HW 00 CMSC 456. SOLUTIONS

1. (0 points)
   (a) READ the Syllabus! The ENTIRE thing.
   (b) What is the day and time of the take home part of the midterm?
   (c) What is the day and time of the timed part of the midterm?
   (d) What is *the dead-cat policy*?
   (e) Why is is called *the dead-cat policy*?
   (f) What is the *Mask Policy*?

2. (0 points)
   (a) Learn Python 3 and write some simple programs in it.
   (b) Write a program in Python 3 that does the following: input is two vectors of reals of the same length, and output is their dot product.
   (c) Write a program in Python 3 that does the following:
   Input is a text T of English (our intention is that T be a normal English text, like a short article from Wikipedia).
   (1) eliminate all punctuation, numbers, and whitespace,
   (2) replace a and A with 1, ..., replace z and Z with 26.
   EXAMPLE: On input *I'm Bill* the output is *9 13 2 9 12 12*.
   NOTE: We use $\{1, \ldots, 26\}$ not $\{0, \ldots, 25\}$.

3. (0 points) Given a, b we want to find if $a^{-1} \pmod b$ exists, and if it does we want to find it.
   (a) Look up *The Euclidean Algorithm* which is for this problem.
   (b) Code up the algorithm (it will be used in many later assignments).

GOTO NEXT PAGE

4. (0 points)

   (a) Learn LaTeX and write some simple documents in it.

   (b) Write a LaTeX document that summarizes the lecture on the Shift Cipher. Note that you will need to typeset some mathematics.

5. (0 points) Alice and Bob use a 26-letter alphabet. Alice and Bob are going to use the shift cipher. Bob has an idea! Bob says they should pick s so that the encode-key and the decode-key are the same!

   (a) List all s so that the encode-key and the decode-key are the same.

   SOLUTION

   All $\equiv$ are mod 26.

   We need

$$(x+s)+s \equiv x$$

$$x+2s \equiv x$$

$$2s \equiv 0$$

   So $s \equiv 0$ or $s \equiv 13$.

   END OF SOLUTION

   (b) Give a reason why Bob's idea is a good idea.

   SOLUTION

   Once Alice gives Bob s, Bob does not have to figure out the inverse shift.

   END OF SOLUTION

   (c) Give a reason why Bob's idea is a bad idea.

   SOLUTION

   Normally the set of all s is of size 26.

   If the encode-key and decode-key are the same then there are only 2 possible s's. Hence this shift will be easier to crack.

   END OF SOLUTION

6. (0 points) Read Vannevar Bush's paper from July 1945:

   `http://web.mit.edu/STS.035/www/PDFs/think.pdf`

   Write down three predictions in made that came true.

   (Note- this is not a paper in crypto but it is such a good paper that every undergraduate should read it!)

   SOLUTION

   (a) Much faster computers.

   (b) Computers being used by individual people. In his time most computers were used by either scientists or businesses.

   (c) What he called the Memex we would now think of as a cell phone without the phone part.

   END OF SOLUTION