



Linguistics 294L

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.

Course Book

The textbook is *The Code Book*, by Simon Singh. You should buy this and expect to read all of it as background to the course. There will be some overlap between the technical material of the course and that presented in the book, but there will be material presented in class that is not covered at all in the book.

Course Objectives:

Students in 294L 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.

Instructor Details

Chris Brew
200A Oxley Hall
1712 Neil Ave
Columbus Ohio 43210-1298
Email: will be disclosed in class
Office hours: 4pm-5pm TWR

Class location

Bolz Hall 314: 10:30-12:18 Monday Wednesday

Topics

Codes

- Monoalphabetic ciphers: Caesar cipher, keywords
- Polyalphabetic ciphers: Vigenère cipher
- Transposition ciphers
- Polygraphic ciphers: Playfair; Hill Cipher
- Perfect ciphers: The one-time pad.
- Enigma: the technology

Linguistic Codes

- Linear-B: Decoding Ancient Texts
- Hangul: Korean Writing

Codes and Intelligence in War

- Enigma: the intelligence
- Exploiting Intelligence from Cryptography

Assessment

There will be regular short code-breaking assignments. To succeed on these you need to attend the classes, and make a serious attempt to solve the codes. There will also be in-class 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 occasional extra credit opportunities

Component	Score
Weekly assignments	50 points (10 at 5 points each)
Quizzes	5 points (5 at 1 point each)
Mid-term	20 points
Final project	20 points
Class participation	5 points
Available extra credit	5 points

Grade	Point Range
A range	90-100
B range	80 – 89
C range	70 – 79
D range	60-69
E	0-59

Your responsibilities

All class members are responsible for

- Keeping up with the assignments and reading

- Monitoring your own progress and understanding of the material. If there is something you don't understand, please do ask, preferably in class.
- Contributing to class discussion.
- Helping to form a "course community". This includes responding appropriately and helpfully to other class members.

Academic Misconduct

It is the responsibility of the Committee on Academic Misconduct to investigate or 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

(http://studentaffairs.osu.edu/resource_csc.asp).

Cheating is wrong, wastes your time and ours, and will not be tolerated.

Working together to find the answer is fine, but talking to someone who has already figured out the answer is cheating. You must also do your homework by yourself unless it is specifically designated as group work. We will assume that you are honest, but if we are confronted with clear evidence of cheating, it is our duty to take action.

Students with Disabilities

Ohio State is committed to extending access and opportunity to those who are disabled. Any student who feels s/he may need an accommodation based on the impact of a disability should contact me privately to discuss your specific needs. You may also contact the Office for Disability Services at 614-292-3307 in room 150 Pomerene Hall.

Rough schedule

The table below indicates roughly when which piece of the course will be covered. Things may change as the course develops.

Week	Dates	Topic	Notes
1	Mar 26, 28	Monoalphabetic ciphers	Singh ch 1
2	Apr 2, 4	Polyalphabetic ciphers	Singh ch 2
3	Apr 9, 11	Decoding ancient languages	Singh ch 5
4	Apr 16, 18	Polygraphic ciphers	Singh ch 3
5	Apr 23, 25	Enigma: the intelligence	Singh ch 6
6	Apr 30, May 2	Transposition ciphers	Midterm May 2nd
7	May 7, May 9	Korean writing	Singh ch 7
8	May 14, May 16	Perfect ciphers	Singh ch 8
9	May 21, May 23	Enigma, the technology	Singh ch 4
10	May 30	Exploiting intelligence	Memorial Day
Exam	Jun 6	Final project due	