

Linguistics 484: Code Making and Code Breaking

Class location

Bolz Hall 314: 1:30-3:18 Monday Wednesday

Remember that Friday 4 Jan counts as the first Monday

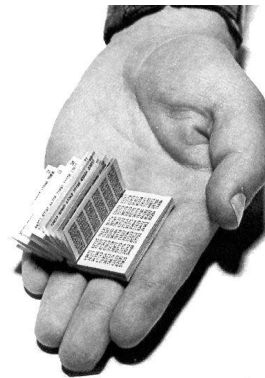
Instructor Details

Chris Brew

583 Dreese Labs or 200 Oxley Hall
Columbus Ohio

Email: will be disclosed in class

Office hours: 4pm-5pm TWR



These images are of an Enigma rotor cipher machine, a tiny Soviet one-time pad, a 19th century US cipher device and a modern version of the ancient Greek scytale. We'll study all of these.

Aims

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. This course is still listed as experimental, so the number is 294, but it has now been approved as Linguistics 484 and the material is at 400 level.

Course Book

The textbook is *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (ISBN 0-385-49532-3), 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. There will be quizzes on the Code Book every Wednesday except for the Wednesday of the midterm.

Course Objectives:

Students in Linguistics 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.

Topics

Codes

- Monoalphabetic ciphers: Caesar cipher, keywords
- Polyalphabetic ciphers: Vigenère cipher
- Transposition ciphers
- Polygraphic ciphers: Playfair; Hill Cipher
- The one-time pad.
- Quantum cryptography (easy version: physics major not required)
- 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 small extra credit opportunities

The Final Project

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 me 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.

Points table

Component	Score
Weekly assignments	48 points (8 at 6 points each)
Quizzes	7 points (7 at 1 point each)
Mid-term	15 points
Final project	25 points

Component	Score
Class participation	5 points
Total	100 points
Available extra credit	5 points

The table below shows the connection between grades and point scores. If you make the point score, you can count on getting **at least** the grade listed. I reserve the right to give a higher grade if this is warranted by something you do in the course, but I will never give a lower grade.

As a rough guide, you can get a B by simply learning and understanding the material I teach in the course. To get an A you need to do that, but also show some originality.

Grade	Point Range
A	94-100
A-	90-93
B+	86-89
B	83-85
B-	80-82
C+	77-79
C	74-76
C -	70 – 73
D+	64-69

Grade	Point Range
D	60-63
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.

Winter 2008

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

Week	Dates	Topic	Notes
1	Jan F 4, M 7	Monoalphabetic ciphers	Singh ch 1
2	Jan W 9, M 14	Polyalphabetic ciphers	Singh ch 2
3	Jan W 16, W 23	Decoding ancient languages	Singh ch 5 (MLK Day Jan 21)
4	Jan M 28, W 30	Polygraphic ciphers	Singh ch 3
5	Feb M 4, W 6	Enigma: the intelligence	Singh ch 6
6	Feb M 11, W 13	Transposition ciphers	Midterm, Feb 13
7	Feb M 18, W 20	Korean writing	Singh ch 4
8	Feb M 25, W 27	Enigma, the technology	Singh ch 7
9	Mar M 3, W 5	Quantum Cryptography Project reports	Singh ch 8
Exam	Mar M 10	Final project writeup due	