HW 1 CMSC 389. DUE Jan 3

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

1. (10 points) READ the syllabus- Content and Policy. READ my NOTES on line. 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. (0 points by VERY IMPORTANT). I emailed the entire class a message. I want to make sure that I have everyones email correctly. SO- if you GOT the message, write it down. If NOT then EMAIL Me your email address AS SOON AS POSSIBLE¿ (Email will be the main way I communicate with the class so its important I have all of your email addresses.)

3. (30 points) The following was coded by a shift cipher.

KVSMO KXNLY LVSUO DYOHM RKXQO WOCCK QOCDR KDOFO MKXXY DLBOK U

   (a) Which letters in the above ciphertext occurs the most times? Second most number of times? The third most number of times?

   (b) GUESS that the letter that occurs the most number of times decodes to an e. Use this to decode and see if it makes sense as a message. If it does then YOU ARE DONE. If not then try the second most. If that works then YOU ARE DONE. If not then try the third most.

4. (30 points) In this problem we work in mod 12.

   (a) Write down all of the numbers in $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ that are relatively primes to 12.

   (b) For each number in the first part write down its multiplicative inverse mod 12.

5. (30 points) Consider the equation $x^2 + 5x + 6 \equiv 0 \pmod{12}$. Find ALL of the x that satisfy this by plugging in EVERY $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ to see if its a root.

6. (0 points but you MUST do it to be able to do tomorrows assignment. So you really have the weekend to work on it, but you should get an early start.) Write programs that do the following (you will not be asked to turn them in but you will be asked to use them)

   (a) Given a plaintext, reformat it so that it is in groups of 5 letters.

   (b) Given a plaintext, and a shift s, output the text where all letters are shifted by s mod 26.

   (c) Given a plaintext, and numbers $a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ and $b \in \{0, 1, 2, \ldots, 25\}$ output the text where all letters L have $aL + b \pmod{26}$ applied to them.

(d) Given a ciphertext, output how often each letter appears.

(e) Given a ciphertext, find q_i, the relative freq of the ith letter.

(f) Given a ciphertext that you know was encoded with a linear cipher, find very good candidates for a, b such that the encoding was $f(x) = ax + b$. TEST it on texts that you generate.