HW 3 CMSC 389. DUE Jan 7

NOTE- THIS HW IS TWO PAGES LONG.

1. (0 points) Write your name!
2. (20 points) Alice and Bob want to use the alphabet $\{a, b, c, \ldots, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Alice and Bob want to use a variant of the Playfair cipher that works with this alphabet.
   (a) Explain how the variant of the Playfair cipher for this alphabet works.
   (b) The keyword is *Vince*. Write down the square they need to tell them how to code pairs-of-letters.
   (c) With this key word Alice wants to send the message *CS 250 Rocks*. What does she send?
3. (20 points) Alice wants to use a Vigenere cipher with keyword *CAT*.
   (a) Present the tables for all the shift ciphers you will need.
   (b) Alice wants to send the sentence *Deal or no Deal*. What does she send?
4. (20 points) Alice and Bob want to use the alphabet $\{a, b, c, \ldots, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
   (a) Describe carefully how they would use a shift cipher.
   (b) For SHIFT BY 3 write the table that Alice uses to code the message.
   (c) Alice wants to send the message *CMSC 250 Rocks* She wants to use SHIFT BY 3. What does she send?
   (d) IF Alice and Bob wanted to use small letters, digits, and the symbols

   $$\{\pm, \div, \star, \vee, \bullet, \dagger, \cap, \wedge, \times, \cup, \oplus, \circ\}$$

   then what mod would the need to use?
   (e) Bill meets with Alice and Bob and says *Gee, if you only used one less symbol then the affine cipher would be easier to use.* Why is this?

5. (20 points) Eve intercepts a message that Alice send Bob. Eve knows that it used the Vigenere cipher. Eve tries to find the LENGTH of the key. She notes that the three word sequence $ABZG$ appears with A in the following places: 30, 105, 180. List ALL reasonable guesses for the key length.

6. (20 points) Alice and Bob want to use a variant of Vigenere where they code a sequence of Affine ciphers rather than a sequence of shift ciphers.

   (a) Alice and Bob first try to do this by having the key word by two keywords of the same length (like VINCE ZELLZ) and use the first one for the a needed for the affine cipher and the second one for the b (RECALL that affine ciphers map x to $ax + b \pmod{26}$.) Show that there are pairs of words for which this is a bad idea. Give such a pair and say WHY its a bad idea. MAKE SURE YOUR ANSWER IS COHERENT, CLEAR, AND SHORT.

   (b) Propose a way that Alice and Bob CAN easily have two words of the same length translate into a sequence of affine ciphers. MAKE SURE YOUR ANSWER IS COHERENT, CLEAR, AND SHORT.

   (c) Is this affine-vig cipher any more secure than the ordinary Vig-cipher? Discuss. MAKE SURE YOUR ANSWSER IS COHERENT, CLEAR, AND SHORT.