HW 2 CMSC 389. DUE Jan 7

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 but you REALLY WANT to do this so you can use it on HW03 and other later HWs) Write programs to do the following.

   (a) Given a word (could just be a sequence of letters) produce the corresponding sequence of numbers. For example, on input AND output (0,13,3).

   (b) Given a plaintext and a word:

   (c) i. Change all of the letters in the text to numbers.

      ii. Apply the Vigenere cipher to it using the word as the key.

   (d) Given a ciphertext and a word:

      i. Change all of the letters in the text to numbers.

      ii. Assuming that what you have was coded with the Vigenere cipher and that word as the key, recover what the plaintext was.

3. (40 points) (Use the code you wrote for hw01) Code the following passage with the affine cipher $f(x) = 7x + 13$ (the resulting text should be in blocks of five). NOTE- the passage has some numbers and some punctation. How did your program deal with that?

   The New York Times' James Risen reported that Snowden's decision to leak NSA documents "developed gradually, dating back at least to his time working as a technician in the Geneva station of the CIA." [113] Snowden first made contact with Glenn Greenwald, a journalist working at The Guardian, in late 2012. [114] He contacted Greenwald *anonymously as "Cincinnatus"[115] and said he had "sensitive documents" that he would like to share.[116] Greenwald found the measures that the source asked him to take to secure their communications, such as encrypting email, too annoying to employ. Snowden then contacted documentary filmmaker Laura Poitras in January 2013.[117] According to Poitras, Snowden chose to contact her after seeing her New York Times documentary[118] about NSA whistleblower William Binney. The Guardian reported that what originally attracted Snowden to both Greenwald and Poitras was a Salon article written by Greenwald detailing how Poitras' controversial films had made her a "target of the government."[116][119]*

4. (40 points) The following text was encoded with a shift cipher:

   znkhx ozoyn yzgzk oyvxk vgxkj zulux mobkn oyzux oigrn usuyk dagrg izyvx ubojo tmznk eckxk vkxlu xskjh egtgz outgr nkxug igjks oimog tzuxc uxrji ngtmo tmott ubgzu xznoy oyznk vurgx uvvuy ozkul znkiu xxkiz skyyg mkzax otmyn uarjh kluxm obktt uzhki gaykn kcgyg sujkx trkmk tjhaz hkiga yknkj ojghy urazk retuz notmc xut

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

   (b) Use that information to guess what the shift is (GUESS that the most common letter is e and from that you can guess the shif. If that does not work go to the next most common letter.) Test it by just looking at it (we did not go ovef how to have a computer do this). If its not correct, try again.

   (NOTE- this is NOT a trick question, I DID not make the passage something like *Watch Jeopardy, Alex Trebek's fun TV quiz game* or *The quick brown fox jumped over the lazy dog*

5. (10 points) Either find a quadratic polynomial $p(x) = x^2 + bx + c$ such that $p(x) \pmod{13}$ is 1-1 OR show that there is NO such polynomial.