HW 4 CMSC 389. DUE Jan 8

1. (0 points) What is your name? Write it clearly. Staple your HW. What is the day and time of the first midterm? Are you free then? (if not then SEE ME IMMEDIATELY) What is the day and time of the second midterm? Are you free then? (if not then SEE ME IMMEDIATELY) When is the final? Are you free then? (if not then SEE ME IMMEDIATELY)

2. (20 points) Alice and Bob are going to use a 1-time pad. Alice gives Bob the key 000111001100101.

   (a) Bob wants to send 1001. What does he send?

   (b) THEN Alice wants to respond 1111. What does she send?

3. (20 points) Alice and Bob want to use a Faux-1-time pad with the key 1000101001000101001

   (a) Alice wants to send a 10 bit message. What key does she use?

   (b) THEN Bob wants to reply with a 5-bit message. What key does he use?

4. (30 points) (This will use the code you've written in the past.) Let T be the text on the web having that is next to this HW on the website (its about the Turing Pardon). For $s = 10, 20, 30, 40, \ldots, 400$ do the following:

   (a) Restrict the text to every sth letter. (e.g., if $s = 30$ then you will look at the 30th, 60th, 90th, etc letter). Within this subset of the text find, for each i, the freq of the ith letter. Denote this by $p_{i,s}$.

   (b) Compute $F(s) = \sum_{i=1}^{26} p_{i,s}^2$.

   Hand in a nice table of the $F(s)$ for $s = 10, 20, \ldots, 400$. If you have time an inclination make a graph out of it. What happens as s increases? Speculate on why this happens.

5. (30 points) Let $f_1 = 1$, $f_2 = 1$, $(\forall n \geq 3)[f_n = f_{n-1} + f_{n-2}]$. Let $b_i = f_i \pmod 2$. Alice and Bob use a Faux-1-time-pad using the sequence b_i.

   (a) Alice wants to send Bob 100110. What does she send?

   (b) THEN Bob wants to send Bob 1111. What does he send?