MATH 498: Cryptological Mathematics
Dr. Boersma [Cryptmaster]
Spring 2009

Goals: This course will study the mathematical underpinnings of a variety of ciphers. For each cipher studied, we will study techniques of enciphering, deciphering, and cryptanalysis. Some of the ciphers we will study this quarter will include: Cesar, substitution, polyalphabetic, affine, the Hill Cipher, Vigenere Cipher, Enigma, and RSA.

Office: Bouillon 107E, phone: 963-1395, email boersmas@cwu.edu. Office hours will be announced in class shortly. You may of course drop by anytime. If I'm not busy I'll be glad to talk with you.

URL: Reading assignments and other course information can be found at:

http : www.cwu.edu/ boersmas/cryptology

Required Materials

1. **Text:***Invitation to Cryptology*, by Thomas H. Barr
2. A desire to encrypt, decrypt, and break ciphers.

Your Grade: Your final grade in this course will depend numerous reading assignments (20%), class participation/attendance/problems (20%), and a neatly organized *Code Book* (60%).

Reading Assignments There will be reading assignments nearly every day. There are several reasons for these assignments. First, there is no reason for me to spend an enormous amount of time copying the book to the board so you can copy the board back into your notes. Second, I would like to use as much class time as possible going over the more complicated aspects of code-making and codebreaking; the easier stuff you can read on your own. Third, in order to have fruitful class discussions, it is important that you come to class prepared. Reading assignments are meant to be completed **before 11:00 a.m.** on the following class day. To successfully complete a reading assignment, first read the assigned portion of our textbook or handout and then send me an email with your responses to the following:

1. Using two or three sentences, briefly summarize what you just read.
2. Was there anything in the reading that you did not fully understand?
3. Were there any examples or statements that you found particularly interesting.

Please place "math498" (all lowercase) in your "Subject" line or your reading assignment may not be properly recorded.

Attendance etc.

I will assume that everyone attends every class meeting. If you happen to miss a day, be advised that you are still responsible for any assignments that were made in class. If we worked on problems out of the textbook in class, you will need to make those up to keep from having your attendance/class participation grade lowered.

Code Book

The majority of your grade will be based on the creation of a *Code Book*. This book will contain examples of enciphering, deciphering, and cryptanalysis of four or five ciphers which we study. This book will be collected periodically during the course and specific instructions on its content will be given in class.