

HW 1 CMSC 389D. DUE Jan 4

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?
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 followingbelow:

The values of a they may use are in the set They need to use just these values since if they use something NOT inthen

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

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 than 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 $g(x) = a_2x^2 + b_2x + c_2$. They think $f(g(x))$ 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.)

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.*
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 P**

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 $a_{99}, \dots, a_0 \in \{0, \dots, 25\}$. Let

$$f(x) = a_{99}x^{99} + \dots + a_1x + a_0 \pmod{26}$$

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.

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 $\{0, \dots, 25\} \pmod{26}$.