Lign 17: Making and Breaking Codes

Prof. Andrew Kehler
UCSD Department of Linguistics
akehler@ucsd.edu
(858) 534-6239

Winter, 2017
MWF 11:00-11:50, Center Hall 105
Office Hours: Mondays 1-2 and Fridays 2-3:30 (AP&M 4256)

TA: Eric Meinhardt (emeinhardt@ucsd.edu)
TA Section Times and Office Hours: TBA

Overview

A rigorous analysis of symbolic systems. Encryption and decryption of information using progressively more sophisticated methods. Other types of codes and their applications.

Prerequisites

There are no prerequisites. The course satisfies various formal skills requirements in the Human Development Program and Marshall, Roosevelt, Warren, and Sixth colleges.

The course does not presume familiarity with any field of knowledge. In particular, you do not need to know any linguistics, number theory, or statistics in advance. However, bear in mind that because it satisfies a number of formal skills requirements, this course will involve a fair bit of problem solving and some unusual arithmetic. Expect it to be challenging (but hopefully fun!).

Textbook

Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Press, 2000. Available at the bookstore and Amazon.com ($11.48 paperback; $9.99 kindle). Note that there is more than one version; the version you buy should have a brown cover.

Administrivia

There will be five assignments distributed on TED at relatively regular intervals, cumulatively worth 15% of your grade.

There will be two exams: a midterm and a final, worth 35% and 50% of your grade respectively.

Students are permitted to consult with each other and/or work together in learning the concepts necessary for completing the homework, *as long as each student completes his or her own homework alone, using no notes resulting from the collaboration.* **Collaborative efforts not meeting this restriction are strictly forbidden!**

Any students who require OSD accommodations should meet with me during the first week of class to discuss arrangements.

Needless to say, please turn off your cell phones before entering the classroom.

Provisional Schedule

I. Course Overview (Monday, Jan 9)

II. Introduction to Codes and Ciphers (Wednesday, Jan 11 – Friday, Jan 20)

Reading: Singh, Chapter 1

Monday, Jan 16: Happy Martin Luther King Day!

Assignment #1: Available on Jan 19, *due Tue, Jan 26, at 11:55pm*

III. More Advanced Ciphers, and How to Crack Them (Monday, Jan 23 – Wednesday, Feb 1)

Reading: Singh, Chapter 2; Chapter 3 (pp. 115-124 only)

Assignment #2: Available on Jan 29, *due Sun, Feb 5, at 11:55pm*

IV. Number Theory, Protocols, and RSA (Friday, Feb 3 – Wednesday, Feb 15)

Reading: Singh, Chapter 6

Assignment #3: Available on Feb 7, *due Tue, Feb 14, at 11:55pm*

Friday, Feb 17th: Midterm Exam

V. Probability, Randomness, Information Theory, and Data Compression (Wednesday, Feb 22 – Wednesday, March 1)

Reading: To be distributed

Monday, Feb 20th: Happy President's Day!

Assignment #4: Available on Feb 26, *due Sun, March 5, at 11:55pm*

VI. Error Detecting Codes (Friday, March 3 – Monday, March 13)

Reading: To be distributed

Assignment #5: Available on Mar 7, *due Tues, Mar 14, at 11:55pm*

VII. The Language Code (Wednesday, March 15)

Reading: To be distributed

VIII. Summary and Review (Friday, March 17)

Final Exam: Monday, March 20, 11:30-2:30