HW 1 CMSC 389D. DUE Jan 4
SOLUTIONS
NOTE- THE HW IS FOUR PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. READ my NOTES on ciphers. What is your name? Write it clearly. Staple your HW. What is the day and time of the first midterm? When is the final?

2. (0 points VERY IMPORTANT). I emailed the entire class a message. I want to make sure that I have everyone's email correctly. SO - if you GOT the message, write it down. If NOT then EMAIL me a message as soon as possible. It can be blank. MY email is *gasarch@cs.umd.edu* (Email will be the main way I communicate with the class so it's important I have all of your email addresses.)

3. (15 points) In the affine cipher $f(x) = ax + b \pmod{26}$ should $a = 0$ be allowed? Why or why not?

   SOLUTION TO PROBLEM THREE

   NO $a = 0$ should not be allowed. The function $f(x) = b$ is not invertible.

4. (10 points) (In this problem we do not allow $a = 0$ for the affine cipher.) Vulcans use an alphabet of 40 letters. They want to use an affine cipher of the form $f(x) = ax + b$. Fill in the following _____below:

   The values of $\boldsymbol{a}$ *they may use are in the set* _____. *They need to use just these values since if they use something NOT in* _____*then* _____.

   NOTE- DO NOT say something like 'the squares less than 40" Actually LIST out the set of a's that are allowed.

   SOLUTION TO PROBLEM FOUR

   The values of a they may use are in the set of numbers in $\{1, \ldots, 39\}$ *that are relatively prime to 40 (I give the set below). They need to use just these values since if they use something NOT rel prime to 40 then* $f(x) = ax+b$ *will not be invertible, so you cannot decode uniquely.*

   The actual set is

   $\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$

GO TO NEXT PAGE

5. (15 points) Alice and Bob want to make their cipher more secure. By this they mean that there are more possibilities for Eve to go through if she uses a brute force search. For each proposal below say whether it would increase security relative to the cipher they started with. (We omit the mods in this problem but they are there!)

   (a) Alice and Bob want a cipher that is more secure than a shift. Alice comes up with a shift function $f(x) = x + s_1$. Bob comes up with a shift function $g(x) = x + s_2$. They think that $f(g(x))$ is MORE secure than either f or g. Are they correct? (We assume that f and g are bijections so $f(g(x))$ is also.)

   (b) Alice and Bob want a cipher that is more secure than an affine. Alice comes up with an affine function $f(x) = a_1x + b_1$. Bob comes up with an affine function $g(x) = a_2x + b_2$. They think that $f(g(x))$ is MORE secure then either f or g. Are they correct? (We assume that f and g are bijections so $f(g(x))$ is also.)

   (c) Alice and Bob want a cipher that is more secure than quadratic. Alice comes up with a quadratic function $f(x) = a_1x^2 + b_1x + c_1$. Bob comes up with a quadratic function $g(x) = a_1x^2 + b_2x + c_2$. They think $f(g(x))$ is MORE secure then either f or g. Are they correct? (We assume that f and g are bijections so $f(g(x))$ is also.)

SOLUTION TO PROBLEM FIVE

a) NO increase in security since the composition of two shift functions is a shift function.

b) NO increase in security since the composition of two affine functions is a shift function.

c) YES there is an increase in security. The composition of two quadratics is a quartic which has more coefficients to guess.

GO TO NEXT PAGE

6. (35 For this problem we assume the 15-letter alphabet $\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o\}$.

   (a) (5 points) Alice and Bob are going to use the *Keyword Shift Cipher*. They are going to use keyword *bill*. Write down the encoding table.

   (b) (5 points) Use this table to encode *I am a lion*

   (c) (5 points) Alice and Bob are going to use the *Keyword-Mixed Cipher*. (Use that $15 = 5 + 5 + 5$.) They are going to use keyword *bill*. Write down the encoding table.

   (d) (5 points) Use this table to encode *I am a lion*

   (e) (5 points) (You will need to look up Playfair Cipher. The Wikipedia entry is a good place.) Alice and Bob are going to use the *Playfair Cipher*. They are going to use keyword *bill*. Write down the 5×5 encoding block.

   (f) (5 points) Using this block to encode *I am a lion*

   (g) (5 points) Rank *Keyword Shift Cipher*, *Keyword Mixed Cipher, and* Playfair cipher *in terms of security. Hint: There is no one right answer. You need to give an intelligent argument for your ranking. Ties are also allowed.*

SOLUTION TO PROBLEM SIX

Parts a,b,c,d,e,f all omitted.

Part g: I give several answers

- They are all equally tied for security. If you assume Kerschoff's principle the enemy knows what kind of cipher you are using. Since it all cases the key is a word or phrase in English, hey are equally hard.
- Playfair is harder. Since replaces 2 letters by 2 letters the freq analysis is harder since you need to look at the freq of pairs. The other two are about the same.
- Keyword-Mixed is more secure than Keyword-Shift since with the keyword shift the latter letters tend to map to the latter letters so the search space is not as big.

7. (15 points) Alice and Bob are going to use the Vig cipher. The keyword is Sina. They want to send *Gradescope is okay* What do they send?

GO TO NEXT PAGE

8. (10 points) Eve is going to use Brute Force (she does not know about Freq analysis). Alex thinks he has a substitution cipher (so every letter goes to a letter, like shift, affine, quadratic, general) that is MORE secure than the general sub cipher! Here is his idea:

   Pick 100 random coefficients $a_{99}, \ldots, a_0 \in \{0, \ldots, 25\}$. Let

   $$f(x) = a_{99}x^{99} + \cdots + a_1 x + a_0 \pmod{26}$$

   Use this to encode a letter. There are $26^{100} > 26!$ possible polynomials. Hence there is a bigger space for Eve to search.

   Is Alex right? Explain.

   SOLUTION TO PROBLEM EIGHT

   Alex is wrong (note- this is NOT the Alex who TAs this course). There are only 26! possible maps from the letters to themselves. Hence of those 26^{100} polynomials many of them compute the same function.

9. (For fun, not for points, and don't hand in) Find ALL a, b such that the function $f(x) = ax^2 + bx \pmod{10}$ is a bijection. Try to do this with Math, not with a program. The notes give you a head start.

10. (For Fun, not for points, and don't hand in). Look up permutation polynomials on the web and see if you can characterize all cubics that are bijections over $\{0, \ldots, 25\}$ mod 26.