HW 3 CMSC 456. Morally DUE Oct 5
SOLUTIONS
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.

   SOLUTION

   (This is Bill G) I went to the web and googled

   calculate a determinant

   and got to

   `https://matrix.reshish.com/determinant.php`

   I then guessed a few detemrinants until I got one whose det was rel prime to 26.

$$\begin{pmatrix} 1 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{pmatrix}$$

   had det -3 which is rel prime to 26.

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

   SOLUTION

   F is 5

   B is 1

   I is 8

$$\begin{pmatrix} 1 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{pmatrix} \begin{pmatrix} 5 \\ 1 \\ 8 \end{pmatrix}$$

   The entries are:

   $1 \times 5 + 1 + 2 \times 8 = 22 \equiv 22 \pmod{26}$

   $3 \times 5 + 4 + 5 \times 8 = 15 + 4 + 40 \equiv 19 + 14 \equiv 33 \equiv 7 \pmod{26}$

   $6 \times 5 + 7 + 8 \times 8 = 30 + 7 + 64 \equiv 4 + 7 + 12 \equiv 24 \pmod{26}$

   22 is W

   7 is H

   24 is Y

So FBI maps to WHY.

(No, I did not plan that!)

END OF SOLUTION

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

SOLUTION

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Since the det is not rel prime to 26 there will be two strings that map to the same string. Hence the decoding is not unique. We will give an example in the next question.

END OF SOLUTION

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

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 5 \\ 1 \\ 8 \end{pmatrix}$$

The entries are:

$5 + 1 + 8 = 14$

$5 + 1 + 8 = 14$

$5 + 1 + 8 = 14$

So we get OOO (thats three oh's, not three zeros).

NOTE that any (a, b, c) such that $a+b+c = 14$ will map to OOO, Hence

$(7, 7, 0)$ also maps to OOO.

Hence OOO cannot be uniquely decoded.

(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?

As noted above, even though ENCODING has no problems, DECODING has issues.

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, n, m and NOT have any O-of terms. (You can assume that n divides m.)

SOLUTION

You have to to look at 26^{n^2} matrices.

For each one you have to test if they are invertible, which takes an^3. So thats $an^3 26^{n^2}$.

For each of the $c26^{n^2}$ matrices M that are invertible you have to apply M to the text and apply IS-ENGLISH.

- The text is of length m and can be viewed as $\frac{m}{n}$ blocks of length n. Hence we apply M to a vector $\frac{m}{n}$ times. This takes $\frac{m}{n}dn = dm$ nsecs.
- IS-ENGLISH takes bm steps.
- Hence this takes $c26^{n^2}(dm + bm) = (d + b)mc26^{n^2}$ nsecs.

Putting this all together we get

So thats $an^3 26^{n^2} + (b + d)mc26^{n^2} = (an^3 + bmc + dmc)26^{n^2}$ nsecs.

END OF SOLUTION

(b) (0 points) Assume $a = b = c = d = e = 2$. 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, n, m and NOT have any O-of terms. (You can assume that n divides m.)

SOLUTION

There are n rows. For each row there are 26^n possbilities. We will be doing the following for each guess of each row, so we mulitply the time for the following by $n26^n$:

Multiply the row by each of the $\frac{m}{n}$ block of length n. This takes $\frac{m}{n}en = em$ steps.

Apply IS-ENGLISH to every rth letter that was decoded by the rth row. This takes $b\frac{m}{n}$ nsecs.

Hence the entire process takes $(en + b)m26^n$ nsecs.

END OF SOLUTION

(d) (5 points) Assume $a = b = c = d = e = 2$. 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.

SOLUTION

OMITTED

END OF SOLUTION

(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.)

   SOLUTION

   Assume matrix is:

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

   Note that FDR is 5,3,17.

   Note that WHH is 22,7,7.

   Hence the equations are

   $5a + 3b + 17c = 22$

   $5d + 3e + 17f = 7$

   $5g + 3h + 17i = 7$

   END OF SOLUTION

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

   SOLUTION

   Each pair gives 3 equations. Since there are 9 variables we need 9 equations. Hence we need 3 pairs.

   END OF SOLUTION

   (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?