HW 3 CMSC 389. DUE Jan 7

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. (10 points) Alice and Bob will use a Vig cipher. Alice gives Bob the key CAT. Use this to code the following phrase:

   I watch Breaking Bad

3. (40 points) (NOTE- you may want to write a program to do this one for you. Read the entire question first so you can do this.)

   (a) Find on the web frequencies for a,b,c,e,...,z in English. Write them down for the HW.

   (b) For $1 \leq i \leq 26$ let p_i be the frequency for the ith letter. Compute $s_0 = \sum_{i=1}^{26} p_i^2$. Write down s_0.

   (c) For all $j \in \{0, 1, 2, \ldots, 25\}$ compute $s_j = \sum_{i=1}^{26} p_i p_{i+j}$. (The $i+j$ is done mod 26.) Write down all of the s_j.

   (d) What is the max value of s_j ($j \neq 0$). Call this $s_{\max}$. What is $s_0 - s_{\max}$.

4. (50 points) (In this problem you use the program you wrote for HW02) Let T be the text on the course website.

   (a) Encode it using your program and the shift $f(x) = x + 4$.

   (b) Find $q_1, q_2, \ldots, q_{26}$, the frequencies of the 1,2,...,$26th$ letter.

   (c) (Let p_i be from the last problem.) For all $j \in \{0, 1, 2, \ldots, 25\}$ compute $s_j = \sum_{i=1}^{26} p_i q_{i+j}$. (The $i+j$ is done mod 26.) Write down all of these values. IF you didn't know it was a shift 5 cipher, how could you use this to find the shift?

5. (0 points but you will need this program later).

   (a) Write programs that will, given a key K and a plaintext T, produces the encoding of T from the Vig cipher using key K.

   (b) Write a program that will, given a text that was coded via a Vig cipher, will determine a small finite set of values so that at least one of them is the length of the key.

   (c) Write a program that will, given a text that was coded via a Vig cipher, will find the length of the key, the key, and the decoding.