HW 3 CMSC 456. Morally DUE Oct 5
NOTE- THE HW IS FIVE PAGES LONG

1. (0 points)
   (a) What is the day and time of the midterm?
   (b) IF you CANNOT make the day and time of the TIMED midterm let me know ASAP (AS SOON AS POSSIBLE).
   (c) What is the day and time of the final?
   (d) What is the *dead-cat policy*?
   (e) What is the *mask policy*?

2. (30 points) For this question, use $A = 0, B = 1, ..., Z = 25$ where applicable.

   (a) (6 points) Give a 3×3 matrix M that CAN be used for the Matrix Cipher. Say WHY it is usable.

   (b) (6 points) Apply your matrix M to the plaintext FBI and output the three LETTERS that you get.

   (c) (6 points) Give a 3×3 matrix N that CANNOT be used for the Matrix Cipher. Say WHY it is NOT usable.

   (d) (6 points) Apply your matrix N to the plaintext FBI and output the three LETTERS that you get.

   (e) (6 points) Note that even though N CAN be used to encode a string, it CANNOT be used in the matrix cipher. Why is that? (NOTE- a student pointed out that this is really the same as question c. So you can just say SEE ANSWER TO c. Though make sure to get c right.)

3. (30 points) Recall that there were two different brute force attacks on the matrix cipher: (a) look at every single matrix, (b) look at rows one at a time. In this problem we will compare the two carefully (no big-O). We abbreviate *nanoseconds* with *nsecs*

   Assume that

   - Testing if an $n \times n$ matrix is invertible takes an^3 nsecs.
   - The IS-ENGLISH program on a text of length m takes bm nsecs.
   - The number of $n \times n$ matrices that are invertible is $c26^{n^2}$. (Note that $c < 1$.)
   - Appying an $n \times n$ matrix to a vector of length n takes dn nsecs.
   - The dot product of two length n vectors takes en nsecs. (Note that e is NOT the e from calculus.)

   So far this is all stuff you need for the questions. The QUESTIONS are on the next page.

(a) (10 points) How many nsecs does the brute force algorithm (the one that looks at every $n \times n$ matrix) take to crack the $n \times n$ matrix cipher if you have a text of length m? The answer should be in terms of a, b, c, d, e, n, m and NOT have any O-of terms. (You can assume that n divides m.)

(b) (0 points) Assume $a = b = d = e = 2$ and $c = \frac{1}{2}$. Assume that a code is feasible to crack if it takes ≤ 5 hours to crack it. Assume that the text is of length n^2 (so $m = n^2$). What is the smallest n such that the brute-force-matrix code is NOT feasible to crack.

(c) (15 points) How many nsecs does the brute force algorithm (the one that looks at one row at a time) take to crack the $n \times n$ matrix cipher if you have a text of length m? The answer should be in terms of a, b, c, d, e, n, m and NOT have any O-of terms. (You can assume that n divides m.)

(d) (5 points) Assume $a = b = d = e = 2$ and $c = \frac{1}{2}$. Assume that a code is feasible to crack if it takes ≤ 5 hours to crack it. Assume that the text is of length n^2 (so $m = n^2$). What is the RANGE of n such that both (a) the brute-force-matrix attack is NOT a feasible attack, but (b) the brute-force-row attack IS a feasible attack.

(e) (0 points- I have some ideas here, lets see if you do also!) What can you do to speed up either algorithm?

(f) (0 points- I was unable to find the answers to this on the web but would be delighted if you do- and if so email me as well as write it down.) Find REAL values for a,b,c,d,e.

(g) (0 points. Only do if you did the last item). Use the REAL values for a, b, c, d, e. Assume that a code is feasible to crack if it takes ≤ 5 hours to crack it. Assume that the text is of length n^2 (so $m = n^2$). What is the RANGE of n such that both (a) the brute-force-matrix attack is NOT a feasible attack, but (b) the brute-force-row attack IS a feasible attack.

4. (40 points) Eve knows that Alice and Bob are using a 3×3 matrix cipher.

   (a) (20 points) Eve knows from yesterdays message and what happened that

   FDR is coded as WHH

   Write down the equations that Eve will obtain to help her crack the cipher. (You do not have to solve them, and actually you can't.)

   (We assume A is 0, B is 1, and the math is mod 26.)

   (b) (20 points) How many plaintext-ciphertext pairs does Eve have to know in order to crack the cipher?

   (c) (0 points) Assume Eve uses an $n \times n$ matrix code. How many plaintext-ciphertext pairs does Eve to have know in order to crack the cipher?

   (d) (0 points) Assume Eve has one less plaintext-ciphertext than she needs to crack the cipher. Can she still, with some cleverness and guesswork, crack the cipher?