HW 3 CMSC 389. DUE Jan 8

NOTE- THERE ARE TWO PAGES TO THIS ASSIGNMENT!!!!

1. (10 points) READ my NOTES on line. What is your name? Write it clearly. Staple your HW.

2. (0 points but you REALLY WANT to do this so you can use it on HW04 and other later HWs) This programming assignment will have you write a program that will, given a ciphertext that was coded using the shift cipher, FIND the shift without any help from humans. (The text has to be fairly long and not, like the novel *Gadsby*, written without any e's)

   (a) Write a program that will, given a ciphertext, determine how often each letter appears (this program you already wrote). Let the number of times they appear be $h_a, h_b, \ldots, h_z$. Note that the h_σ are natural numbers.

   (b) Write a program that will, given numbers $h_a, \ldots, h_z$, find for all σ in the alphabet, $q_\sigma = h_\sigma / (\sum_{\sigma \in \Sigma} h_\sigma)$ (Divide the number of times q appears by the total number of letters.) These are the relative frequencies of the letters. Note that q_σ are real numbers that are between 0 and 1.

   (c) Let $p_a, p_b, p_c, \ldots$ be the frequencies in English. (Obtain them from the web. Your program should store them. Note that the p_σ are real numbers between 0 and 1.) Write a program that will, given numbers $q_a, q_b, \ldots, q_z$ and given $s \in \{0, \ldots, 25\}$ compute $\sum_{\sigma \in \Sigma} p_\sigma q_{\sigma+s}$.

   (d) (This program uses all of those above.) Write a program that will, given the a ciphertext T, outputs for all $s \in \{0, \ldots, 25\}$, $\sum_{\sigma \in \Sigma} p_\sigma q_{\sigma+s}$. Shift by the value of s that makes this largest and see if it looks like good English.

3. (30 points) Describe an algorithm for the following problem: Given a ciphertext T that has been coded by an affine cipher, and given (a, b) where $0 \leq a, b \leq 26$ and a is relatively prime to 26, determine if the ciphertext was coded with $f(x) = ax + b$. (This will be similar to the summation technique used for a similar problem with Shift Ciphers.)

4. (30 points) Let T be the sentence *Alan Turing helped win World War II.*

   (a) Code T with a shift cipher with a shift of 2.

   (b) Code T with an affine cipher $f(x) = 2x + 3$. (YES I am using 2 as the coefficent even though 2 is not rel prime to 26.)

   (c) Code T with a Vigenere cipher with keyword DOG

5. (30 points) (Use the code you wrote on hw02.) Using the Vigenere cipher with keyword ENGLISH code the following message.

   Gadsby is a 1939 novel by Ernest Vincent Wright. The plot revolves around the dying fictional city of Branton Hills, which is revitalized thanks to the efforts of protagonist John Gadsby and a youth group he organizes. The novel is written as a lipogram and does not include words that contain the letter "e". Though self-published and little-noticed in its time, the book is a favourite of fans of constrained writing and is a sought-after rarity among some book collectors. Later editions of the book have sometimes carried the alternative subtitle 50,000 Word Novel Without the Letter "E". In 1968, the novel entered the public domain in the United States due to failure to renew copyright in the 28th year after publication. I think this is a stupid stunt. If you want to write a novel then just write a novel. I doubt it has literary merit. Its impressive that one can do it, but its not an impressive creation.