Assignment 4  
Computer Science 349  
Spring 2004  
Due: Start of class on Thursday February 26

Reading: Stinson, Sections 2.1, 2.2, 2.3

Exercise 4.0. The fewer the words you use in a telegram, the less it costs.
   (a) The following “thriftigram” arrived a few days ago from a friend. Unfortunately, I couldn’t figure out what it said. Can you help? Sanctuary much!

   (b) Here is a Valentine from a friend, also a mystery.

Exercise 4.1. The purpose of this problem is to show the unbreakability of the one-time pad. Suppose that we are using a Vigenère scheme with 27 characters in which the
twenty-seventh character is the space character, but with one-time key that is as long as the message. Given the ciphertext

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Explain how you would find two distinct one-time pads, the first of which yields the following plaintext:

MR MUSTARD WITH THE CANDLESTICK IN THE HALL

and the second that yields the following plaintext

MISS SCARLET WITH THE KNIFE IN THE LIBRARY

Comment on the result.

Exercise 4.2. (Stinson 2.1) Referring to Example 2.2, determine all the joint and conditional probabilities, $\Pr[x, y]$, $\Pr[x \mid y]$, and $\Pr[y \mid x]$, where $x \in \{2, \ldots, 12\}$ and $y \in \{D, N\}$.

Exercise 4.3. (Stinson 2.2) Let $n$ be a positive integer. A Latin Square of order $n$ is an $n \times n$ array $L$ of the integers $1, \ldots, n$ such that every one of the $n$ integers occurs exactly once in each row and each column of $L$. An example of a Latin square of order 3 is as follows:

$$
\begin{array}{ccc}
1 & 2 & 3 \\
3 & 1 & 2 \\
2 & 3 & 1 \\
\end{array}
$$

Given any Latin square $L$ of order $n$, we can define a related cryptosystem. Take $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, 2, \ldots, n\}$. For $1 \leq i \leq n$, the encryption rule $e_i$ is defined to be $e_i(j) = L(i, j)$. (Hence each row of $L$ gives rise to one encryption rule.) Give a complete proof that this Latin Square Cryptosystem achieves perfect secrecy provided that every key is used with equal probability.

Exercise 4.4. (Stinson 2.4) Suppose a cryptosystem achieves perfect secrecy for a particular plaintext probability distribution. Prove that perfect secrecy is maintained for any plaintext probability distribution.

Exercise 4.5. (Stinson 2.5) Prove that if a cryptosystem has perfect secrecy and $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$, then every ciphertext is equally probable.

Let $y \in \mathcal{C}$; then