SIGN 26002/LING 26040 Fall 2017
University of Chicago TuTh 11-12.20

Code Making/Code Breaking

Instructor: Chris Kennedy (ck@uchicago.edu)
Office hours: M 11-12 or by appointment, Rosenwald 205E

TA: Julian Grove (juliang@uchicago.edu)
Office hours: W 3-4 or by appointment, Social Sciences 010B (Landahl Center for Linguistic Research)

TA: Orest Xherija (orest.xherija@uchicago.edu)
Office hours: W 11.30-12.30 or by appointment, Rosenwald 203 (Linguistics Department)

Course Description

This course investigates the nature and use of codes and ciphers throughout the ages: what they are, how they have been used, and ways that they have affected (and maybe even determined) the course of history and human development. We will start out by looking at writing, the most basic tool for encoding human thought. We will then turn to an exploration of ways that information is concealed and revealed in areas ranging from literature and religious texts to wartime communications and the human genome, with particular focus on questions arising from computer science on the nature of consciousness and the limits of privacy. We will conclude by returning to questions about the linguistic code: where it comes from, whether it can be perfected, and how we would recognize messages from outer space.

Sections

There are two sections for this course, which will be devoted to learning basic computational skills for text analysis, by studying and computationally implementing different kinds of encryption and decryption algorithms. Sections are not obligatory; however, they will provide the skills and background necessary for completing the exercises in code making and code breaking (see below), which *are* obligatory. If you already have a strong background in programming, and either know or can teach yourself the Haskell programming language, then you do not have to attend section, though your presence and expertise would still be welcome. The times/locations for the sections are:

- Section 1D01: Friday 1.30-2.20, Walker Museum 302
- Section 1D02: Friday 11.30-12.20, Campus North Residential Commons 158

Assessment

Grades will be based on participation in class discussion (5%) and performance on the following tasks:

- *Exercises in code making and code breaking* (20%) Students will complete weekly exercises in coding using the Haskell programming language (www.haskell.org). We will begin by writing programs for simple text-manipulation tasks, then move to encryption and decryption algorithms. Exercises will be assigned and discussed in section, and must be turned in **on Thursdays by 5pm**. Credit will be given on a pass/fail basis depending on whether assignments are turned in at all (and in the correct format), not on whether students are successful in actually writing code that does what it is supposed to do.
- *Short (5-7) paper on writing systems* (25%) Although there are thousands of different languages, which vary along a broad range of typological distinctions, there are only three types of writing systems: logographic, syllabic, and alphabetic/phonetic systems. (Or four, depending on how you count, since some systems are combinations of these.) Why just these three?

To address this question, construct an alternative writing system of your own design that is neither logographic, syllabic, nor alphabetic. Explain how your system works in detail, giving illustrative examples where necessary. Contrast your writing system with the three listed above, and use this comparison to advance a hypothesis about why only these three systems are used as the primary means of encoding linguistic communication. Papers are due by **the beginning of class on Tuesday, October 24**.

- *Group projects in cryptography and cryptanalysis* (15%) Students will be divided into groups of four or five. Each group will first devise an encryption algorithm and create a ciphertext, which will be shared with all the other groups. Each group will then try to decipher each of the other groups' work. At the end of the quarter, groups will give short presentations describing their encryption algorithms and their attempts to break the other groups' codes. Some constraints:

  - The plain text should consist of 500 contiguous words from the Project Gutenberg online edition of *Moby-Dick*: `www.gutenberg.org/files/2701/2701-h/2701-h.htm`
  - The encryption methodology must not be PERFECTLY SECRET, in the sense defined in chapter 2 of *The Introduction to Modern Cryptography*.
  - The algorithm must be computationally implementable.

  Ciphertexts are due by **5pm, Friday, November 3**, and should be submitted in a format that allows posting on Canvas. Solutions are due by **the beginning of class on Tuesday, November 28**, but can be turned in at any time. Prizes will be given to the group that breaks the first code and to the group that breaks the most codes. Presentations will take place on the evening of **Wednesday, November 29**.

- *Final project* (35%) Students must put together a final project on a topic of their choice that is related to the material covered in class. The exact nature of the final project is up to the student: it could be a research paper, a creative work, a computational work, etc. (This list is not meant to be exhaustive.)

  A one-page abstract describing and motivating the project must be submitted for approval by the instructor no later than **Tuesday, November 21**; the final version of the project is due on **Thursday, December 7**.

The Plan

On the next page are the topics we will cover in the course, in the order that we will discuss them. Readings for each class will be available on Canvas.

Note: Please check Canvas regularly, as I may add or subtract a few readings based on class interest and discussion.

Part 1: Introduction

9.26	Introduction	Doyle, "The Dancing Men"
9.28	On secret writing	Poe, "Cryptography"; Singh chs. 1-2; *Intro. to Modern Cryptography*, ch. 1

Part 2: Writing

10.3	History, development and relation to the structure of language	Gnanadesikan, ch. 1; Sampson chs. 1-2
10.5	The decipherment of cuneiform (guest lecture by Professor Christopher Woods, Department of Near Eastern Languages and Civilizations and Director of the Oriental Institute)	Pope, chs. 4-5
10.10	The decipherment of Mayan (guest lecture by Professor Claudia Brittenham, Department of Art History)	Coe chs. 2-4; Pope, "The Maya glyphs", **NOVA: Cracking the Mayan Code**, Stuart, "Ten phonetic symbols"
10.12	The sociology and politics of writing	Sebba, "Sociolinguistic approaches to writing systems research"; Young, "Should writer's use they own English?"; Fish, "What should colleges teach?"

Part 3: The Search for Hidden Meaning

10.17	In literature	Poe, "The Gold Bug"; Toner, "The 'remarkable effect' of 'silly words': Dialect and signature in 'The Gold Bug"'
10.19	In speech	Khoo, "Code words in political discourse"; Albertson "Dog-whistle politics: Multivocal communication and religious appeals"
10.24	In the structure of language	Stern, "Language"; Schloem, "The name of God and the linguistic theory of Kabala"
10.26	In dreams	Freud, *The Interpretation of Dreams*, ch. 2, pp. 121-145; Lear, *Freud*, ch. 3; **Spellbound**

Part 4: The Computational Turn

10.31	From difference engine to quantum computing	Singh, ch. 3; **The Imitation Game**
11.2	Coding consciousness?	Turing, "Computing machinery and intelligence," Searle, "Minds, brains and programs"
11.7	Cracking the genetic code	The Human Genome Project; Lippert et al., "Identification of individuals by trait prediction using whole-genome sequencing data"; Erlich, "Major flaws in 'Identification of individuals..."'
11.9	Security and privacy	Singh, ch. 6; *Intro. to Modern Cryptography*, ch. 2

Part 5: The Linguistic Code

11.14	In order to form a more perfect language	Frege, preface to *Begriffsschrift*; Borges, "The analytical language of John Wilkins"; Mineault and Pack, "The Cerebral Emporium of Benevolent Knowledge"
11.15	Where did language come from, anyway?	Nowak, "Evolutionary biology of language"
11.21	NO CLASS	
11.28	Messages from outer space	**Contact, Arrival**