# Lign 17: Making and Breaking Codes

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

Winter, 2018
MWF 11:00-11:50, Center Hall 105
Office Hours: Mondays 1-2 and Fridays 1:30-3 (AP&M 4256)

TA: Eric Meinhardt (emeinhardt@ucsd.edu)
Office Hours: Tuesdays 10-11 (AP&M 2442)
Optional Sections: Wednesdays 10-11 and Thursdays 11-12 (AP&M 2442)

## 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 (about $15). 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 TritonEd 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. Please make note of the exam dates.

We adhere to the UCSD Policy on Integrity of Scholarship, so please consult it:

https://academicintegrity.ucsd.edu/process/policy.html

Note that per UCSD policy, we are obligated to report instances of suspected academic dishonesty to the Academic Integrity Office.

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 8)

**II. Introduction to Codes and Ciphers** (Wednesday, Jan 10 – Friday, Jan 19)

Reading: Singh, Chapter 1

Monday, Jan 15: Happy Martin Luther King Day!

Assignment #1: Available on Jan 18, *due Tue, Jan 25, at 11:55pm*

**III. More Advanced Ciphers, and How to Crack Them** (Monday, Jan 22 – Wednesday, Jan 31)

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

Assignment #2: Available on Jan 28, *due Sun, Feb 4, at 11:55pm*

**IV. Number Theory, Protocols, and RSA** (Friday, Feb 2 – Wednesday, Feb 14)

Reading: Singh, Chapter 6

Assignment #3: Available on Feb 6, *due Tue, Feb 13, at 11:55pm*

**Friday, Feb 16th: Midterm Exam**

**V. Probability, Randomness, Information Theory, and Data Compression** (Wednesday, Feb 21 – Wednesday, Feb 28)

Reading: To be distributed

Monday, Feb 19th: Happy President's Day!

Assignment #4: Available on Feb 25, *due Sun, March 4, at 11:55pm*

**VI. Error Detecting Codes** (Friday, March 2 – Monday, March 12)

Reading: To be distributed

Assignment #5: Available on Mar 6, *due Tues, Mar 13, at 11:55pm*

**VII. The Language Code** (Wednesday, March 14)

Reading: To be distributed

**VIII. Summary and Review** (Friday, March 16)

**Final Exam: Monday, March 19, 11:30-2:30**