Term Information

Effective Term	Autumn 2020
Previous Value	*Summer 2012*

Course Change Information

What change is being proposed? (If more than one, what changes are being proposed?)

We have created an online section of the course.

What is the rationale for the proposed change(s)?

We would like students to have an option to learn the same content in the course in a virtual format.

What are the programmatic implications of the proposed change(s)?

(e.g. program requirements to be added or removed, changes to be made in available resources, effect on other programs that use the course)?

None.

Is approval of the requrest contingent upon the approval of other course or curricular program request? No

Is this a request to withdraw the course? No

General Information

Course Bulletin Listing/Subject Area	Linguistics
Fiscal Unit/Academic Org	Linguistics - D0566
College/Academic Group	Arts and Sciences
Level/Career	Undergraduate
Course Number/Catalog	3801
Course Title	Codes and Codebreaking
Transcript Abbreviation	Code Breaking
Course Description	Introduction to old and new technology associated with codes and code-breaking and the ways in which it has impacted people's lives.
Semester Credit Hours/Units	Fixed: 3

Offering Information

Length Of Course	14 Week, 12 Week, 8 Week, 7 Week, 6 Week, 4 Week
Flexibly Scheduled Course	Never
Does any section of this course have a distance education component?	Yes
Is any section of the course offered	100% at a distance
Previous Value	*No*
Grading Basis	Letter Grade
Repeatable	No
Course Components	Lecture
Grade Roster Component	Lecture
Credit Available by Exam	No
Admission Condition Course	No
Off Campus	Never
Campus of Offering	Columbus

Prerequisites and Exclusions

Prerequisites/Corequisites	
Exclusions	
Electronically Enforced	No

Cross-Listings

Cross-Listings

Subject/CIP Code

Subject/CIP Code	16.0102
Subsidy Level	Baccalaureate Course
Intended Rank	Freshman, Sophomore, Junior, Senior

Requirement/Elective Designation

The course is an elective (for this or other units) or is a service course for other units

Course Details

Course goals or learning objectives/outcomes

- 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)

Previous Value

Content Topic List

- Monoalphabetic ciphers
- Playfair cipher
- Enigma
- Public key cryptography
- Vigenere cipher

Sought Concurrence No

Attachments

- Linguistics 3801 Tech_Assurance.docx: Technology_Assurance

  (Other Supporting Documentation. Owner: McGory,Julia Tevis)

- 3801_AU_20_Syllabus.pdf: On-Line Syllabus

  (Syllabus. Owner: McGory,Julia Tevis)

- 3801_InPersonSyllabus.pdf: In-Person Syllabus

  (Syllabus. Owner: McGory,Julia Tevis)

Comments

Workflow Information

Status	User(s)	Date/Time	Step
Submitted	McGory,Julia Tevis	06/01/2020 04:27 PM	Submitted for Approval
Approved	McGory,Julia Tevis	06/01/2020 04:27 PM	Unit Approval
Approved	Heysel,Garett Robert	06/01/2020 10:53 PM	College Approval
Pending Approval	Jenkins,Mary Ellen Bigler Hanlin,Deborah Kay Oldroyd,Shelby Quinn Vankeerbergen,Bernadette Chantal	06/01/2020 10:53 PM	ASCCAO Approval

Linguistics 3801: Codes and Code Breaking, Autumn 2020

Classroom: On Zoom Times: Tues/Thurs 2:20-3:40 pm

Instructors

Micha Elsner elsner.14@osu.edu 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).

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 even if it's not physically open), 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, **10/22-11/17**.
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.

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 my 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 has **scheduled online lectures** at 2:20-3:30 Tues/Thurs every week. 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 (probably 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. 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 as 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.

Other Help Resources

- **Your Instructor:** I make the rules and run the class, so if 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
- You can get free, confidential, expert help with many personal and academic concerns from **Counseling and Consultation Services.** They also offer self-help resources online. ccs.osu.edu, 614-292-5766, sl-ccs@osu.edu, Younkin Success Center 4th Floor.
- Title IX prohibits discrimination on the basis of sex under any OSU program or activity. That includes assault, harassment, and limiting your enjoyment of opportunities or rights. You can find help, file grievances, and learn to help others via **OSU's Title IX Coordinator.** The Title IX office also has information about many other forms of discrimination. titleix.osu.edu, 614-247-5838, titleix@osu.edu, 21 East 11th Ave.

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			
Homework	2700 pts	(27%)	A	9300 - 10000+ pts
Quizzes	600 pts	(6%)	A-	9000 - 9299
Exam	2000 pts	(20%)	B+	8700 - 8999
Competitive Analysis	300 pts	(3%)	B	8300 - 8699
Final Project (Part 1)	1500 pts	(15%)	B-	8000 - 8299
Final Project (Part 2)	1500 pts	(15%)	C+	7700 - 7999
Minute papers	400 pts	(4%)	C	7300 - 7699
Superquiz	1000 pts	(10%)	C-	7000 - 7200
			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 11:59pm 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. Late homework is graded at 80% of normal value if received within the first week, 40% within the second week, zero after that. Do inform me if you have extenuating circumstances such as a health crisis.

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 250 points for answering the questions that pertain to the usual methods of decipherment 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 on the day 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.

Minute papers

Some lectures will be followed by "minute paper" assignments, which must be submitted **on Carmen** in the last 15 minutes of lecture and the 15 minutes following. These will ask you for one thing you learned in the lecture and one thing you're still not sure about. They are intended to encourage participation.

Security Clearance Exam

There will be a mid-term "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.). See the class schedule below for the exact date and time when the midterm will become available on Carmen. You will have 48 hours to complete the midterm. **You may not work with other students on the midterm or discuss it with them. If you anticipate a problem taking it as scheduled, you must notify me in writing during the first three weeks of the semester.** Don't expect me to work around you after that.

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.** If it is late, it's a zero.

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.** Don't expect me to work around you after that. Portions of the project submitted late will not count towards your final grade.

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 showing up to sit through a lecture. Participation includes making comments, asking questions, answering questions, contributing to group work, etc.

You can be penalized for 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 or phone, sending text messages, playing games on your phone, etc.

I understand that sometimes situations arise that keep you away from class. Do let me know if you have a good reason 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 slides, keeping up in the readings, and beginning any new homework assignment. I will not repeat entire lectures during office hours, but I will gladly answer specific questions after you have studied the slides.

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, and always examine things closely, as there 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 11:59pm on the day listed. You can take the quiz anytime on that day between 12:01 am and 11:59 pm.

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	Aug 25 T		Intro to course, intro to ciphers	TCB 1
	8/27 R		Monoalphabetic	AFM 1, 2
2	Sept 1 T		Steganography and Kerckhoff's Principle	AFM 3, 4
	9/3 R	HW 1: Shift	Monoalphabetic cont'd	TCB 2
3	9/8 T	Quiz 1: TCB 1 (Mary's)	Polyalphabetic: Vigenere	
	9/10 R	HW 2: Monoalphabetic	Polyalphabetic cont'd	TCB **5, not 3!**
4	9/15 T	Quiz 2: TCB 2 (Chiffre)	Writing systems: ABCማጟᔦᕗআ ϸhᑌვ 表記法	AFM 5
	9/17 R	HW 3: Vigenere	Polygraphic: Playfair	**AFM 6, 7 on**

				Playfair
5	9/22 T	Quiz 3: TCB **5 (Lang)**	Playfair Cont'd	
	9/24 R	HW 4: Strange Writing, Strange Reading	Decoding ancient languages	
6	9/29 T		Ancient languages cont'd	AFM 11- 13
	Oct 1 R	HW 5: Playfair	Transposition	TCB 3
7	10/6 T		Transposition cont'd	
	10/8 R	HW 6: Transposition, Quiz 4: TCB 3 (Mech)	Cipher Signatures, Midterm Review	
8	10/13 T	**Security Clearance Exam (Midterm) opens 12:01am, Tuesday, 13 October; due 11:59pm Wednesday, 14 October; no lecture, you have plenty to do!**		
	10/15 R	**Autumn Break! Relax and prepare yourself for the trials ahead!**		
9	10/20 T		Applied competitive cryptanalysis	
	10/22 R		field op skills, Crypto Cell Primer	TCB 4
10	10/27 T	RJ-16s due for ACC	Brand X cipher; op sec WWII to present, Scarlet Sentinel Briefing	Briefing Materials
	Operation Scarlet Sentinel begins 12:01am, Wednesday 28 October			
	10/29 R		Modern symmetric ciphers; team time	
11	11/3 T	Quiz 5: TCB 4	Gray Guardian briefing; counterintelligence; team time	
	11/5 R		Computer security; team time	TCB 6a pp 243-67
12	11/10 T		DHM, Public-key encryption; team time	
	Scarlet Sentinel ends (and all cryptanalyses due) 11:59pm, Tuesday, 10 November Operation Gray Guardian begins 12:01am, Wednesday, 11 November			
	11/12 R		Public-key encryption applications; team time	TCB 6b pp 268-92
13	11/17 T	Quiz 6: TCB 6a pp 243-67	Passwords, Off-the-Record; team time	Begin reviewing all slides after Midterm
	11/19 R	Quiz 7: TCB 6b pp 268-92	Zero-knowledge proofs; team time	
14	11/24 T		Voting systems, Crypto-currency	
	Operation Gray Guardian ends 11:59pm, Tuesday, 24 November			
	11/26 R	**Happy Thanksgiving!**		
	Operation Gray Guardian reports due 12:01am, Tuesday, 1 December			
15	Dec 1 T		Flex day, material TBD	

	12/3		Flex day, material TBD	
	12/8		Flex day, material TBD	
	Modern Crypto Superquiz opens 12:01am Thursday, 23 April; due 11:59 PM Friday, 24 April			

Linguistics 3801: Codes and Code Breaking, Spring 2020

Classroom: Hopkins Hall 246 Times: Tues/Thurs 9:35 - 10:55 am

Instructors

Daniel Puthawala puthawala.1@osu.edu Oxley Hall 300

Office hours: You are welcome to come to either my hours or another instructor's. See the Carmen page "Office Hours and Directions" for details. 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 Office: 114 Oxley Hall

Course Materials

1. Simon Singh, The Code Book ("TCB"), edition of 1999 or 2000. **Do not get the 2001, 2002, or young adult edition. They are missing information that you will need.** See the Carmen page "Getting the right edition of The Code Book" for details.
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
4. A Nerf or similar dart gun, any size, any kind, needed by the midterm (2/25)

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 2/25. Clearance is required for project ops.
Projects: 33%, Above your current security clearance. 4 weeks, 3/16 - 4/12.
Presentation: 4%, A short small-group presentation on a security breach.
Participation: Come to class and take part. You'll need to do this anyway to master the skills for the rest of your homework and projects. If you can't be bothered, then perhaps this isn't the right class for you.

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:

- Make students well-versed in the basic principles of secure communication
- Enable students to critically question the structures of information systems.
- Understand where cryptosystems leak information, and how leaks can be exploited or mitigated.
- Provide students with a background of the historical trends in cryptography and security.

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.
- Engage in live-action secret missions with and against your peers, gaining practical security skills, and mastering tactical nerf operations.
- According to my reviews, take the best college course of your life and miss it when it's over.

Disability Accommodation

If you may face a disability (including mental health issues and other chronic or temporary medical conditions), please contact me privately within the first three weeks of class. If a disability arises later, contact me as soon as is practical. I rely on Student Life Disability Services to help establish appropriate accommodations and sometimes to implement them, so I may request that you register there. They can be reached at slds.osu.edu, 614-292-3307, slds@osu.edu, or 098 Baker Hall, 113 W 12th Ave.

Other Help Resources

- **Your Instructor:** I make the rules and run the class, so if 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.

- You can get free, confidential, expert help with many personal and academic concerns from **Counseling and Consultation Services.** They also offer self-help resources online. ccs.osu.edu, 614-292-5766, sl-ccs@osu.edu, Younkin Success Center 4th Floor.
- Title IX prohibits discrimination on the basis of sex under any OSU program or activity. That includes assault, harassment, and limiting your enjoyment of opportunities or rights. You can find help, file grievances, and learn to help others via **OSU's Title IX Coordinator.** The Title IX office also has information about many other forms of discrimination. titleix.osu.edu, 614-247-5838, titleix@osu.edu, 21 East 11th Ave.

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.

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			
Homework	2700 pts	(27%)	A	9300 - 10000+ pts
Quizzes	600 pts	(6%)	A-	9000 - 9299
Exam	2000 pts	(20%)	B+	8700 - 8999
Competitive Analysis	300 pts	(3%)	B	8300 - 8699
Final Project (Part 1)	1500 pts	(15%)	B-	8000 - 8299
Final Project (Part 2)	1500 pts	(15%)	C+	7700 - 7999
Presentation	400 pts	(4%)	C	7300 - 7699
Superquiz	1000 pts	(10%)	C-	7000 - 7200
			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 11:59pm 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. Late homework is graded at 80% of normal value if received within the first week, 40% within the second week, zero after that. Do inform me if you have extenuating circumstances such as a health crisis.

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 250 points for answering the questions that pertain to the usual methods of decipherment 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 on the day 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.

Security Clearance Exam

There will be a mid-term "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.). See the class schedule below for the exact date and time**. If you anticipate a problem taking it as scheduled, you must notify me in writing during the first three weeks of the semester.** Don't expect me to work around you after that.

Modern Cryptography "Superquiz"

There will be an extended quiz covering the material presented in lectures after the midterm. This quiz will also be open-book, open-notes, etc., but you will have much more than 10 minutes for the attempt, and it will be open for 48 hours (the last day of classes and the following Reading Day). **If you cannot take it as scheduled, contact your instructor ASAP.** If it is late, it's a zero.

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.** Don't expect me to work around you after that. Portions of the project submitted late will not count towards your final grade.

Presentation

You will give a short presentation on a security breach that has been reported in the news in recent years, or from history if it is still relevant to security precautions today. You are encouraged to start reading around now, looking for a security breach that catches your interest. If you are not ready to present on time, the late policy is just like the homework: 80%/40%/0%. Depending on interest and timing constraints, I may offer optional assignments that can be done in lieu of the group presentation.

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 showing up to sit through a lecture. Participation includes making comments, asking questions, answering questions, contributing to group work, etc.

You can be penalized for 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 or phone, sending text messages, playing games on your phone, etc.

I understand that sometimes situations arise that keep you away from class. Do let me know if you have a good reason to miss class, since that will shape my impression of your participation.

To keep an eye on who is coming to class, and to get feedback so I can improve the course over the semester I will require you to complete minute papers on arbitrary days. This simply means that I will provide you with an index card on which you must legibly write the following three things: (1) Your name, (2) The most important thing you learned in class today, and (3) a question that you still have about the material or other constructive feedback.

If you will be missing class on a given day, you are still responsible for submitting homework on time via Carmen, studying the slides, keeping up in the readings, and beginning any new homework assignment. I will not repeat entire lectures during office hours, but I will gladly answer specific questions after you have studied the slides.

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, and always examine things closely, as there 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 11:59pm on the day listed. You can take the quiz anytime on that day between 12:01 am and 11:59 pm.

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	1/7 Tu		Intro to course, intro to ciphers	TCB 1
	1/9 Th		Monoalphabetic	AFM 1, 2
2	1/14 Tu		Steganography and Kerckhoff's Principle	AFM 3, 4
	1/16 Th	HW 1: Shift	Monoalphabetic cont'd	TCB 2
3	1/21 Tu	Quiz 1: TCB 1 (Mary's)	Polyalphabetic: Vigenere	
	1/23 Th	HW 2: Monoalphabetic	Polyalphabetic cont'd	TCB **5, not 3!**
4	1/28 Tu	Quiz 2: TCB 2 (Chiffre)	Writing systems: ABCሟቻᏎᏭআ թսց 表記法	AFM 5
	1/30 Th	HW 3: Vigenere	Polygraphic: Playfair	**AFM 6, 7 on Playfair**
5	2/4 Tu	Quiz 3: TCB **5 (Lang)**	Playfair Cont'd	
	2/6 Th	HW 4: Strange Writing, Strange Reading	Decoding ancient languages	
6	2/11 Tu		Ancient languages cont'd	AFM 11- 13
	2/13 Th	HW 5: Playfair	Transposition	TCB 3
7	2/18 Tu		Transposition cont'd	
	2/20 Th	HW 6: Transposition, Quiz 4: TCB 3 (Mech)	Cipher Signatures, Midterm Review, ACC briefing	
8	2/25 Tu	**Security Clearance Exam (Midterm)**		
	2/27 Th	Bring your Nerf gun	Applied Competitive Cryptanalysis	
9	3/3 Tu		field op skills, Crypto Cell Primer	TCB 4
	3/5 Th	RJ-16s due for ACC	Brand X cipher; op sec WWII to present, Scarlet Sentinel Briefing	Briefing Materials
10	3/10 Tu	**Spring Break! Go somewhere warm and prepare yourself for the trials ahead! The Code Book makes excellent reading material on long flights/road trips! Annoy your friends and family with Crypto-Trivia!**		
	3/12 Th			

	Operation Scarlet Sentinel begins 12:01 am Monday, 16 March			
11	3/17 Tu		Modern symmetric ciphers; team time	
	3/19 Th	Quiz 5: TCB 4	Gray Guardian briefing; counterintelligence; team time	
12	3/24 Tu		Computer security, DHM; team time	TCB 6a pp 243-67
	3/26 Th		DHM Cont'd, Public-key encryption; team time	Briefing Materials
	Operation Scarlet Sentinel Ends (and all Cryptanalyses due) 11:59 PM Sunday, 29 March Operation Gray Guardian begins 12:01 AM Monday, 30 March			
13	3/31 Tu		Public-key encryption applications; team time	TCB 6b pp 268-92
	4/2 Th	Quiz 6: TCB 6a pp 243-67	Passwords, Off-the-Record; team time	Begin reviewing all slides after Midterm
14	4/7 Tu	Quiz 7: TCB 6b pp 268-92	Zero-knowledge proofs; team time	
	4/9 Th		Voting systems, Crypto-currency	
	Operation Gray Guardian ends 11:59 PM Sunday, 12 April			
15	4/14 Tu	Presentations Ready	Presentations	
	4/16 Th		Presentations	
	Operation Gray Guardian reports due 11:59 PM Saturday, 19 April			
	Modern Crypto Superquiz opens 12:01am Thursday, 16 April; due 11:59 PM Friday, 17 April			

Arts and Sciences Distance Learning Course Component Technical Review Checklist

Course: LING 3801
Instructor: Micha Elsner
Summary: Codes and Code Breaking

Standard - Course Technology	Yes	Yes with Revisions	No	Feedback/ Recomm.
6.1 The tools used in the course support the learning objectives and competencies.	X			• Carmen • Office 365
6.2 Course tools promote learner engagement and active learning.	X			• Zoom lectures • Zoom project meetings • Carmen discussion boards
6.3 Technologies required in the course are readily obtainable.	X			.All are available free of charge via OSU
6.4 The course technologies are current.	X			All are updated regularly
6.5 Links are provided to privacy policies for all external tools required in the course.	X			No external tools are used.
Standard - Learner Support				
7.1 The course instructions articulate or link to a clear description of the technical support offered and how to access it.	X			Links to 8HELP are provided
7.2 Course instructions articulate or link to the institution's accessibility policies and services.	X			a
7.3 Course instructions articulate or link to an explanation of how the institution's academic support services and resources can help learners succeed in the course and how learners can obtain them.		X		Please include statement b
7.4 Course instructions articulate or link to an explanation of how the institution's student services and resources can help learners succeed and how learners can obtain them.	X			Please include statement c
Standard – Accessibility and Usability				
8.1 Course navigation facilitates ease of use.	X			Recommend using the Carmen Distance Learning "Master Course" template developed by ODEE and available in the Canvas Commons to provide student-users with a consistent user experience in terms of navigation and access to course content.
8.2 Information is provided about the accessibility of all technologies required in the course.	X			Instructions are provided
8.3 The course provides alternative means of access to course materials in formats that meet the needs of diverse learners.	X			Instructions are provided
8.4 The course design facilitates readability	X			
8.5 Course multimedia facilitate ease of use.	X			All assignments and activities that use the Carmen LMS with embedded multimedia facilitates ease of use. All other multimedia resources facilitate ease of use by being available through a standard web browser

Reviewer Information

- Date reviewed: 6/1/20
- Reviewed by: Ian

Notes: This one is ready to move on!

[a]The following statement about disability services (recommended 16 point font): Students with disabilities (including mental health, chronic or temporary medical conditions) that have been certified by the Office of Student Life Disability Services will be appropriately accommodated and should inform the instructor as soon as possible of their needs. The Office of Student Life Disability Services is located in 098 Baker Hall, 113 W. 12th Avenue; telephone 614- 292-3307, slds@osu.edu; slds.osu.edu.

[b]Add to the syllabus this link with an overview and contact information for the student academic services offered on the OSU main campus.
http://advising.osu.edu/welcome.shtml

[c]Add to the syllabus this link with an overview and contact information for student services offered on the OSU main campus. http://ssc.osu.edu. Also, consider including this link in the “Other Course Policies” section of the syllabus.