HW 5 CMSC 456. Morally DUE Oct 19
NOTE- THE HW IS FIVE PAGES LONG

1. (0 points)

   (a) What is the day and time of the midterm?

   (b) What is the day and time of the final?

   (c) What is the dead-cat policy?

   (d) NOTE: I am no longer going to put GOTO THE NEXT PAGE on every page. So MAKE SURE TO DO ALL OF THE PROBLEMS!!!!!!!!!

2. (25 points. BASED ON SLIDES on Other Ciphers.) The Daleks have a 12 letter alphabet $\{a, b, c, d, e, f, g, h, i, j, k, l\}$. They want to use a Playfair Cipher but *they do not want to add or subtract letters to their alphabet!* They really want to use their 12 letters. Describe a variant of the Playfair cipher that they can use and give examples of how to code all possible 2-letter sequences. Use keyword FBI.

3. (25 points, BASED ON SLIDES on Randomized Shift) Alice and Bob use a randomized shift cipher with function :

   $f(r) = 11r + 5$.

   They do not have a good random number generator, so they use $i \pmod{26}$ to code the ith letter. So, for example, if they want to code

   Zan

   They would use random numbers 1,2,3 and hence shifts $11 \times 1 + 5 \equiv 16 \pmod{26}$, $11 \times 2 + 5 \equiv 1 \pmod{26}$, and $11 \times 3 + 5 \equiv 12 \pmod{26}$.

   Alice wants to send Bob the following:

   The Abel Prize is the Nobel Prize for Math!

   What do they send?

   (You can write a program for this or do it by hand. You DO NOT need to show your work.)

4. (25 points) (NOT BASED on any particular slides.) Alice and Bob are using the Gen Sub Cipher. The alphabet is $\{a, \ldots, z\}$. Alice sends Bob a LONG NORMAL TEXT T. Alice will, as usual, break up their text into blocks-of-5 and get rid of all punctuation.

   Eve of course knows they are using the Gen Sub Cipher and that they do blocks-of-5 and no punctuation.

   Eve also knows that their text T will have the following phrase in it:

   Pack my box with five dozen liquor jugs

   Note that this is a 32-letter sentence which contains all the letters of the alphabet, and

   8th and 19st and 27th letter are the same.

   11th and 15th and 24th letter are the same.

   17th and 21st letter are the same.

   26th and 30th letter are the same.

   NO other letters are the same.

   And now finally our problem: Describe how she can use the presence of that phrase to to crack the cipher.

5. (25 points) (BASED on slides on Randomized Shift.)

   Assume the usual alphabet $\{a, \ldots, z\}$ and the usual coding into numbers a is 0, ..., z is 25.

   In class we described a *randomized shift cipher*.

   Describe a *randomized affine cipher*. Include:

   (a) (5 points) What the key is.

   (b) (7 points) How to encrypt a text $t_1, \ldots, t_N$.

   (c) (8 points) Do a small example of our encryption by encrypting the word BOOK. IF you need a sequence of random numbers then use the sequence of odd numbers 1,3,5,7,...,23,25,1,3,....

   (d) (5 points) How to decrypt a text $c_1, \ldots, c_N$.