MATH 134:
Cryptography
SU 2016 Syllabus

- **Disclaimer:** The information presented in this course syllabus is subject to change (with notification) at the discretion of the Instructor.
- **Course Instructor** Dr. Elizabeth Jurisich ejurisic@ucsc.edu, office hours TBA
- **Lecture Meetings:** MW 09:00AM-12:30PM Soc Sci 2 165 06/20/16 - 07/22/16
- **Course Materials:** *An Introduction to Mathematical Cryptography* by Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, 1st edition (2008), ISBN 978-0387779935. **Note:** a complete PDF version of this textbook is available through the library.
- **Course LMS:** Course information, assignments, and announcements will be available at the course LMS (eCommons). Students are responsible for checking the site regularly for any information relevant to the class.
- **Prerequisites:** course 100; course 110 recommended as preparation.
- **Student Learning Outcomes:**
  - Identify and describe several historical and contemporary cryptosystems.
  - Identify aspects of private-key and public-key cryptography that ensure the secure communication of information in the presence of a third party, and identify how cryptosystems are vulnerable to attack.
  - Demonstrate proficiency in several mathematical topics related to cryptography, including groups, finite fields, and number theory.
- **Attendance:** Attendance to all lectures is expected, and students are responsible for materials covered in classes that are missed. The instructor will make every attempt to be helpful to students who miss class meetings due to illness or other unavoidable circumstances. Students who are absent excessively from class may be dropped from the class.
- **Homework:** Homework assignments will be given to students on a regular basis. Homework may be discussed in class.
- **In Class Work:** Periodically, group work will be given in class. The content of the worksheets will be based on lectures, reading assignments, and homework problems. No make-up in class work will be given.
- **Midterm Exams:** There will be two (midterm) exams administered throughout the quarter. If a student misses an exam **without** a valid excuse, the grade will be zero. A portion of the exams may be given as open book, and/or as take home.
- **Mini-Reports:** Students will complete two (2) brief reports on a topic related to cryptography. The instructor will provide a list of potential topics early in the semester, and the student is allowed to propose their own topic. For each Mini-Report, students will write a brief (1-2 page) report/handout to distribute to the rest of the class and give a 5-10 minute presentation to the rest of class on their topic at the end of a scheduled lecture period. One report will count as the "final report" and be given at the end of the class.
- **Grading Policy:**

Final Grade

Homework/In class work	25%
Two Exams (25% each)	50%
Mini-Reports (10%, 15%)	25%

- **Grading Scale:**

A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
93-100	90-92	87-89	83-86	80-82	77-79	73-76	70-72	67-69	63-66	60-62	0-59

- **Extra Credit: There will be no opportunities for extra credit in this course. Your grade will be calculated using the structure given above.**
- **Accommodations:** UC Santa Cruz is committed to creating an academic environment that supports its diverse student body. If you are a student with a disability who requires accommodations to achieve equal access in this course, please submit your Accommodation Authorization Letter from the Disability Resource Center (DRC) to me privately during my office hours or by appointment, preferably within the first week of the Summer quarter. At this time, I would also like us to discuss ways we can ensure your full participation in the course. I encourage all students who may benefit from learning more about DRC services to contact DRC by phone at 831-459-2089 or by email at drc@ucsc.edu.