Math 299
Introduction to Cryptology
Spring 2018

Instructor: Christian Millichap **Office:** Taylor 209

Contact: email: cmillich@linfield.edu, office phone: x2428

Time and Location: MTWF 2:55-3:45 PM in Taylor 201.

Office Hours: M 8:45-9:45 and 1:45-2:45, T 8:45-9:45, W 11-1, Th 8:45-9:45, F 11-1.

Text: Bauer, *Secret History: The Story of Cryptology*, Taylor & Francis Group, 2013.

Additional Resources: Cryptologia (online journal available through the Linfield library website)

Course Goals and Objectives

- Develop the mathematical skills necessary to utilize both classical and modern ciphers.
- Strengthen problem solving skills by practicing cryptanalysis.
- Use coherent arguments to analyze the strengths and weaknesses of a cipher.
- Develop independent research and learning skills.
- Examine cryptology in the context of the current PLACE theme: The Digital Citizen.

Topics Covered

For this class, students will learn how to encrypt (scramble a message using a cipher), decrypt (unscramble a message sent using a cipher), and break a number of classical and modern ciphers.

Ciphers: The following ciphers will be covered in this class: the Caesar shift cipher, monoalphabetic substitution ciphers, the Vigenère cipher, the re-used one-time pad, transposition ciphers, the Playfair cipher, the affine cipher, the Hill Cipher, DES, Diffie-Hellman Key Exchange, and RSA.

Mathematics: Along the way, we will learn a variety of mathematics necessary for the analysis and implementation of these ciphers. This includes fundamental ideas from probability & statistics, combinatorics, number theory, and linear algebra.

Connections to PLACE: This interdisciplinary cryptology course will tie in with the PLACE theme, The Digital Citizen, by addressing issues related to freedom of speech and privacy rights at the end of the semester. Relevant topics include could include the Snowden files, Pretty Good Privacy, NSA encryption policies, and Apple's conflict with the FBI over iPhone privacy policies in 2016.

Grades

Grades will be counted as follows:

Homework:	20%
Course Engagement:	20%
Kryptos:	10%
Mastery Quizzes:	15%
Project:	25%
Collaborative Final:	10%

Letter grades correspond to the following percentages:

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

However, I reserve the right to curve the scale.

Homework: Each week, students will be given a homework assignment on Wednesday that will be due the following Wednesday in class. A large portion of homework questions will involve using quantitative reasoning skills (encryption, decryption, breaking ciphers, mathematics problems related to cryptology, etc.). Students will also have some homework assignments that are reflective in nature (critiquing the strengths and weaknesses of a cipher, writing reflections on ethical issues related to cryptology, etc.). Late homework usually won't be accepted; exceptions will possibly be made for students that have a legitimate excuse that is communicated in a timely fashion.

Course Engagement: Course Engagement points are earned by regularly attending class, actively participating in class activities, and engaging both the "mathematics culture" and PLACE culture at Linfield. In class, students should expect an active learning environment where group work and class discussions are frequently used rather than lecture. In addition, students will be **expected to participant in at least 3 events that go beyond the classroom - 1 math event, 1 PLACE event, and 1 additional event (either related to math or PLACE)**. Math events include Taylor Series events, Math Club events, and participation in a mathematics conference; for a list of math events, go to: https://www.linfield.edu/math/math-events.html. For the schedule of PLACE events, check the website: http://www.linfield.edu/place/place-upcoming-events.html. Other events could possibly fulfill this requirement, though they must be first approved. After a student attends an event, she/he must write a (approximately) one page reflection on how the event relates to our class, the PLACE theme, and/or mathematics.

Kryptos: All students must participate in Kryptos, an online cryptanalysis competition open to undergraduate students across the country. This event takes place from April 5-9, 2018, during which students work in teams of at most three to break a series of ciphers and submit their solutions online. Students will be graded based on participating in this event and writing a reflection on their experiences. For more details see the website: https://www.cwu.edu/math/kryptos.

Mastery Quizzes: There will be two mastery quizzes in this class, each worth 7.5% of your final grade. The first mastery quiz will focus on encryption and decryption of classical ciphers. The second mastery quiz will focus on mathematical skills necessary for modern encryption. For these quizzes, students work individually but have multiple opportunities to demonstrate mastery of concepts essential to succeed in cryptology. The following rules apply to both mastery quizzes:

- Students have up to 4 attempts (1 in class and 3 during office hours) to demonstrate mastery of a topic. Attempts made during office hours MUST occur within the two weeks after receiving your in class quiz back.
- Each student must achieve at least an 80% on a mastery topic (not necessarily on the first try) in order TO PASS a mastery quiz. Failure to achieve above an 80% on a mastery quiz will result in a 0% grade for that quiz.
- If a student receives a 95% or higher on her/his first attempt, then that will be rounded up to 100%.

Project: Each student must develop an interdisciplinary project related to cryptology and share their project with the Linfield community. All students will be required to present their findings at the Linfield Symposium Day on May 18, 2018. A project rubric including suggestions for topics will be given out before spring break. Students can work individually or in groups of at most three for this project.

Collaborative Final: For the final, students will work in groups to practice their encryption, decryption, and cryptanalysis skills in small teams. This final will feature most of the ciphers analyzed over the course of the semester. Students will be graded based on how well they work efficiently and effectively with their teammates, and their individual abilities to implement a variety of problem solving techniques in the context of cryptology. Expect a non-traditional setup for this final that will be both fun and competitive!

Our final exam will occur on Monday, May 21st, starting at 3:30pm. **There will be no alternative final exam times**.

Advising Information

The prerequisite for this course is MATH 170 Calculus I. In particular, students will need to be very comfortable with functions and performing abstract problem solving. This course counts toward both the major and minor in mathematics.

Academic Integrity

Our class adheres to the college policy on academic honesty, as published in the Linfield College Course Catalog. Violating this policy has immediate consequences, ranging from a zero on the given assignment to immeidate failure of the course, depending on the specifics of the violation. Please consult the Course Catalog and your Student Handbook and Planner for more details on Linfield's policy.

Disability Statement

Students with disabilities are protected by the Americans with Disabilities Act and Section 504 of the Rehabilitation Act. If you are a student with a disability and feel you may require academic accommodations please contact Learning Support Services (LSS), as early as possible to request accommodation for your disability. The timeliness of your request will allow LSS to promptly arrange the details of your support. LSS is located in Melrose Hall 020 (503-883-2562). We also encourage students to communicate with faculty about their accommodations.