HW 2 CMSC 389. DUE Jan 6
SOLUTIONS

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?

   SOLUTION TO PROBLEM THREE

   a) NO- if you compose two linear ciphers you get a linear cipher.

For the next two problems, if A is a square matrix, then let c_A be the associated cipher; and for each n, let I_n be the $n \times n$ identity matrix.

b) NO- Let A be a 2×2 matrix and let B be a 4×4 matrix. Let A^* be the 4×4 block matrix $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$. Then $c_A = c_{A^*}$, that is, if you encode a text using A, that's the same as encoding it using A^*. Hence $c_A \circ c_B = c_{A^*} \circ c_B = c_{A^*B}$, i.e. applying A and then B is the same as applying the 4×4 matrix A^*B

c) YES- we want to show that the set

$C_{2\times 2-3\times 3} := \{c_A \circ c_B : A \text{ is } 2 \times 2 \text{ and invertible, } B \text{ is } 3 \times 3 \text{ and invertible}\}$

strictly contains the set

$$C_{3\times 3} := \{c_B : B \text{ is } 3 \times 3 \text{ and invertible}\}.$$

But given $c_B \in C_{3\times 3}$, note that $c_B = c_{I_2} \circ c_B \in C_{2\times 2-3\times 3}$, and if A is 2×2, invertible and not the identity, then $c_A \circ c_{I_{3\times 3}} \in C_{2\times 2-3\times 3} \backslash C_{3\times 3}$.

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?

SOLUTION TO PROBLEM FOUR

ALL $\equiv$ are mod 26.

a) We just do an example. Lets say we note that 3 maps to 7 and 12 maps to 11. We want a, b such that if $f(x) \equiv ax + b$ then $f(3) \equiv 7$ and $f(12) \equiv 11$.

$f(3) \equiv 7$: $a \times 3 + b \equiv 7$

$f(12) \equiv 11$: $a \times 12 + b \equiv 11$.

$3a + b \equiv 7$

$12a + b \equiv 11$

Subtract to get

$-9a \equiv 4$

$9a \equiv -422$

KEY1: $-4 \equiv 22$. So

$9a \equiv 22$

KEY2: 9 HAS an inverse mod 26. We'll do this by brute force and find that its 3. So mult both sides by 3

$3 \times 9a \equiv 3 \times 22$

$a \equiv 66 = 66 - 52 = 14$.

GREAT we have a.

What about b?

$b \equiv 7 - 3a \equiv 7 - 3 \times 14 \equiv 7(1 - 3 \times 2) \equiv 7(1 - 6) \equiv 7 \times -5 \equiv -35 \equiv 52 - 35 \equiv 17$.

(I took all of these steps to avoid doing hard multiplications. It could be shorter.)

KEY- This WORKED since 9 had an inverse mod 26. More generally you will get a set of 2 equations in 2 variables. How to solve them- The SAME way you normally solve such a system. You can add, subtract, multiply mod 26. What about division? You CAN"T always do this, but in the cases that arise you will be able to divide (actually find inveses). Why? It seems like a cirular argument- since there IS a solution you will find it. (For now just take my word for this.)

b) This is simlar to part a, though I won't do an example. Let A be the matrix. We do not know what it is. It has 400 entries, all variables (things like x_{ij}).

By applying A to the first 20 elements of the plaintext you get the first 20 elements of the ciphertext. This gives you ONE linear equation in 20 variables. Then apply A to the next 20 elements to get another equation. If the text is 400 characters or more you will be able to get 20 equations in 20 variables. This can be solved using the usually methods though over mod 26. Much like part a, there will be a solution so you'll find it without running into numbers that you need inverses of but can't find them.

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 $(3, 1)$.