HW 4 CMSC 389. DUE Jan 9

NOTE- THIS HW IS TWO PAGES LONG.

THROUGH OUT THIS ENTIRE HW THE ALPHABET IS

$$\{a, b, c, \ldots, z, 0, 1, \ldots, 9\}$$

1. (0 points) Read the notes on Vigenere, Vigenere Plus, Playfair, autocode, and 1-time pad. 1-time pad is IMPORTANT to know before Monday's lecture, and there is a problem on it in this HW.

2. (15 points) (I did not do this in class- so READ THE NOTES on it.) Alice and Bob want to use a variant of the Playfair cipher that works with the alphabet

$$\{a, b, c, \ldots, z, 0, 1, 2, \ldots, 9\}.$$

   (a) (THROUGH OUT THIS ENTIRE HW THE ALPHABET IS

   $$\{a, b, c, \ldots, z, 0, 1, \ldots, 9\}$$

) Explain how the variant of the Playfair cipher for this alphabet works.

   (b) The keyword is *phong*. 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 389 rocks.

   What does she send?

3. (20 points) (THROUGH OUT THIS ENTIRE HW THE ALPHABET IS

   $$\{a, b, c, \ldots, z, 0, 1, \ldots, 9\}$$

) Alice wants to use a Vigenere cipher with keyword *2two*. Alice wants to send the sentence

   cs 389 rocks

   What does she send?

4. (15 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 four word sequence $ABZG$ appears with A in the following places: 30, 70, 140. List ALL reasonable guesses for the key length.

   (THERE IS ANOTHER PAGE!!!!!!!!!!!!!!!!!)

5. (20 points) (READ THE NOTES ON VIGENERE PLUS) 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 be two keywords of the same length (like JUSTIN GRADES) 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 $ax+b \pmod{36}$ because our alphabet is $\{a \ldots, z, 0, \ldots, 9\}$. 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 ANSWER IS COHERENT, CLEAR, AND SHORT.

6. (15 points) (I did not do this in class- so READ THE NOTES on it.) Alice and Bob are going to use a 1-time pad. They use the key 0111100001100

   (a) Alice wants to send 0000. What does she send?

   (b) Bob wants to reply 111111. What does he send?

   (c) After Alice and Bob have send these messages, what is the length of the longest message Alice can then send?

7. (15 points) (I did not do this in class- so READ THE NOTES on it.) Alice and Bob are doing to use the autocode with key 8. Alice wants to send

   cs 389 rocks

   What does she send?