MATH 337: Cryptological Mathematics
Dr. Boersma
Spring 2016

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: Caesar, substitution, polyalphabetic, affine, the Hill Cipher, Vigenere Cipher, Enigma, and RSA. As time permits we will look at some more modern enciphering systems such as DES, AES, and Elliptic Curve Cryptography.

Office: Bouillon 108E, phone: 963-1395, email stuart.boersma@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.

Canvas: We will make extensive use of the course management system Canvas. You can logon using your standard CWU Novell credentials. A link to Canvas appears off of the CWU homepage under the "MyCWU" wildcat symbol.

http : //www.cwu.edu/

Required Materials

1. **Text:***Secret History: The Story of Cryptology*, by Craig P. Bauer
2. A desire to encrypt, decrypt, and break ciphers.

Your Grade: Your final grade in this course will depend numerous reading assignments, class participation/attendance, and your ability to encipher, decipher, and break a variety of ciphers. Final grades

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

Alice-Bob-Eve Assignments Cryptology is all about enciphering, deciphering, and cryptanalysis (the breaking of codes). Most every week you will need to complete an ABE assignment which involves all three of these processes. **Each ABE assignment is worth 6 points.** See the ABE assignments on Canvas for a more detailed description.

Reading Assignments There will be reading assignments nearly every day. Sometimes these reading assignments will allow you to come to class better prepared to discuss

the more complicated aspects of code-making and codebreaking. Sometimes these reading assignments will allow you to learn about certain encryption systems that we won't have time to discuss in class. Reading assignments will be made in class and will appear in Canvas. Reading assignments are meant to be completed **before noon** on the following class day. To successfully complete a reading assignment, first read the assigned portion of our textbook and then answer the accompanying posted questions. These responses are submitted through Canvas as well and are **worth 2 points** per assignment.

Attendance etc. It is important to attend class everyday and participate in the discussions. Sometimes you will need to work in small groups during class which makes missing class difficult for yourself as well as your other group members. I will assume that everyone attends every class meeting. For every absence I record, you will suffer a **1 point deduction**. Also, if you happen to miss a day, be advised that you are still responsible for any assignments that were made in class.

Extra Credit There are a handful of extra credit challenges that you may complete if you need a few extra points. These challenges are posted on Canvas. If you solve one of them, please type up a detailed description of how you solved it and hand it in to me. **Each challenge is worth 2 points.** You may only submit one extra credit challenge solution per week.

Students who have special needs or disabilities that may affect their ability to access information or material presented in this course are encouraged to contact me or the Center for Disability Services.