HW 2 CMSC 389. DUE Jan 6

WARNING- THIS IS TWO PAGES LONG SO DON"T MISS SECOND PAGE

1. (0 points) What is your name? Write it clearly. Staple your HW. What is the day and time of the first midterm? Are you free then? (if not then SEE ME IMMEDIATELY) What is the day and time of the second midterm? Are you free then? (if not then SEE ME IMMEDIATELY) When is the final? Are you free then? (if not then SEE ME IMMEDIATELY)

2. (10 points) Let A be the following matrix.

$$\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 8 \end{pmatrix}$$

   Use this matrix to encode the following topic for this course (I abbreviated it so that it's not so hard to do.)

   Quad Sieves

3. (50 points)

   (a) Alice has a clever idea to INCREASE the security of the linear cipher. She will FIRST apply one linear function f_1 and THEN another one f_2. Is this more secure than the usual linear cipher?

   (b) Alice has a clever idea to INCREASE the security of the matrix cipher. She will FIRST apply a 2×2 matrix M_1 and THEN a 4×4 matrix M_2. Is this more secure than the 4×4 matrix cipher?

   (c) Alice has another clever idea to INCREASE the security of the matrix cipher. She will FIRST apply a 2×2 matrix M_1 and THEN a 3×3 matrix M_2. Is this more secure than 3×3 matrix cipher?

4. (40 points) Suppose you are GIVEN a text that you know is coded by shift (or linear or ...). In class we discussed the problem of decoding it. In this problem we explore what happens if you are GIVEN a long text T and its decoding T', and another text S that you NOW want to decode.

   (a) You are given a text T that you are told was created by a linear cipher. You are also GIVEN the text T' that it came from. You are then given S and told it used the same linear function. How do you decode S? (This should be EASIER than the technique to just decode S not given T, T'.)

   (b) You are given a text T that you are told was created by a 20×20 matrix cipher. You are also GIVEN the text T' that it came from. You are then given S and told it used the same shift. How do you decode S?

5. (0 points for now- I will ask you to hand it in later in the semester, but SOON. DO IT NOW so we can discuss it in class.) You will use the programs you wrote that I put into hw01 for this problem. There is a text on the course website next to where this hw is posted.

   (a) Encode that text using the linear cipher $f(x) = 3x + 1$.

   (b) Try to decode the text. In particular, for all ordered pairs (x, y) where $x, y \in \{0, 1, 2, \ldots, 25\}$ and x is rel prime to 26, compute the appropriate quantity, check for which (x, y) the quantity is highest, and try those out. (There should be only one.) That will yield the correct (a, b), namely $(3, 1)$.