

Math 440: Advanced Topics in Algebra: Cryptology
Spring 2008
MWF 2-2:50 pm, AA 202

Professor: Dr. Cheryl Beaver
Office: AA 201
Web Page: www.wou.edu/~beaverc

Phone: (503) 838-8404
Email: beaverc@wou.edu

C. Beaver's OFFICE HOURS & SCHEDULE

Time	Monday	Tuesday	Wednesday	Thursday	Friday
8 - 9				213	
9 - 10	213		213	Lab	213
10 - 11	213		213	213	213
11 - 12	366		366	Lab	366
12 - 1				Not usually on campus	
1 - 2		<i>Office</i>	<i>Office</i>		<i>Office</i>
2 - 3	440		440		440
3 - 4	<i>Office</i>				

COURSE PREREQUISITE

Instructor Approval

REQUIRED COURSE MATERIALS

Text: *Invitation to Cryptology*, Thomas H. Barr, 2002

Calculator: A TI-84 calculator is highly recommended for this course. Please see me if you are purchasing a new calculator.

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
- Hash Functions
- Computational Complexity
- 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 an appropriate deduction of points from the attendance portion of 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. Any homework not turned in by this time is considered late. An assignment may be turned in by the end of one class day late for 75% credit or 2 class days late for 50% credit. Homework turned in later than 2 class days late will **NOT** receive credit. Consistently turning in late homework will have a very detrimental effect on your grade.

Course Project & Presentation: Cryptology has many applications in modern society and has served important roles historically. You will be required to write a paper and give a presentation on a cryptographic topic. You will give a 25 minute Power Point (or Beamer) presentation to the class sometime during the last two weeks of class and your final paper will be due on Monday of Finals Week. Detailed instructions and a schedule of milestones for your project will be provided.

Exams: There will be two midterm exams. The midterms are *tentatively* scheduled for 4/30 and 5/28. If you must miss an 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.

Grading: Your grade will be based on the following:

Homework	35%
Course Project (including milestones, presentation, paper, and attendance of presentations)	25%
2 Midterm Exams	20% each

Standard Grading Scale for this Course:

% Range	Grade	% Range	Grade	% Range	Grade
93 – 100	A	80 – 82	B-	60 – 69	D
90 – 92	A-	77 – 79	C+	Below 60	F
87 – 89	B+	73 – 76	C		
83 – 86	B	70 – 72	C-		

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 documented learning disability, please talk to me during the first few days of class, I will be more than happy to accommodate you in any way that I can. If you have a documented disability which requires any academic accommodations, you must go to the Office of Disability Services (ODS) for appropriate coordination of your accommodations. You can drop by APSC 405 or contact ODS at (503) 838-8250 to schedule an appointment.

Incomplete Policy

An Incomplete can only be granted for a student who is passing a class and has a documented emergency that prevents them from completing a small component of the course.