

FIRST-YEAR SEMINAR COURSE PROPOSAL
UNIVERSITY OF MARY WASHINGTON

Use this form to submit **FSEM 100 topics** courses for review **or** any **other existing course** that you wish to have designated to meet the first-year seminar requirement.

COURSE NUMBER:	FSEM 100E4		
COURSE TITLE:	CRYPTOLOGY		
SUBMITTED BY:	Keith Mellinger & Randall Helmstutler	DATE:	10/28/14
<i>This course proposal has the department's approval. (Put a check in the box to the right.)</i>			X

COURSE DESCRIPTION. In the space below, provide a one- to two-sentence description of this class. The description will be entered in Banner and will also be used in other publications about the first-year seminar program (such as the “Eagle Essentials” booklet).

We explore the mathematical foundations of cryptology, the study of how to transmit secrets. Different types of ciphers will be applied to text, sounds, and images, in an attempt to understand the challenges that emerge in this most important area of modern research.

RATIONALE. Include short statement addressing how this course meets the FSEM's basic components and new student learning outcomes (see FSEM call above), and why this course should be approved to meet the FSEM General Education requirement.

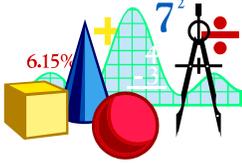
Cryptology was modified recently to meet the demands of the QEP. Regarding research, students employ the research process within mathematics as they investigate the various ciphers. Through a visit with the library staff, they learn information retrieval techniques they then utilize as they work on their term paper. Several short writing assignments allow the instructor to provide necessary feedback early on, and the lengthier term paper is coupled with an editing and revision workshop facilitated by the Writing Center. The students are expected to participate in regular class discussions as well as small group projects that lead to presentations. The instructor spends class time discussing proper use of PowerPoint, and provides written feedback to the groups after their presentations. All of these activities are complemented by the on-line learning modules which are assigned throughout the semester. Together, the course provides all of the necessary tools to develop the skills needed for success at UMW.

SYLLABUS. *Attach a course syllabus.*

SUBMIT this form and attached syllabus **electronically as one document** to Dave Stahlman (wdstahlm@umw.edu). All submissions **must** be in electronic form.

FSEM 100 – Cryptology

Spring 2014 – TR 8:00-9:15 – 119 Trinkle Hall



"There was a footpath leading across fields to New Southgate, and I used to go there alone to watch the sunset and to contemplate suicide. I did not, however, commit suicide, because I wished to know more of mathematics."
-B. Russell

Professor

Dr. Keith E. Mellinger

 kmelling@umw.edu

Office

Trinkle 129

 (540) 654-1333

Text

Cryptology by Albrecht Beutelspacher
Published by the Mathematical Association of America

Other good reference books:

Mathematical Ciphers: from Caesar to RSA by Anne L Young

Cryptological Mathematics by Robert Edward Lewand

Office Hours

TR after class until 11:00, or by appointment

I have many other times available, so just ask if you need to see me.

The Course

This course is a seminar focusing on the art of hiding information using mathematical techniques. We will explore the foundations of modern cryptology, from the ciphers used by Julius Caesar, to the modern RSA encryption algorithm that is used today. Along the way, we will develop a variety of mathematical ideas, primarily through collaborative learning methods, including basic number theory, modular arithmetic, matrix multiplication, iteration and orbit structures, and the basic statistical tools used in crypt-analysis (the art of breaking codes). The mathematical content should be accessible to anybody with solid high school algebra skills and, more importantly, an interest in and curiosity for real mathematics. Students will be expected to participate through regular group projects and class presentations, and will be writing formal papers. Participation is absolutely essential to your success in this course.

Grades

Your grade this semester will be based on several components:

Quizzes	2 @ 5%	10%
Group Projects	4 @ 10%	40%
On-Line Modules	5 @ 4%	20%
Contribution		10%
Paper #1		10%
Paper #2		10%

Class Engagement

As is indicated on the grading scale, *contribution* is of utmost importance in this course. There is a fine line between *participating* and *contributing* to course direction, discussion, and content. This is no time to sit back and enjoy the show. Ask questions when you have them, answer questions when I pose them, and engage in the material. We are here to learn all we can about this very exciting and contemporary field.

Writing Assignments

You will have two formal (and some less-formal) writing assignments during the semester. The first one is a critique where you will compare and contrast three of the algorithms that we learn early in the semester. All students will be expected to obtain at least one peer-review before submitting their final paper and details on this will be provided in class. Grades will be based on the quality of your paper along with the quality of the feedback you provide in your peer review.

The second paper has a somewhat open topic and will be written in two stages. The first draft will be due in early November. Students will participate in a peer editing and revision workshop facilitated by the UMW Writing Center. After obtaining this feedback, the final paper will be due at the end of the semester. More on the writing projects will be distributed separately.

Speaking Assignments

Of equal importance in the class will be the preparation and delivery of various speaking assignments. Certainly, your oral participation in class will contribute toward your contribution grade. In addition, two of the group projects will require some small presentation to the class, and your final paper will require a short individual presentation. Prior to the first presentation, the class will engage in a several discussions on how to prepare a good presentation.

Group Projects

One major part of this course will involve the actual making and breaking of ciphers. This process will take place as a collaborative exercise. More details will be provided as the topics are introduced. With the Vigenère cipher, for instance, your group will create a stream of ciphertext, and another group will be challenged with breaking your cipher. I expect to have software available on the mathematics computer lab in Trinkle B9 that can be used for these purposes (you can also use your own personal computer)

On-Line Learning Modules

UMW has a series of on-line learning modules that you will be expected to complete outside of class. Content of the modules is fundamental to your success at UMW and your scores on the module quizzes will make up a small portion of your final grade in the course. More details will be discussed in class.

Student Learning Objectives

This course satisfies the First-Year Seminar requirement of the general education curriculum at UMW. By the end of the semester, students will

- Utilize a variety of research techniques to retrieve information efficiently, evaluate retrieved information, and synthesize information effectively to support their messages or arguments;
- Improve development and organization of written arguments;
- Demonstrate the ability to edit and revise in the writing process;
- Apply the basic theories and principles of oral communication;
- Communicate effectively in a variety of settings, including public speaking and group discussion.

Tentative schedule

Online learning modules are indicated in blue and should be completed in the week they appear.

	Topics	notes/assignments	Readings
Week 1	Fundamental problems, Ceasar ciphers, shift ciphers, affine ciphers, ITCC visit	Communication Apprehension , Grammar	Chapter 1
Week 2	Vigenère Cipher, software implementation, cryptanalysis	Quiz #1 – basic ciphers	
Week 3	Group projects and presentations on Vigenère	Group Project #1 – breaking Vigenère	Chapter 2
Week 4	Substitution ciphers applied to images	The Writing Process , Checking for CRAAP Library visit	
Week 5	Theory – perfect security, one-time pads	Group Project #2 – Sounds and images Draft of Paper #1 due Using PowerPoint	Chapter 3
Week 6	Group projects and presentations on sounds and images	Paper #1 due Deconstructing citations	
Week 7	Authentication, key exchange, and the famous NP-hard problems that make it happen	Group Project #3 – Key Exchange & Hill Cipher	Chapter 4
Fall Break			
Week 8	Group projects and presentations on key exchange		
Week 9	The mathematics behind RSA – Euler phi function	Draft of Paper #2 due editing workshop	
Week 10	The mathematics behind RSA – Euclidean algorithm, gcds	Quiz #2 – mathematics behind RSA	Chapter 5
Week 11	The RSA public-key algorithm		
Week 12	RSA group activity		Chapter 6
Week 13	Group projects and presentations	Group Project #4 – check digits, attacks, threshold schemes	
Week 14	Final project presentations	Final paper due	

The fine print:

Missed classes: If you miss a lecture, it is entirely your responsibility to obtain any missed notes, handouts, announcements, etc. In the event that you miss a quiz, a make-up will be given only if the absence was cleared with me beforehand. In some cases, a medical excuse will be granted if proper documentation is provided. Appointments for missed quiz must be made by the first class after the excused period.

The *Office of Disability Services* has been designated by the university as the primary office to guide, counsel, and assist students with disabilities. If you receive services through the Office of Disability Services and require accommodations for this class, make an appointment with me as soon as possible to discuss your approved accommodation needs. Bring your accommodation letter with you to the appointment. I will hold any information you share with me in strictest confidence.

Remember that Group Projects require a group. Failure to contribute to a group project will be reflected in your contribution grade.