Assignment 6
Computer Science 349
Spring 2004
Due: Start of class on Monday, March 29

Reading: Singh, Chapter 5, Stinson §2.6

Exercise 6.0. List the three passwords that you chose in Exercise 1.0 of assignment 1. No PKN.

Exercise 6.1. What useful advice is hidden in this following design?

Exercise 6.2. When calculating a lower bound on the number of spurious keys we used the inequality: \( H(K \mid y) \leq \log |K(y)| \), where
\[
K(y) = \{K \in \mathcal{K} : \Pr[X \in \mathcal{P} \mid \text{Pr}[X] > 0] e_k(x) = y \}.
\]
Use Jensen’s inequality to prove this result.

Exercise 6.3. (Stinson 2.15) Consider the Vigenère Cipher with keyword length \( m \). Show that the unicity distance is \( 1/R \), where \( R \) is the redundancy of the underlying language.

Figure 6.1. Words of wisdom.
Cryptography

This result is interpreted as follows. If \( n_0 \) denotes the number of alphabetic characters being encrypted, then the “length” of the plaintext is \( n_0/m \), since each plaintext element consists of \( m \) alphabetic characters. So, a unicity distance of \( 1/R_L \) corresponds to a plaintext consisting of \( m/R_L \) alphabetic characters.

**Exercise 6.4. (Stinson 2.17a)** A Substitution Cipher over a plaintext space of size \( n \) has \( |K| = n! \). Stirling’s formula gives the following estimate for \( n! \): 
\[
 n! 
\approx \sqrt{2\pi n} \left( \frac{n}{e} \right)^n .
\]
Using Stirling’s formula, derive an estimate of the unicity distance of the Substitution Cipher.

**Exercise 6.5.** Visit [http://www.stegoarchive.com/](http://www.stegoarchive.com/) or any other archive of your choice. Select your favorite steganographic software, install and play with it. Hide a message for your instructor and submit the result together with a brief explanation of the steganographic technique used. Include the name of the software used for this assignment. A gold star for the most creative hiding.

**Exercise 6.6.** A simple form of steganography, but one that is time-consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. Figure 6.3 shows an example in which a subset of the words of the overall message is used to convey the hidden message. What does it say?

Figure 6.2. A puzzle for Inspector Morse.

3rd March

**Dear George,**

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I’m told, by the 21st. Admin has improved here, though there’s room for improvement still; just give us all two or three more years and we’ll really show you! Please don’t let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,

Figure 6.2. A puzzle for Inspector Morse.