get lost. Rigor should be a signal to the historian that the maps have been made, and the real explorers have gone elsewhere.”  
-W.S. Anglin

“In the broad light of day mathematicians check their equations and their proofs, leaving no stone unturned in their search for rigour. But at night, under the full moon, they dream, they float among the stars and wonder at the miracle of the heavens. They are inspired.”  
- Michael Atiyah

Course Objectives:  
As the culmination of your mathematical studies, this course will make use of your previous mathematical studies while giving you the opportunity to experience the thrill of mathematical discovery. In this course, you will:

• develop skills necessary for independent work, including greater mathematical maturity
• learn the theory of Cryptology
• improve your mathematical writing and public speaking skills

Class Structure: Modern mathematics research is highly collaborative. Mathematicians work months to years tackling challenging problems and extending the boundaries of what is known. Making progress on a problem or theorem is tremendously rewarding, in no small part because that progress is so hard won, and comes so infrequently. This course is designed to give you the full experience of mathematics research - the excitement, fear, frustration, and elation. In the interest of time, and to ensure that your experience includes the thrill of discovery and not just the frustration of confusion,
we will be collaborating on math that is new (to you). We only achieve the desired effect if you are discovering this math for yourself, i.e. NO OUTSIDE RESOURCES!

As a class, we will collaboratively author a Cryptology text. Homework will consist of portions of the text that need to be filled in (definitions, proofs, examples, etc.). Class time will be spent presenting these missing portions of the text, and critiquing the results of your peers. For each section of the text, two class recorders will be assigned. These recorders are responsible for facilitating discussion and recording the presented proofs/solutions. These presented proofs and solutions will be entered into the text scaffold by the recorders. Once a section has been completed by the recorders, the class will proofread their work and a third recorder will be assigned to make any changes necessary. Grades will be based in part on the overall quality of the final text, and the quality of class discussions.

While the text of this course is a collaborative effort, there are many areas in which you will be individually responsible for your grade. While I encourage you to work together on the homework, your final \LaTeX{ed} write-ups must be your own. There will be three individual quizzes given throughout the semester. Quiz problems will be taken directly from the text. Each student will independently research a topic and write up their findings for inclusion in the course text. Findings will be presented to the Math Department. These presentations should be well researched and prepared and be approximately 25 minutes in length. Presentations will be created with the \LaTeX{ program Beamer.

---

Grading: Your course grade will be determined as follows:
(a) Class text (overall quality of the text and class discussions): 20%
(b) Individual homework grades (turned in assignments and problems presented in-class): 25%
(c) Class participation (involvement in class discussions and attendance at Math colloquia): 5%
(d) Recorder duties (facilitating class discussion, correctly tex-ing presented results, ensuring code COMPILES and is completed on time): 5%
(e) Individual quiz grades: 20%
(f) Individual projects and presentations: 25%

---

Cell Phone/Screen Policy: Unless specifically stated for class use, no laptops, iPads, or other devices which take your eyes off your fellow classmates and the class discussion are allowed. Electronic devices such as cell phones, pagers, iPods, etc. must be turned off during class meetings. If your cell phone goes off, or it is clear that you are using one of these devices during class, you will be responsible for bringing beverages for the entire class at the next class meeting. During class you should be focused on the speaker and ready to ask questions and provide feedback.

Academic Integrity: As is stated in the Willamette University CLA catalog

“Plagiarism and cheating are offenses against the integrity of the courses in which they occur and against the college community as a whole. Plagiarism and cheating involve intellectual dishonesty, deception and fraud, which inhibit the honest exchange of ideas. In accordance with Willamette University Standards of Conduct and the Willamette Ethic, students are entitled to notice of what constitutes plagiarism and cheating, and the right to appeal penalties. Plagiarism and cheating may be grounds for dismissal from the college.”

Because of the goals and collaborative nature of this course, it is important that everyone understand what is an acceptable resource and what is not. To that end, each student will sign an honor pledge. Additional information about the University’s Plagiarism and Cheating Policy can be found at the website http://www.willamette.edu/cla/catalog/resources/policies/