HW 1 CMSC 456. DUE Sep 10
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?

2. (15 points) Vulcans use an alphabet of 21 letters. They want to use an affine cipher of the form $f(x) = ax + b$. Fill in the following _____below:

   The values of **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 TWO

   The values of a they may use are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

   This is the set of primes in $\{1, \ldots, 21\}$ that are relatively prime to 21.

GO TO NEXT PAGE

3. (25 points) (READ ON YOUR OWN about the Keyword Cipher from my notes) (READ ON YOUR OWN about the Keyword-Mixed Cipher from my notes) 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 *jacob* and shift 1. Write down the encoding table. Write down the decoding table. Show all steps. Both table should be in order $a, b, c, \ldots, o$.

   (b) (5 points) Use this table to encode *FBI good, CIA bad* (NOTE- end result should be in blocks of 5 and all in Capitol letters. (NOTE- the sentence was used because it uses only letters in $\{a, \ldots, o\}$ and does not reflect the opinion of the professor or the TA's.)

   (c) (5 points) Alice and Bob are going to use the *Keyword-Mixed Cipher*. (Use that $15 = 5 + 5 + 5$, so have three rows of letters) They are going to use keyword *jacob*. Write down the encoding table.

   (d) (5 points) Use this table to encode *FBI good, CIA bad*

   (e) (5 points) Discuss the PROS and CONS of both the *Keyword Shift Cipher* and the *Keyword Mixed Cipher*.

SOLUTION TO PROBLEM THREE

a) First we write down the letters in $\{j, a, c, o, b\}$ and then the letters in $\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o\}$.

$j, a, c, o, b, d, e, f, g, h, i, k, l, m, n$

We then write this down along with the shift of 1 in this order

ENCODE:

j	a	c	o	b	d	e	f	g	h	i	k	l	m	n
a	c	o	b	d	e	f	g	h	i	k	l	m	n	j

We then put this in order:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
c	d	o	e	f	g	h	i	k	a	l	m	n	j	b

DECODE: First I just swap the two rows:

c	d	o	e	f	g	h	i	k	a	l	m	n	j	b
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o

We then put this in order:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
j	o	a	b	d	e	f	g	h	n	i	k	l	m	c

b)

FBI good, CIA bad

I will first change to the encoding keeping the spacing so I can check my work. I will then put it into blocks of 5.

gdk hbbe okc dce

gdkhb beokc dce

c) As in part a, we first write the letters with j,a,c,o,b and then the rest:

$j, a, c, o, b, d, e, f, g, h, i, k, l, m, n$

We then write these in three rows of five

j	a	c	o	b
d	e	f	g	h
i	k	l	m	n

We get table by reading it off column by column for where things code to:

ENCODE:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
j	d	i	a	e	k	c	f	l	o	g	m	b	h	n

DECODE: I first swap the two rows:

j	d	i	a	e	k	c	f	l	o	g	m	b	h	n
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o

And now I put them in order:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
d	m	g	b	e	h	k	n	c	a	f	i	l	o	j

d) Omitted.

e) I give several answers

BOTH:

- CON: Can be cracked by either freq analysis.
- CON: Can be cracked by Eve going through English words or phrases.
- PRO: Easy to use.

Keyword-shift

CON: Not that random-looking since letters towards the end of the alphabet tend to map to letters at the end of the alphabet.

Keyword-mixed

PRO: From a short string like *jacob* you get a very random-looking cipher. So it has the short-key advantage of Shift, with the random-looking adv of general sub.

GO TO NEXT PAGE

4. (30 points) PROGRAMMING ASSIGNMENT.

   (a) (6 points) Write a program that does the following:

   Input: A text T of English and a number b

   Output: That text with with punctuation removed, all letters small, and in blocks of size b, except that the last block can be shorter. (If there are numbers just you do not need to change them to anything. There is no thing as a lower case number!)

   Submit your program with the HW- Not on the Submit Server or anything else.

   (b) (6 points) *[YOUR FULL NAME] is taking [SOME CLASS YOU ARE TAKING THAT IS NOT CMSC/MATH 456] and loving it! The teacher is [INSERT TEACHER HERE]*

   with $b = 5$.

   For example, Jacob could run the program on

   Jacob Prinz is taking PHYS 402 and loving it! The teacher is Theodore Jacobson.

   Submit both your input and your output.

   (c) (6 points) Write a program that on input a text T in English (which could be long) and a number b AND a numbers $s \in \{0, 1, \ldots, 36\}$ does the following:

   Input: A text T of English and a number b

   Output: That text **shifted by** s with with punctuation removed, all letters small, and in blocks of size b, except that the last block can be shorter. **Submit your program with the HW- Not on the Submit Server.**

   (d) (6 points) Run the program on the same text you did in Part b, with $s = 13$.

   Submit both your input and your output.

   (e) (6 points) Find some text T on the web that is between 1/2 a page and a page and

   i. Run your first program on it with $b = 5$.

   ii. Run your second program on it with $b = 5$ and $s = 27$

   In both cases submit your input and your output.

GOTO NEXT PAGE

5. (15 points) Alice and Bob are going to use the Vig cipher. The keyword is bill. They want to send *Gradescope is okay* What do they send? (You can either (1) do this by hand, (2) write a program to do it for you, or (3) find software on the web to do it for you. Let us know which one you did. If (3) then give us the website where you found it and say if the answer leaked information.)

   SOLUTION TO PROBLEM FIVE

   I did option (3).

   I used `https://www.dcode.fr/vigenere-cipher`

   to obtain:

   Hzlofanzqm td pslj

   The spacing is the same in the input and the output. This leaks information.

6. (15 points) Goto the website:

   `http://rumkin.com/tools/cipher/caesar.php`

   (It is also on the course website under NOTES so you can click it there.)

   (a) Using a shift of 3 type in:
   CMSC 456 Rocks! Or does it?
   What does it return?

   (b) Name several things this program does that will leak information (aside from using the shift cipher in the first place).

   SOLUTION TO PROBLEM SIX

   That website takes

   CMSC 456 Rocks! Or does it?

   with shift 3 and outputs

   FPVF 456 Urfnv! Ru Grhv lw?

   It leaks information:

   1) It leaves numbers un coded so that 456 is 456

   2) It keeps spacing in so I can tell that the first word is four letters

   3) It keeps caps and small letters as caps and smalls, so I can tell the first word is all caps.

4) It keeps punctuation so I can tell the last part is a question. Also, the writer is very excited about the first part!

7. (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 of $\mathbb{Z}_{26}$.