HW 2 CMSC 389. DUE Jan 5
SOLUTIONS
WARNING- THE HW IS THREE PAGES LONG!!!!!!!!!!!! MUST USE GRADESCOPE
Note: When you submit your assignment on Gradescope, make sure to assign each question to its corresponding page(s). This can be done by clicking on the question on the left side and clicking on its page on the right.

1. (0 points) Write your name! READ cipher and english notes.
2. (30 points) Vulcans use the alphabet $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The frequencies are

   - $P(1) = .05$
   - $P(2) = .05$
   - $P(3) = .05$
   - $P(4) = .05$
   - $P(5) = .05$
   - $P(6) = .1$
   - $P(7) = .15$
   - $P(8) = .25$
   - $P(9) = .25$

   Alice and Bob are Vulcans that want to use the shift cipher. Carol is a Vulcan who finds their message and knows that it used the shift cipher. For this problem you may assume you have the following programs:

   - $FREQ(T)$: on input T this returns $\vec{F} = (F(1), \ldots, F(9))$, the vector of frequencies of the letters in T.
   - $SHIFT(T, s)$: on input T and shift s, returns T shifted by s.
   - $DOT(a, b)$: on input vectors a, b of the same length (it will always be 9) output the dot product.
   - P- the vector above of freq in real Vulcan.

GOTO NEXT PAGE

(a) I want to ask the question: *Write psuedocode for a program IS-VULCAN that will, given a document, output YES if its likely in Vulcan and NO if its not (e.g., was shift-ciphered).* But there is some information I am missing. What is it? How can I find it?

(b) Write psuedocode for code IS-VULCAN using the following information. Assume you already have (1) a program that finds the frequencies of each letter in the ciphertext, and (2) a program that will, given a Text T and $s \in \{1, \ldots, 9\}$, output the text shifted by s.

SOLUTION TO PROBLEM TWO

a) We need to know:

- $DOT(F, F)$. We will call this GOOD.
- Let $F(s)$ be the vector F shifted. We need to know the MAX of $DOT(F, F(s))$. We call this BAD.

b) The Key question is how far apart are GOOD and BAD. We'll assume that if a documents freq DOT F is $\geq (GOOD - BAD)/2$ then its good. In reality we'd prob use a higher number. Let $(GOOD - BAD)/2 = GOODENOUGH$.

IS VULCAN:

Input(T)

G=FREQ(T)

D=DOT(F,G)

If D > GOODENOUGH output YES, else NO

c) I didn't ask this one but its enlightening.

What if you know that T was done by shift. We want to decode it. Here is how:

We want to see which s makes $DOT(FREQ(SHIFT(T, s), P)$ maximum. We will also check in the end of this number is close to GOOD – if it is not then it is likely that a shift cipher was not used after all!

Input(T) (the ciphertext)

For s=1 to 9

A[s]= $DOT(FREQ(SHIFT(T,s),P)$.

s=the index of the max component ot A.

If $DOT(FREQ(SHIFT(T,s),P)$ is close to GOOD then output $SHIFT(T,s)$.

else output *GEE, this code was not shift ciphered!*

END OF SOLUTION TO PROBLEM TWO

3. (20 points) Alice and Bob are using a Vig cipher. Eve notices that the sequence of letters *adbzga* appears 3 times! She notices that the first and second appearances are 105 apart, the second and third appearances are 60 apart. Give a small set of candidates for the key length (1 is a candidate). Make the set of candidates as small as possible (don't be a wiseguy and list lots of candidates and argue with me about the definition of *small*).

SOLUTION TO PROBLEM THREE

We want all numbers that divide 105 and 60 and 105+65=165.

KEY- must list ALL divisors of 105, 60, and 165 and output all numbers that are on all the lists.

$105 = 3 \times 5 \times 7$ so there are $2 \times 2 \times 2 = 8$ divisors

$3^0 \times 5^0 \times 7^0 = 1$

$3^0 \times 5^0 \times 7^1 = 7$

$3^0 \times 5^1 \times 7^0 = 5$

$3^0 \times 5^1 \times 7^1 = 35$

$3^1 \times 5^0 \times 7^0 = 3$

$3^1 \times 5^0 \times 7^1 = 21$

$3^1 \times 5^1 \times 7^0 = 15$

$3^1 \times 5^1 \times 7^1 = 105$

We list these numbers in numeric order: $\{1, 3, 5, 7, 15, 21, 35, 105\}$

$60 = 2^2 \times 3 \times 5$ so there are $3 \times 2 \times 2 = 12$ divisors.

We COULD list them all out. OR we could just see which divisors of 105 are also divisors of 60. They are $\{1, 3, 5, 15\}$

$165 = 3 \times 5 \times 11$.

We list out all divisors of 165 that are already in our set. They are $\{1, 3, 5, 15\}$. Oh well. Anyway, we have our small set.

4. (20 points) Alice and Bob are using a Vig cipher. Eve notices that the sequence of letters *aqzbef* appears 3 times! She notices that the first and second appearances are 30 apart, the second and third appearances are 105 apart, the third and fourth are 385 apart, and the fourth and fifth are 1001 apart. Give a small set of candidates for the key length (1 is a candidate). Make the set of candidates as small as possible (don't be a wiseguy and list lots of candidates and argue with me about the definition of *small*).

   SOLUTION TO PROBLEM FOUR

   $30 = 2 \times 3 \times 5$

   $105 = 3 \times 5 \times 7$

   $385 = 5 \times 7 \times 11$

   $1001 = 7 \times 11 \times 13$

   The only number that divides all of this is 1. So 1 is the only candidate.

   END OF SOLUTION TO PROBLEM FOUR
   GO TO NEXT PAGE

5. (20 points) (For this problem you should feel quite free to look it up on the web.)

   (a) Let $a, b, c, d \in R$ (the reals). Let

   $$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

      i. Give a condition $INVR$ on a, b, c, d such that A has an inverse *with real entries* iff $INVR(a, b, c, d)$ holds.

      ii. Assume that $INVR(a, b, c, d)$ holds. Write down the inverse of A.

   (b) Let $a, b, c, d \in Z$ (the integers). Let

   $$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

      i. Give a condition $INVZ$ on a, b, c, d such that A has an inverse *with integer entries* iff $INVZ(a, b, c, d)$ holds.

      ii. If $INVZ(a, b, c, d)$ holds then write down the inverse of A.

   SOLUTION TO PROBLEM FIVE

   a) $INVR(a, b, c, d)$ is that $ad - bc \neq 0$.

   b) OMITTED- Cmon, this you can look up.

   c) There are two answers and they are equivalent and both fine.

   ANSWER ONE: Note from (b) that for the inverse to have integer entries the det must divide all of them. So the answer is

   $ad - bc$ divides a, b, c, and d.

   ANSWER TWO: The det is 1 or -1. Easy to see that if det is 1 or -1 then inverse has integer entries. The other direction is nontrivial, but the web says its true, so its true.

6. (10 points) Go to `https://www.dcode.fr/caesar-cipher`

   Set it to encode a message by a shift of 3. Type in

   CMSC 389 Rocks! Do you agree?

   What does it return? Would you call what you see evidence of a bug or of a feature?

SOLUTION TO PROBLEM SIX

List one bug? I can list many!

(a) The encoding preserves spacing so Eve can guess from length-of-words some information

(b) Numbers do not get encoded. 8 goes to 8.

(c) Punctuation does not get encoded. So even Eve does not know what the sentence is she knows that they are excited about it or that it was a question.

When I typed in

CMSC 389 Rocks! Do you agree?

I got:

FPVP 389 Urfnv! Gr brx djuhh?

END OF SOLUTION TO PROBLEM SIX