HW 1 CMSC 456. Morally DUE Sep 9
NOTE- THE HW IS FIVE PAGES LONG

1. (0 points) GOTO course website. READ the entries *conent* and *policy*. READ the notes on ciphers. READ my slides for all days the class has met. What is your name? What is the day and time of the midterm?

2. (20 points) Klingons use an alphabet of 29 letters. Vulcans use an alphabet of 30 letters. Spock notes that Klingons have an easier time using the affine cipher than Vulcans. He is correct.

   (a) (10 points) Why is it easier for Klingons to use the affine cipher than Vulcans?

   (b) (10 points) Fill in the following sentence:
   It is easier to use the affine cipher if the number of letters in the alphabet is _________because _________.

GO TO NEXT PAGE

3. (25 points) Alice and Eve play the game where Alice randomly chooses to send Eve a perm generated by a random 7-letter keyword and a shift OR a truly random perm, and Eve tries to figure out which one. In this problem we give Eve a strategy.

   For this problem, assume that if Alice picks keyword-shift (so her perm is generated by keyword-shift) then the encoding table will ALWAYS have three consecutive letters in consecutive positions in the second row. (That is, either a, b, c or b, c, d or $\ldots$ or x, y, z or y, z, a or z, a, b. We DO count if a, b are the 25th and 26th letters in the second row, and c is the 1st.) In general, a perm generated by keyword-shift will not always have the above property, but it almost always will, so we assume that it always will.

   (a) (5 points) Give an upper bound on the number of perms of $\{a, \ldots, z\}$ there are that have three consecutive letters in them. (It cannot be trivial or later problems will be harder.)

   (b) (5 points) Obtain an upper bound on the probability that a randomly chosen perm has three consecutive letters in them. Your bound has to be < 1. Express as a fraction in lowest terms, but also give an approximation as a decimal.

   (c) (15 points) Alice and Eve play the game where Alice randomly chooses to send Eve a perm generated by a random 7-letter keyword and a shift OR a truly random perm, and Eve tries to figure out which one. Eve's strategy: if the perm she gets has three consecutive letters then she'll guess it comes from Keyword-shift, otherwise rand perm. Express answers to the questions below as a fraction in lowest terms, but also give an approx as a decimal.

      - What is a bound on the probability that Alice chose a keyword-shift cipher AND Eve got it wrong?
      - What is a bound on the probability that Alice chose a rand perm AND Eve got it wrong?
      - What is a bound on the probability that Eve is wrong?

   (d) (0 points but think about) How well can Eve do if the game used keyword-mixed cipher instead of keyword-shift?

GO TO NEXT PAGE

4. (40 points) This is a programming problem. You will write a program that outputs five numbers, each on separate lines.

   (a) Input (from standard input) a 26-vector of probabilities $(p_0, \ldots, p_{25})$. This input will be formatted as a string of 26 floating point numbers separated by spaces. You may assume that all input provided is valid (in particular, entries are between 0 and 1, and sum to 1). We DO allow entries to be 0 or 1.

   (b) Compute $\sum_{i=0}^{25} p_i^2$. Print this number (to standard output) on the first line.

   (c) For all $0 \le s \le 25$, compute

   $$\sum_{i=0}^{25} p_i \times p_{i+s} \pmod{26}.$$

   Output on the second line the SECOND LARGEST value among these computed values. (The largest will be the number from part (b), when $s = 0$.) Output the distance between the largest value and the second largest value on the third line.

   (d) For all $0 \le a \le 25$ that are rel prime to 26, and $b \in \{0, \ldots, 25\}$, compute

   $$\sum_{i=0}^{25} p_i \times p_{ai+b} \pmod{26}.$$

   Output on the fourth line the SECOND LARGEST value among these computed values. Then output the distance between the largest value and the second largest value on the fifth line. Compare it to the gap from part (d).

YOU ARE NOT DONE! GOTO NEXT PAGE TO SEE WHAT YOU RUN THIS PROGRAM ON

Run the program on the prob vector from

`https://en.wikipedia.org/wiki/Letter_frequency`

Note that this website has percents, not probabilities. So for example the prob of an a is 0.08167. Report the output of your program on this input along with the rest of your homework. Your code should be uploaded separately (see below).

You are free to choose from various programming languages to complete this problem. By default, we support Java, Python2/3, and Ruby. Ask on Piazza if you want more options. You will be submitting all code files you used to complete this problem to the Gradescope assignment called "hw01 - problem 4". Since you will probably want to submit multiple files, you should merge all files into a single zip file and submit that zip file to Gradescope. Upon submission, your code will be automatically run on a Linux machine and tested against various test cases to ensure correctness. You are allowed to submit your code as many times as you want.

Regardless of the language you choose, your submission must include a bash script called `run` (with no file extension). This file must begin with the shebang `#!/usr/bin/env bash` on the very first line. This script will be run each time the autograder tries to run your code, so add to this file any commands that are needed to run your code. This gives you greater flexibility regarding how you want to organize your code. Additionally, if you are using a non-scripting language such as Java, also upload a bash script called `build`, also with shebang. This script will be called once upon submission to compile your code before execution.

If you have any questions or confusions, or if you encounter any technical difficulties, feel free to ask for help on Piazza.

GOTO NEXT PAGE

5. (15 points) Alice and Bob are going to use the Vig cipher. The keyword is *justin.* Alice want to send

   Bill's course on Ramsey Theory this spring will be awesome!

   What does Alice 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.)