Lign 17: Making and Breaking Codes

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

Winter, 2009
MWF 11:00-11:50, Ledden Auditorium
Office Hours: Mondays 1-2, Fridays 2-3, or by appt. (AP&M 4256)

TA: David Hall (dhall@ling.ucsd.edu)
Section Times and Office Hours: TBA

Overview

A rigorous analysis of symbolic systems. Encryption and decryption of information using progressively more sophisticated methods. Various linguistics problems analyzed as codebreaking problems.

Prerequisites

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

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 ($10.85). Note that there is more than one version; the version you buy should have a brown cover.

Administrivia

There will be approximately five assignments distributed on WebCT 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.

There may be opportunities for obtaining extra credit by participating in ongoing psycholinguistic experiments. More details will be provided in class.

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 is strictly forbidden.

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

Provisional Schedule

I. Course Overview (Monday, Jan 5)

II. Introduction to Codes and Ciphers (Wednesday, Jan 7 – Wednesday, Jan 14)

Reading: Singh, Chapter 1

Friday, Jan 9: CLASS CANCELLED

III. More Advanced Ciphers, and How to Crack Them (Friday, Jan 16 – Monday, Jan 26)

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

Monday, Jan 19: Happy Martin Luther King Day!

IV. Number Theory, Protocols, and RSA (Wednesday, Jan 28 – Friday, Feb 6)

Reading: Singh, Chapter 6

V. Probability, Randomness, Information Theory, and Compression (Monday, Feb 9 – Monday, Feb 23)

Reading: To be distributed

Friday, Feb 13th: Midterm Exam

Monday, Feb 16th: Happy President's Day!

VI. Error Detecting Codes (Wednesday, Feb 25 – Wednesday, March 4)

Reading: To be distributed

VII. Language Modeling and Its Applications (Friday, March 6 – Wednesday, March 11)

Reading: To be distributed

VIII. Summary and Review (Friday, March 13)

Final Exam: Monday, March 16, 11:30-2:30