

## Math 440: Special Topics in Algebra: Cryptology Winter 2015

Professor: Dr. Cheryl Beaver

Office: MNB 123

Web Page: [www.wou.edu/~beaverc](http://www.wou.edu/~beaverc)

Phone: (503) 838-8404

Email: [beaverc@wou.edu](mailto:beaverc@wou.edu)

OFFICE HOURS & SCHEDULE					
Time	Monday	Tuesday	Wednesday	Thursday	Friday
10					Office
11	Office	Meeting			
12	MTH 440		MTH 440		MTH 440
1			Office		Meeting
2	Office				
3	MTH 403W	Meeting	MTH 403W		
4		Meeting			

**Course Prerequisite:** Instructor Approval

### Required Course Materials

**Text:** *Secret History: The Story of Cryptology*, Craig P. Bauer, 2013

**Learning Outcomes:** This course is designed as an introduction to modern cryptology. A student passing this course should understand the following:

- Classical Encryption and Cryptanalysis Techniques
- Elementary Number theory as it applies to Cryptology including the following topics
  - modular arithmetic, prime numbers, factoring, discrete logarithm
- Symmetric Cryptographic Methods including:
  - Stream Ciphers
  - Block Ciphers
- Asymmetric Cryptographic Methods including:
  - Key Exchange
  - Encryption Schemes
  - Digital Signature Schemes

**Attendance:** Daily attendance is required for your success in this course. If you miss class it is your responsibility to ask a classmate for notes on the material that you have missed. Attendance is REQUIRED during your classmate's presentations. Failure to attend a presentation will result in a deduction of points from your final project grade.

**Homework:** The complexity of cryptographic algorithms is often not understood until one personally works out problems. Homework and reading the text will be very important to your understanding of the concepts. Homework will be assigned regularly to be turned in for direct grading.

**Late homework:** Homework is due by 4:30pm on its due date. **Late homework will not be accepted.** Your lowest homework score will be dropped.

**Exams:** There will be one midterm exam and a take home final exam. If you must miss the exam due to a documented emergency or a documented university sanctioned absence from class please inform me ASAP. Cell phones may not be used as calculators during an exam and must be turned off. The final exam will be due no later than our final exam time of Friday, March 20<sup>th</sup> at noon.

**Course Project:** Cryptology has many applications in modern society and has served important roles historically. You will work alone or in groups of 2-3 to investigate a particular topic. Your group will create a poster and give a 20-40-minute presentation (depending on group size) on your topic. On the last day of class we will have a poster session to present your work. You will also be asked to present your poster at the academic showcase in May. Attendance at presentations is required. Detailed information will be provided.

**Grading:** Your grade will be based on the following:

Homework	35%
Course Project (including milestones, presentation, poster, and attendance)	25%
Midterm Exam	20%
Final Exam	20%

The standard grading scale will apply.

### **Appropriate Classroom Behavior**

You are ultimately responsible for your own attendance and performance. Disruptive classroom behavior of any kind, such as talking during lecture or consistently coming to class late etc., is not appropriate. Proscribed Conduct for all students is described in the University Catalog. In particular for this course any student found cheating on an exam or copying from another student's exam paper will receive a zero score on that exam.

### **Learning Disabilities**

If you have a disability for which you are or may be requesting an accommodation, you are encouraged to contact both your instructor and the Office of Disability Services, APSC 405, or at 503-838-8250, as early as possible in the term. Students needing medical or mental health care can access the Student Health and Counseling Center by calling 503-838-8313, emailing at [health@wou.edu](mailto:health@wou.edu), or by walking in to schedule an appointment.

**Veterans and active military personnel** with special circumstances are welcome and encouraged to communicate these, in advance if possible, to the instructor.

### **Cell Phone Policy<sup>1</sup>**

Silence your cell phones and put them away – please no texting during class!

### **Incomplete Policy**

An Incomplete can only be considered for a student who is passing a class and has a documented emergency that prevents them from completing a very small portion of the course (e.g. the final exam) after Friday of week seven of the course, which is the last day to withdraw from the course with a “W” grade.

---

<sup>1</sup> If you are in an emergency situation in which you need to have your cell phone on quiet; please speak to me about it before class.