Linguistics 3801: Codes and Code Breaking, Autumn 2020

Online Times: Mon/Wed 3:55-5:15 pm (EST)

Instructors

Byung-Doh Oh oh.531@osu.edu Office hours on Zoom

Office hours: My office hours will be held on Zoom. You are welcome to come to either my hours or another instructor's. **See the Carmen page "Office Hours and Directions"** for the times and locations of all instructors' hours. If none of the listed hours work for you, contact me to request a meeting at another time (please suggest options).

My Boss

If you have concerns about me as an instructor or about this course that you cannot resolve with me directly, please feel free to contact:

Dr. Hope Dawson dawson.165@osu.edu Oxley Hall 114/on Zoom

Course Materials

1. Simon Singh, The Code Book ("TCB"). The editions of 1999 or 2000 are preferred. Due to the pandemic, we will accommodate students who are only able to obtain the 2001, 2002, or young adult edition, but be aware that they are missing some historical information. You may obtain the book via the University bookstore (which can deliver it to you), but if you are not on campus, the book is easily ordered online.
2. Army Field Manual 34-40-2 ("AFM"). http://www.umich.edu/~umich/fm-34-40-2/
3. A quad ruled (graph paper, square ruled) notebook, needed asap

Course-at-a-Glance

Reading: While not onerous, there will be some required instructional reading.
Quizzes: 6%, To keep your reading on track. The lowest quiz grade gets dropped.
SuperQuiz: 10%, Covers modern cryptography topics.
Homework: 27%, Mostly involve breaking encrypted messages. Practice makes competent agents!
Midterm Clearance Exam: 20%, on Carmen. You will have 48 hours to complete this exam. Clearance is required for project ops.
Group Projects: 33%, Above your current security clearance. 4 weeks, **10/26-11/23**.
Participation: 4%, occasional "minute papers" on Carmen, asking you to comment on a lecture immediately after it is finished.
Optional special assignments: Some opportunities for extra credit will be available, mostly as part of the projects. Reading this syllabus carefully may also be worth your while!

Updated September 7, 2020 (changes to "Course Schedule" HW due dates)
Updated September 27, 2020 (changes to "Course Schedule" quiz "release" dates)
Last updated September 28, 2020 (HW6 due date: 10/14→10/19)

Course Description

This course covers the foundations of cryptology and cryptanalysis, the making and breaking of codes and ciphers. These concepts were often discovered in the midst of the fires of history where secure, secret communication literally meant the difference between life and death. Principles of information security are now widely employed in computer science, linguistics, mathematics, archeology, and of course, modern IT security, among other applications.

The course is Linguistics 3801, and the material is intended for well-motivated juniors and seniors from any major. If you are a freshman or sophomore and wish to take this course, please talk to your instructor about your background and motivation.

Course Objectives

The objectives of this course are to:

- Become well-versed in the basic principles of secure communication (by studying cryptosystems and information theory)
- Learn to critically question the structures of information systems (by learning basic principles of cryptanalysis and security)
- Understand where cryptosystems leak information, and how leaks can be exploited or mitigated (by attacking and using ciphersystems)
- Be familiar with the background of the historical trends in cryptography and security (through study of cryptography from classical times to the present)

Students taking this course will have the opportunity to:

- Gain experience in synthesizing ideas, solving problems, coordinating in teams, and writing.
- Write codes, analyze codes, and feel the sweet, sweet satisfaction of breaking them.
- Gain practical security skills.
- According to our reviews, take the best college course of your life and miss it when it's over.

How this course works

Mode of instruction: This course will be presented fully online and has **scheduled online lectures at 3:55-5:15 pm (EST) Mon/Wed every week**. You can access these meetings through the **Zoom tab on Carmen**. We understand that you may need to miss some lectures--- if you are going to miss a lecture, please contact the instructor in advance if possible. **Lectures will be recorded** for later review, and **slides** will be available for each lecture, but these are not a complete substitute for attendance. As a general rule, **we expect you to attend every lecture**, since there will be many hands-on activities for you to try out during class time.

Credit and work expectations: This is a 3-credit-hour course. According to Ohio State policy, students should expect around 3 hours per week of time spent on direct instruction (instructor content and Carmen activities, for example) in addition to 6 hours of homework (reading and assignment preparation, for example).

Group work: During the project, we expect you to meet regularly with your group members (groups should meet online).

Attendance and participation: In addition to lectures, you are expected to schedule time to work with your group on the projects during the announced dates.

Course technology

Carmen support: For help with your password, university email, Carmen, or any other technology issues, questions, or requests, contact the Ohio State IT Service Desk. Standard support hours are available at ocio.osu.edu/help/hours, and support for urgent issues is available 24/7.

- **Self-Service and Chat support:** ocio.osu.edu/help
- **Phone:** 614-688-4357(HELP)
- **Email:** servicedesk@osu.edu
- **TDD:** 614-688-8743

Basic technical skills for online courses:

- Basic computer and web-browsing skills
- Navigating Carmen: for questions about specific functionality, see the Canvas Student Guide
- CarmenZoom virtual meetings

Required equipment:

- Computer: current Linux (any), Mac (OS X) or PC (Windows 7+) with high-speed internet connection
- Webcam: built-in or external webcam, fully installed and tested
- Microphone: built-in laptop or tablet mic or external microphone
- Other: a mobile device (smartphone or tablet) or landline to use for BuckeyePass authentication

Carmen access: You will need to use BuckeyePass multi-factor authentication to access your courses in Carmen. To ensure that you are able to connect to Carmen at all times, it is recommended that you take the following steps:

- Register multiple devices in case something happens to your primary device. Visit the BuckeyePass - Adding a Device help article for step-by-step instructions.
- Request passcodes to keep as a backup authentication option. When you see the Duo login screen on your computer, click **Enter a Passcode** and then click the **Text me new codes** button that appears. This will text you ten passcodes good for 365 days that can each be used once.
- Download the Duo Mobile application to all of your registered devices for the ability to generate one-time codes in the event that you lose cell, data, or Wi-Fi service.

If none of these options will meet the needs of your situation, you can contact the IT Service Desk at 614-688-4357 (HELP) and IT support staff will work out a solution with you.

Disability Accommodation

The university strives to make all learning experiences as accessible as possible. In light of the current pandemic, students seeking to request COVID-related accommodations may do so through the university's request process, managed by Student Life Disability Services. If you anticipate or experience academic barriers based on your disability (including mental health, chronic, or tempoɾaɾy medical conditions), please let me know immediately so that we can privately discuss options. To establish reasonable accommodations, I may request that you register with Student Life Disability Services. After registration, make arrangements with me as soon ɑs possible to discuss your accommodations so that they may be implemented in a timely fashion. SLDS contact information: slds@osu.edu; 614-292-3307; slds.osu.edu; 098 Baker Hall, 113 W. 12th Avenue.

Health and safety requirements:

All students, faculty and staff are required to comply with and stay up to date on all university safety and health guidance (https://safeandhealthy.osu.edu), which includes following university mask policies and maintaining a safe physical distance at all times. Non-compliance will be warned first and disciplinary actions will be taken for repeated offenses.

A reminder that other helpful information can be found on the Safe and Healthy Teaching website: https://safeandhealthy.osu.edu/information/faculty-and-staff/teaching.

Other Help Resources

- **Your Instructor:** I make the rules and run the class, so ɨf you come to me early with problems, chances are I can help with them. Life happens. I know, because I have a life, too.
- The **Student Advocacy Center** is available to help with many problems you might have navigating OSU, including but not limited to dealing with bureaucratic issues, academic issues, health issues (including mental health and hospitalization), and financial issues. advocacy.osu.edu, 614-292-1111, advocacy@osu.edu, 001 Drackett Tower.
- The **OSU advising office** maintains a page for **advising appointments**, the latest **pandemic policies** and **tutoring help** at: http://advising.osu.edu/welcome.shtml
- As a student you may experience a range of issues that can cause barriers to learning, such as strained relationships, increased aɲxiety, alcohol/drug problems, feeling down, difficulty concentrating and/or lack of motivation. These mental health concerns or stressful events may lead to diminished academic performance or reduce a student's ability to participate in daily activities. The Ohio State University offers services to assist you with

addressing these and other concerns you may be experiencing. If you or someone you know are suffering from any of the aforementioned conditions, you can learn more about the broad range of confidential mental health services available on campus via the **Office of Student Life's Counseling and Consultation Service (CCS)** by visiting ccs.osu.edu or calling 614-292-5766. CCS is located on the 4th Floor of the Younkin Success Center and 10th Floor of Lincoln Tower. You can reach an on call counselor when CCS is closed at 614-292-5766 and 24 hour emergency help is also available through the 24/7 National Suicide Prevention Hotline at 1-800-273-TALK or at suicidepreventionlifeline.org.

- Title IX makes it clear that violence and harassment based on sex and gender are Civil Rights offenses subject to the same kinds of accountability and the same kinds of support applied to offenses against other protected categories (e.g., race). If you or someone you know has been sexually harassed or assaulted, you may find the appropriate resources at http://titleix.osu.edu or by contacting the **Interim Ohio State Title IX Coordinator, Molly Peirano**, at titleix@osu.edu

Academic Misconduct

Don't cheat. Don't even seem to cheat, because I am required to report that, because university policy. The reporting paperwork is gnarly and makes everyone sad. Don't make everyone sad.

It is the responsibility of the Committee on Academic Misconduct to investigate and establish procedures for the investigation of all reported cases of student academic misconduct. The term "academic misconduct" includes all forms of student academic misconduct wherever committed; illustrated by, but not limited to, cases of plagiarism and dishonest practices in connection with examinations. Instructors shall report all instances of alleged academic misconduct to the committee (Faculty Rule 3335-5-487). For additional information, see the Code of Student Conduct at http://studentlife.osu.edu/csc/.

Among other forms of misconduct, you are strictly forbidden from soliciting help or answers from internet forums, social media, and other such venues. You are further forbidden from leaking any questions or answers from this course in any format to the public, online or otherwise. If my materials are compromised, I have to make all new ones, which is extraordinarily time-consuming. Time-consumed instructors are not happy instructors. You would not like not-happy instructors.

Finally, regarding the use of electronic or other automated tools: The only computerized cryptanalytical tools that may be used for assignments in this class are those that I link to from Carmen, and those that you make yourself (from scratch, not using an AES or PGP library, for example). For any tool you make yourself, you must submit well-commented code accompanying any assignment that involved use of that tool.

If you have any questions about the above policy or what constitutes academic misconduct in this course, please contact me.

Other sources of information on academic misconduct (integrity) to which you can refer include:

- The Committee on Academic Misconduct web pages (COAM Home)

- *Ten Suggestions for Preserving Academic Integrity* (*Ten Suggestions*)
- *Eight Cardinal Rules of Academic Integrity* (www.northwestern.edu/uacc/8cards.htm)

Assessment and Grading

The way you are assessed in this course is straightforward. Everyone starts at the beginning of the course with 0 points. Your goal is to earn 10,000 points by the end of the semester by completing assignments. Every homework, quiz, project, and other assignment will have a point value associated with it, and you can earn up to that many points towards your total through that assignment. The following table lists the core assignments and their relative point values. These represent the simplest and most straightforward way of earning 10,000 points. To convert a given point value into a percentage/letter grade, simply divide the point value by 100. Thus someone, having earned 7,865 points, is 78.65% of the way to 100% course completion, and would, if they stopped there, earn a C+.

In addition to the core assignments, there are many other ways in which you can demonstrate your skills and mastery of the course content. These are worth a substantial number of points and can compensate for gaps in your performance on the midterm or some of the other core assignments. Some of these opportunities are available early in the course, but most of them will appear after the midterm. Some will be obvious, while others are only available to the observant. Keep your eyes peeled.

Assignment	Value		A	9300 - 10000+ pts
Homework	2700 pts	(27%)	A-	9000 - 9299
Quizzes	600 pts	(6%)	B+	8700 - 8999
Exam	2000 pts	(20%)	B	8300 - 8699
Competitive Analysis	300 pts	(3%)	B-	8000 - 8299
Final Project (Part 1)	1500 pts	(15%)	C+	7700 - 7999
Final Project (Part 2)	1500 pts	(15%)	C	7300 - 7699
Minute papers	400 pts	(4%)	C-	7000 - 7200
Superquiz	1000 pts	(10%)	D+	6700 – 6999
			D	6000 – 6699
			E	0 - 5999

Homework

Richard Feynman allegedly said, "You do not know anything until you have practiced." That is certainly true in cryptology. Therefore you will have regular homework assignments to practice what you learned in lecture.

Homework is to be uploaded to Carmen by 11:59 pm (EST) on the due date (see the schedule below). Homework is only accepted via Carmen. Email is unreliable, and it is difficult for you to verify whether I received your email or not (sometimes messages get put into a spam folder, sometimes they have mistakes in the address, etc). Carmen verifies uploads with time stamps. Each assignment on Carmen will have a text entry field in which to submit your report.

I can be flexible with deadlines, and I am cognizant of the fact that the COVID-19 pandemic is creating challenges for all of us that may make it difficult for you to turn your work in on time. If you need extra time to complete an assignment, please let me know before the due date.

For the most part homework assignments will be enciphered messages that you will need to crack. 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. To receive full credit (450 points) you should demonstrate that the cipher has been broken, by providing:

(1) the names of any people you worked with (or a note indicating that you worked alone),
(2) the cipher key (50 points),
(3) the plaintext (it does not need to be reformatted, 50 points),
(4) Answers to a series of questions about steps in the cryptanalysis (250 points).
(5) a thoughtful and insightful answer to the critical thinking question (100 points)

Note that you can get up to 350 points for answering the questions that pertain to the usual methods of decipherment and the critical thinking section even if you do not manage to break the cipher yourself.

Feel free (in fact, you are encouraged) to work on the homework assignments together, but you must write up your answers separately unless specifically instructed otherwise. That means cracking the encryption and recovering the key together, then leaving and writing your report by yourself. Include a note stating who you worked with. It is university policy that no student should turn in someone else's work as their 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 "Academic Misconduct."

Quizzes

There will be 7 short quizzes over the material contained in the assigned readings. They are all open book, but are very difficult if you have not looked at the material. If you have read the chapter, you will know where to find the answers.

Quizzes will be available on Carmen during the week in which each is due. You will have 1 attempt to take the quiz. Once you begin the quiz, you will have 10 minutes to complete it. Late/missed quizzes score a zero.

I am sure some of you will have ordinary emergencies such as sickness, car trouble, etc. Rather than mess around with make-up quizzes, I will just drop your lowest quiz score. If you must miss an unusual number of quizzes, please contact me to make other arrangements.

Minute papers

Some lectures will be followed by “minute paper” assignments, which must be submitted **on Carmen** in the three hours following the end of the lecture. These are meant to help you keep up with the lessons and help me identify any parts of the lessons that are unclear. Each minute paper should include at least the following:

1. One question, either about something you didn’t understand or something you want to learn more about.
2. One important thing you learned that week.

Security Clearance Exam

There will be a midterm "Security Clearance Exam" over the technical material of the course. Passing the exam will qualify you for project operations under the auspices of the Federal Agency for Kryptology and Encipherment (F.A.K.E.). The midterm will be available on Carmen for 48 hours; see the class schedule below for the exact date and time when the midterm will become available on Carmen. **If you anticipate a problem taking it as scheduled, you must notify me in writing during the first three weeks of the semester.**

Once you begin the exam, you will have 150 minutes to complete it; however, most students are expected to complete this examination in roughly 60 minutes. **You may not work with other students on the midterm or discuss it with them.**

Modern Cryptography "Superquiz"

There will be an extended Carmen quiz covering the material presented in lectures after the midterm. This quiz will be available during the 48 hours after the last day of class. **If you cannot take it as scheduled, contact your instructor ASAP.**

Once you begin the Superquiz, you will have 150 minutes to complete it; however, most students are expected to complete this quiz in roughly 60 minutes. **You may not work with other students on the Superquiz or discuss it with them.**

Final Project

The project is a team exercise in three parts: Applied competitive cryptanalysis, Scarlet Sentinel, and Gray Guardian. You will be cleared to learn the details after the midterm. For now, know that it will occur within the dates specified in the schedule, and that ***it will be work-intensive***. Plan accordingly. **If you anticipate a conflict with these dates you must notify me in writing during the first three weeks of the semester.**

Participation

I, the instructor, try hard to make class fun and interesting, and I expect that you will try to make class interesting as well. That means more than just logging in to Zoom to sit through a lecture. Participation includes making comments, asking questions, answering questions, contributing to group work, etc.

I understand that sometimes situations arise that keep you away from class, especially during the current global public health crisis. Do let me know if you need to miss class, since that will shape my impression of your participation.

If you will be missing class on a given day, you are still responsible for submitting homework on time via Carmen, studying the posted lessons, keeping up in the readings, and beginning any new homework assignment.

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 sinɡle secret, and it is virtually impossible to discover them all. Enjoy yourself as you look for them, and always examine things closely, as thəre may be more than meets the eye.

Course Schedule

The following schedule is tentative and is subject to change. Homework and quizzes are listed by *deadline*. They are due by 11:59 pm (EST) on the day listed. You can take the quiz anytime on that week, up until 11:59 pm (EST).

Readings are listed by recommended *start date*. Readings from The Code Book (TCB) will be **useful** for the very next class session, and **essential** for a quiz later on. The recommended start date gives you time to digest what you read and to clarify or solidify it in class. Digestion time is especially necessary in the second half of the semester, so form the habit during the first half.

Readings from the Army field manual (AFM) are to support your understanding of core techniques and to survey expanded applications. This is not quizzed, but it is **valuable for homework, the midterm exam, and the project.** AFM 6-7 are especially important because the Playfair cipher is one of the more difficult homework analyses, and TCB covers it only very briefly.

Week	Date	Due that day	Lecture	Start Reading
1	8/26 W		Intro to course, intro to ciphers	TCB 1
2	8/31 M		Monoalphabetic	AFM 1, 2
	9/2 W		Steganography and Kerckhoff's Principle	AFM 3, 4
3	9/7 M	**Labor Day**		
	9/9 W	HW 1: Shift	Monoalphabetic cont'd	TCB 2
4	9/14 M	Quiz 1: TCB 1 (Mary's) Answer available for 24 hours on 9/29	Polyalphabetic: Vigenere	
	9/16 W	HW 2: Monoalphabetic	Polyalphabetic cont'd	TCB **5, not 3!**
5	9/21 M	Quiz 2: TCB 2 (Chiffre) Answer available for 24 hours on 9/29	Writing systems: ABCሚቻ৭ঔআ ƥlvვ 表記法	AFM 5
	9/23 W	HW 3: Vigenere	Polygraphic: Playfair	**AFM 6, 7 on Playfair**
6	9/28 M	Quiz 3: TCB **5 (Lang)** Answer available for 24 hours on 9/29	Playfair cont'd	
	9/30 W	HW 4a: Strange Writing	Decoding ancient languages	
7	10/5 M	HW 4b: Strange Reading	Ancient languages cont'd	AFM 11- 13
	10/7 W		Transposition	TCB 3

8	10/12 M	HW 5: Playfair	Transposition cont'd	
	10/14 W	Quiz 4: TCB 3 (Mech) Answer available for 24 hours on 10/15	Cipher Signatures, Midterm Review	
9	10/19 M	**HW 6: Transposition due** **Security Clearance Exam (Midterm) opens 12:01am, Monday, 19 October; due 11:59pm Tuesday, 20 October; no lecture, you have plenty to do!**		
	10/21 W		Applied competitive cryptanalysis, Scarlet Sentinel Briefing	
Operation Scarlet Sentinel begins 12:01am, Monday, 26 October				
10	10/26 M		field op skills, Crypto Cell Primer	TCB 4
	10/28 W	RJ-16s due for ACC	Brand X cipher; op sec WWII to present	Briefing Materials
11	11/2 M		Modern symmetric ciphers; team time	
	11/4 W	Quiz 5: TCB 4 Answer available for 24 hours on 11/5	Gray Guardian briefing; counterintelligence; team time	
Scarlet Sentinel ends (and all cryptanalyses due) 11:59pm, Sunday, 8 November Operation Gray Guardian begins 12:01am, Monday, 9 November				
12	11/9 M		Computer security; team time	TCB 6a pp 243-67
	11/11 W	**Veterans Day**		
13	11/16 M		DHM, Public-key encryption; team time	
	11/18 W		Public-key encryption applications; team time	TCB 6b pp 268-92
14	11/23 M	Quiz 6: TCB 6a pp 243-67 Answer available for 24 hours on 11/24	Passwords, Off-the-Record; team time	Begin reviewing all slides after Midterm
Operation Gray Guardian ends 11:59pm, Monday, 23 November				
	11/25 W	Quiz 7: TCB 6b pp 268-92 Answer available for 24 hours on 11/26	Zero-knowledge proofs; team time	
15	11/30 M		Voting systems, Crypto-currency	
Operation Gray Guardian reports due 11:59pm, Tuesday, 1 December				
	12/2 W		Flex day, material TBD	
Modern Crypto Superquiz opens 12:01am Thursday, 3 December; due 11:59pm Friday, 4 December				