HW 2 CMSC 389. DUE Jan 5

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.

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*).

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*).

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.

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?