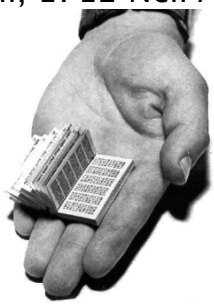
Course Instructors: Chris Brew, Stephen Boxwell
Course Meeting Time: TR 11:30-1:18
Classroom: Page Hall 10 Instructor Mailbox: 225 Oxley Hall
Instructor Phone: (614) 292 6833 mail: brew.2/boxwell.1
Instructor Office: 202/204 Oxley Hall, 1712 Neil Ave





Enigma Cipher cylinder One-time pad Scytale Cipher Disk

Course Description:

This course has two main aims: it introduces some of the old and new technology associated with codes and code-breaking and it discusses ways in which codes have made, are making and might make a difference to peoples' lives. The course number is Linguistics 484 and the material is intended to be suitable for well-motivated juniors and seniors from any major. If you are a freshman or a sophomore, please talk to the instructor(s) about your background and reasons for taking the course. Several freshmen and sophomores have taken the course and done well, but we would like to be sure that you are ready before you commit to the course.

Students in Linguistics 484 will have an opportunity to:

- Acquire a thorough knowledge of the fundamental terminology, concepts and techniques of cryptology.
- Learn some of the history of codes, and their importance, both from the point of view of the code user and the code breaker.
- Develop an understanding of what a cryptanalyst looks for when trying to break a code.
- Gain experience in problem solving, in synthesizing ideas, and in writing reports.

Required texts:

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.
Simon Singh
ISBN-10: 0385495323 **ISBN-13:** 978-0385495325

Army Field Manual 34-40-2
Available for download in PDF and postscript at http://www.umich.edu/~umich/fm-34-40-2/

Students with Disabilities:

Students who need an accommodation based on the impact of a disability should contact us to arrange an appointment as soon as possible to discuss the course format, to anticipate needs, and to explore potential accommodations. I rely on ODS (the Office of Disability Services) for assistance in verifying the need for accommodations and developing accommodation strategies. Students who have not previously contacted the Office for Disability Services are encouraged to do so (292-3307; http://www.ods.ohio-state.edu). Even if you have a legitimate disability, I can make no accommodations except through ODS.

Assessment:

There will be regular short code-breaking assignments. To succeed on these you need to attend class, and make a serious attempt to solve the codes. There will also be CARMEN quizzes on the readings from The Code Book. There will be a mid-term exam testing technical material and a final project that will involve a 5-page write up of a piece of independent work. There will be small extra credit opportunities.

Component	Score
Weekly assignments	400 points (8 at 50 points each)
Quizzes	70 points (7 at 10 point each)
Simulation	80 points
Mid-term	150 points
Final project	250 points
Class participation	50 points
Total	1000 points

Grade	Point Range
A	930-1000
A-	900-929
B+	870-899
B	830-869

B-	800-829
C+	770-799
C	730-769
C-	700-729
D+	670-699
D	600-669
E	0-599

Final Project: 250 Points (25% of your grade)

The final project is group-based and requires you to do four things:

1.Design a cipher system that strikes a good compromise between usability and security.

2.Prove to us that you can use it.

3.Make a serious attempt to break the system created by one of the other groups.

4.As a group, write a well-organized and clear report on the things that you did.

Since this project requires that you work in a group and it is 25% of your grade for the course, it is imperative that you tell us if you anticipate problems working with others over the course of the quarter. Students who anticipate such problems should see us before the end of the third week of classes (January 21, 2011).

NO ACCOMMODATIONS FOR THE FINAL PROJECT WILL BE MADE UNLESS ARRANGEMENTS ARE MADE BY JANUARY 21, 2011.

Weekly Homework Assignments: 400 Points (48% of your grade)

Each Thursday we will assign a short homework assignment from the material that we are covering that week. Each assignment is worth 50 points and should take no more than 1-2 hours to complete. Homework is to be turned in no later than the beginning of class on the following Thursday and must be turned in to us either in hard copy or uploaded to the dropbox on CARMEN. **NO HOMEWORK WILL BE ACCEPTED BY EMAIL.** Email is unreliable, and it is difficult for you to know whether we received your email or not (sometimes messages get put into a SPAM folder, sometimes they have mistakes in the address, etc.). The dropbox on CARMEN allows you to verify that your file was uploaded and it creates an automatic time stamp to show what day and time you uploaded your submission.

For the most part these assignments will be enciphered messages that you will need to decipher. While it would be wonderful if every one of you solved every single cipher, it is neither realistic nor expected. What is expected is that you will spend time trying sensible approaches to solve each cipher. The ideal homework solution will have the completely deciphered message with a description of the method used to break the

cipher. The minimum requirement to receive full credit is to demonstrate that the cipher has been broken. For some ciphers this will be simply providing a keyword, for others it means providing the first line of the deciphered text. Although this will get you full credit, be advised that you may be called on in class to describe the method you used to break the cipher. Failure to demonstrate your ability to solve the cipher will result in your being reported to the Committee on Academic Misconduct. Nearly full credit can be obtained (even if the cipher is not broken) by providing an account of the approaches that you tried when attempting to break the cipher (provided that your approaches are sensible).

Feel free to work on the homework assignments together, but each student must write up his/her answers separately unless specifically instructed otherwise. It is university policy that no student should turn in someone else's work as his/her own. Any suspected violations of this policy must of necessity be reported to the Committee on Academic Misconduct; for more information please see the section entitled "Academic Misconduct".

Midterm: 150 Points (15% of your grade)

There will be a midterm exam over the technical material of the course. I will provide you with a study guide. The midterm is currently scheduled for Thursday February 3, 2011. If you anticipate a problem taking the midterm I must be notified by the end of the third week of classes (January 21).

NO ACCOMMODATIONS FOR THE MIDTERM WILL BE MADE UNLESS ARRANGEMENTS ARE MADE BY JANUARY 21, 2011.

Simulation: 80 Points (8% of your grade)

Fairly soon into the quarter we will split into groups that we will stay in until the end of the quarter. One thing that we will do is a simulation of what it would be like to be a cryptologist in a time of war. Further instructions on this simulation will be provided later in the course.

Weekly Quizzes: 70 Points (7% of your grade)

Each week we will have a short quiz over the material contained in the assigned readings from The Code Book. There will be 7 quizzes, each of which is worth 10 points. The quizzes will be on CARMEN and are timed. You will have 20 minutes to answer questions about the chapter. They are all open book, but are very difficult if you have not looked at the material. These quizzes will be fairly simple if you have read the chapter. These must be completed by the stated end time. There are very few good excuses for not taking a CARMEN quiz. "I forgot" is not acceptable, neither is "I lost track of time" or "I didn't know when it was due". Although there are specific dates and times when the quizzes must be completed by, all quizzes will be made available at the start of the quarter. Students may feel free to complete the quizzes as quickly as they see fit.

NO MAKE-UP QUIZZES WILL BE GIVEN UNLESS I AM NOTIFIED IN ADVANCE.

Class Participation: 50 Points (5% of your grade)

We want to avoid doing this class as a boring 108 minute lecture twice a week. We try hard to make class fun and interesting, and we expect that you will try to make class interesting as well. That means being here to participate in class discussions and group work. To gain participation points for a given class session you must (i) come to class and (ii) participate. Participation includes making comments, asking questions, answering questions, participating in group work, etc. You can lose participation points for a given day by doing things that common sense tells you are not appropriate in a classroom setting like disrupting class, disrespecting other students, reading the newspaper or magazines, doing homework for other classes, surfing the internet on your laptop, sending text messages, playing games on your phone, etc.

We understand that sometimes situations arise that prevent you from being in class for one reason or another. Penalties to your participation grade will not be assessed if you provide us with a legitimate excuse for missing class. If you know that you will be missing class on a given day, let us know **BEFORE** that class session. If you notify us ahead of time we will make sure that you have access to the homework assignment for that session. If you are not in class and you did not notify us beforehand, then **YOU** are responsible for getting class notes and/or the homework assignment. We will not repeat entire lectures during office hours for students who missed class with an unexcused absence. If you will be missing class on the day that homework is due, please submit it early either in our mailbox or in the CARMEN dropbox. If you miss class without letting us know in advance and without some documentation of the emergency that not only explains why you missed class, but also why you were unable to notify us in advance, then the homework due that day will be subject to late penalties if it even is accepted at all.

Academic Misconduct:

Academic misconduct is taken very seriously. We are required to report any suspected violations of Section 3335-23-04 of the Code of Student Conduct (http://studentaffairs.osu.edu/resource_csc.asp) to the Committee on Academic Misconduct (http://oaa.osu.edu/coam/home.html). Please take the time to read the Code of Student Conduct carefully. All OSU students are assumed to be familiar with it. Ignorance of the Code of Student Conduct will not exempt you from guilt. The most common form of misconduct is plagiarism. Remember that you must provide clear citations for any ideas or materials that are not your own. This includes material that you find online. The university provides guidelines for online research at http://liblearn.osu.edu/tutor/. Academic misconduct also includes working together without permission and/or copying answers from other students on homework or exams. Do your own work!

Additional Notes:

Please do not hesitate to contact us with any questions or concerns about this course. We are happy to meet with you for any reason during our office hours or by appointment if office ours are not convenient. If you are having trouble, please come and see us. Let us say that again: PLEASE PLEASE PLEASE PLEASE come and see us if you are having trouble. Only you know if you are really trying and if you really understand the material.

If we don't know about the problem then we can't help. Please come and talk to us if you are having trouble.

Social Media:

Use of certain social media, while not required, can be very helpful for understanding the course material and core concepts of the course. The following steps are recommended for maximum results:

1) Subscribe to get Twitter updates from me: http://www.twitter.com/cbrew

2) Subscribe to DJ Hovermale's YouTube channel: http://www.youtube.com/user/djhovermale (DJ has taught this class a lot, and produced great materials that you will certainly find useful)

Secrets:

This course is full of secrets. Secret homeworks, secret messages, secret meetings, secret competitions, secret organizations, etc. It is entirely possible to complete this course and not discover a single secret, and it is virtually impossible to discover them all. Enjoy yourself as you look for them.

Tentative Schedule:

The following schedule is tentative and is subject to change. AFM stands for the Army Field Manual and TCB stands for The Code Book. Readings from The Code Book are the subject of weekly quizzes. Readings from the Army field manual will be important for understanding the core concepts of the course, which is crucial to passing the mid-term and final exams. This information will also be posted on Carmen.

Week	Day	Date	Topic	Chapter	Due
1	T	Jan 4	Syllabus – Intro		Personal Info sheets
	R	Jan 6	Steganography Monoalphabetic Ciphers	AFM 1-2	Monoalphabetic HW 1
2	T	Jan 11	Monoalphabetic Ciphers (cont.)	TCB 1	Quiz 1 – TCB 1
3	R	Jan 13	Polyalphabetic Ciphers – Vigenère	AFM 3-4	Monoalphabetic HW 2
	T	Jan 18	Polyalphabetic Ciphers (cont.)	TCB 2	Quiz 2 – TCB2
4	R	Jan 20	Decoding Ancient Languages	TCB 5/AFM 5	Vigenère Cipher HW 3
	T	Jan 25	Decoding Ancient Languages	AFM 6, 7	Syllabary HW 4 pt 1 Quiz 3 – TCB 5

5	R	Jan 27	Polyalphabetic Ciphers – Playfair	TCB 3	Syllabary HW 4 pt 2 Quiz 4 – TCB 3
			Polyalphabetic Ciphers (cont.)		
6	T	Feb 1	Mid-term Review		Playfair Cipher HW 5
	R	Feb 3	Mid-term		
7	T	Feb 8	Simulation Instruction/ Transposition Ciphers	AFM 11-13	
	R	Feb 10	Transposition Ciphers	TCB4	Quiz 5 – TCB 4
8	T	Feb 15	Final Project Instruction/Prep Solving Unknown Ciphers		Transposition Cipher HW 6
	R	Feb 17			
9	T	Feb 22	Enigma: The Intelligence		Playfair Cipher 2 HW 7
	R	Feb 24	Public Key Cryptography	TCB 6, pt 1	Quiz 6 – TCB 6, pt 1
10	T	Mar 1	Enigma: The Technology		Mystery Cipher HW 8
	R	Mar 3		TCB 6, pt 2	Quiz 7 – TCB 6, pt 2
11	T	Mar 8	Final Project Presentations		
	R	Mar 10	Final Project Presentations		
Finals	M	Mar 15	Make-up Day (if needed)		Final Project Write-up