HW 1 CMSC 389. DUE Jan 6

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

NOTE- THE HW IS TWO PAGES LONG

1. (0 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. (0 points but you REALLY WANT to do this so you can use it on HW02 and other later HWs) In this assignment you will end up with programs that (1) encode using shift, (2) encode using affine, (3) decode shift cophers, and (4) decode affine ciphers.

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

   (b) Given a text (don't care if its plaintext of ciphertext or whatever) translate into numbers via A goes to 0, B goes to 1, etc.)

   (c) Given a text of numbers, translate into letters via 0 goes to A, 1 goes to B, etc.

   (d) Given a plaintext, and a shift s,

   (e)
      i. Reformat into blocks of 5.
      ii. Change all of the letters to numbers.
      iii. Add s mod 26 to these numbers.
      iv. Change the numbers to letters and output the ciphertext.

   (f) Given a plaintext, and numbers $a, b \in \{0, \ldots, 25\}$

   (g)
      i. If a is NOT rel prime to 26 then output USER YOU ARE A STUPID. YOUR VALUE OF A IS NOT REL PRIME TO 26. If a is NOT rel prime to 26 then do the next steps.
      ii. Reformat into blocks of 5.
      iii. Change all of the letters to numbers.
      iv. For all of the numbers x find $ax + b \pmod{26}$.
      v. Change the numbers to letters and output the ciphertext.

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

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

(j) Given a ciphertext that you know was encoded with a shift cipher, (1) find very good candidates for the shift, and (2) test them using the summation method to determine which shift is correct.

(k) TEST it on texts that you generate.

(l) Given a ciphertext that you know was encoded with an affine cipher, (1) find very good candidates for a, b such that the encoding was $f(x) = ax + b$, and (2) test them using the summation method to determine which a, b is correct.

(m) TEST it on texts that you generate.

4. (30 points)

   (a) Vulcans use an alpabet of 30 letters. If they use an affine cipher of the form $f(x) = ax+b$ then what are the restrictions on a, b.

   (b) Klingons use an alpabet of 31 letters. If they use an affine cipher of the form $f(x) = ax+b$ then what are the restrictions on a, b.

   (c) Ferengi use an alphabet of 32 letters. If they use an affine cipher of the form $f(x) = ax+b$ then what are the restrictions on a, b.

5. (30 points) In this problem we work in mod 15.

   (a) Write down all of the numbers in $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ that are relatively prime to 15.

   (b) For each number in the first part write down its multiplicative inverse mod 15.

6. (30 points) Find all of the roots of $x^2 + 6x + 8 \equiv 0 \pmod{15}$. (NOTE- there are MORE THAN 2.)

7. (10 points) Either find a quadratic polynomial $p(x)$ and a number n such that $p(x) \equiv 0 \pmod{n}$ has at least 2015 roots OR show that no such can exist. In either case prove your result. (NOTE- my TA is NOT going to verify your poly for you.)