HW 4 CMSC 389. DUE Jan 9

NOTE- THERE ARE TWO PAGES TO THIS ASSIGNMENT!!!!
NOTE- DO NOT HAND ME HARDCOPY. INSTEAD EMAIL THE TA
`michaelroberts94@gmail.com`
the hw. Any format fine, pdf prefered.
You MUST email it to him BEFORE 1:00 on Friday.

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

2. (0 points but you want to do this). Take all of the programs you've written for this course. Modify them as follows: (1) On inputting a text the first thing you do is remove all puncation and make all of the letters small letters, (2) consider the alphabet to be $\{a, b, c, \ldots, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and hence do operations mod 36 rather than mod 26, (3) break text into blocks of five.

3. (30 points) In this problem we use the affine cipher with $f(x) = 2x$ (YES, I know that 2 is not rel prime to 26)

   (a) Encode the message: *Discrete*

   (b) Take the encoded message. List all of the ways it can be decoded (there are more than one which is why it's BAD to take the a to NOT be rel prime to 26).

   (c) Give SOME way that the affine cipher can be modified so that it CAN work with any a. (there are many answers for this one question).

4. (30 points) You are given a text T that was coded by the Vigenere cipher. In the text you notice that the sequence *a9q* occurs with a in the 8th, 38th, 48th place. What are good guesses for the length of the key? (There is more than one good guess).

5. (30 points) Doctor Dogz has the following ideas to make ciphers MORE secure. For each one say if it makes it more secure or not. The notion of *more secure* is not a rigorous concept; even so, DISCUSS INTELLIGENTLY (you can't just say YES or NO). All math is mod 36 (with alphabet $\{a, \ldots, z, 0, \ldots, 9\}$).

(a) Let $f_1(x) = x + s_1$ and $f_2(x) = x + s_2$ be two shift ciphers. If we use $f_1(f_2(x))$ that will be more secure than either f_1 or f_2 alone!

(b) Let $f_1(x) = a_1x + s_1$ and $f_2(x) = a_2x + s_2$ be two affine ciphers (a_1, a_2 are rel prime to 36). If we use $f_1(f_2(x))$ that will be more secure than either f_1 or f_2 alone!

(c) Let $f_1(x) = a_1x^2 + b_1x + c_1$ and $f_2(x) = a_2x^2 + b_2x + c_2$. AND they are both 1-1 so both CAN be used for a cipher. If we use $f_1(f_2(x))$ that will be more secure than either f_1 or f_2 alone!

(d) Let f_1 code via a Vigenere cipher and let $f_2(x) = x + s$. If we take a text T and first apply f_1 to the text and then apply f_2 to what we get that will be more secure than f_1 alone! (I am not bothering saying it's more secure than f_2 alone since that is clearly true.)

(e) Let f_1 code via a Vigenere cipher and let $f_2(x)$ be a general substitution cipher. If we take a text T and first apply f_1 to the text and then apply f_2 to what we get that will be more secure than f_1 alone! (I am not bothering saying it's more secure than f_2 alone since that is clearly true.)