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

1. (0 points) READ the syllabus- Content and Policy. READ my NOTES on ciphers. 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 alphabet if the number of letters is _______ because _______.

SOLUTION TO PROBLEM TWO

(a) Why is it easier for Klingons to use the affine cipher than Vulcans. 
   ANSWER: Since all $a \in \{1, \ldots, 28\}$ are relatively prime to 29, 
   Klingons can use any $a$ they want. Vulcans need to be careful to 
   make sure that $a$ is rel prime to 30.

(b) Fill in the following sentence:

   It is easier to use the affine alphabet if the number of letters is _______ because _______.

   ANSWER: It is easier to use the affine alphabet if the number of 
   letters is PRIME because ALL VALUES OF $a$ in $\{1, \ldots, |\Sigma| - 1\}$ 
   are fine to use.
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 and see how well it does.

(a) (5 points) Show that if Alice picks keyword-shift (so her permutation is generated by keyword-shift) then the encoding table has three consecutive letters in the second row. (That is, either $a, b, c$ or $b, c, d$ or ... 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.

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

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

(d) (10 points) Alice and Eve are playing that really fun game where Alice randomly chooses to send Eve a perm generated by a random 5-letter keyword and a shift OR a truly random perm, and Eve tries to figure out which one. Here is 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 approximation in decimal.

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

(e) (0 points but think about) You should have found out that Eve can do pretty well at the game, with a probability of being wrong $< \alpha$ where $\alpha < \frac{1}{2}$, so she does better than guessing. Speculate on if there is a simple strategy for this game with the keyword-mixed cipher, with keyword of length 4.

SOLUTION TO PROBLEM THREE
(a) (5 points) Show that if Alice picks keyword-shift (so her permutation is generated by keyword-shift) then the encoding table has three consecutive letters in the second row. (That is, either \(a, b, c\) or \(b, c, d\) or \(...\) 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.

**ANSWER:** Look at all of the three-tuples \((a, b, c)\), \((d, e, f)\), \((g, h, i)\), \((j, k, l)\), \((m, n, o)\), \((p, q, r)\), \((s, t, u)\) \((v, w, x)\). Since the keyword is only 5 long at least one of these triples will not be disturbed.

(b) (5 points) Give an upper bound on how many permutations of \(\{a, \ldots, z\}\) have three consecutive letters in them? (It cannot be trivial or later problems will be harder.)

**ANSWER:** We form the permutation by first picking the first letter in the set of three. We can do that 26 ways. Say its \(p\). Then we place \(p, q, r\) where \(p\) is the first, second, \(...\), or 26th letter. We can do that 26 ways. Then the remaining 23 letters are permuted an placed around \(p, q, r\). So there are at most \(26 \times 26 \times 23!\) such perms.

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

**ANSWER:** Using the last part the bound is

\[
\frac{26^2 \times 23!}{26!} = \frac{26^2}{26 \times 25 \times 24} = \frac{26}{25 \times 24} = \frac{13}{300} \approx 0.4333
\]

(d) (5 points) Alice and Eve are playing that really fun 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. Here is Eve’s strategy: if the perm she gets has three consecutive letters then she’ll guess it comes from Keyword-shift, otherwise rand perm.

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

**ANSWER:** The prob that Alice chose a keyword-shift is \(\frac{1}{2}\). The prob that Eve got it wrong is 0 since a keyword shift ALWAYS has three consecutive.
• What is a bound on the prob that Alice chose a rand perm AND Eve got it wrong?
  ANSWER: The prob that Alice chose a rand perm is $\frac{1}{2}$. The prob that Eve got it wrong is the prob that a random perm had three consecutive in a row, which is $\frac{13}{300}$. Hence the prob that both happen is

\[
\frac{13}{300} \times \frac{1}{2} = \frac{13}{600} \sim 0.21666
\]

• What is a bound on the Prob that Eve is wrong.
  ANSWER: This is the sum of the two prior answers, so $\frac{13}{60} = \sim 0.21666$.

(e) You should have found out that Eve can do pretty well at the game, with a probability of being wrong $< \alpha$ where $\alpha < \frac{1}{2}$, so she does better than guessing. Speculate on if there is a simple strategy for this game with the keyword-mixed cipher, with keyword of length 7.
  ANSWER: I don’t actually know!

   GO TO NEXT PAGE
4. (40 points) Write a program that does the following:

(a) Input is a 26-vector of probabilities \((p_0, \ldots, p_{25})\). Check that all of the entries are between 0 and 1, and that the sum is 26. We DO allow entries to be 0 or 1.

(b) Compute \(\sum_{i=0}^{25} p_i^2\).

(c) Compute, for all \(0 \leq s \leq 25\),
\[
\sum_{i=0}^{25} p_i \times p_{i+s} \pmod{26}.
\]
Output them in order and note the distance between the first one (which should happen when \(s = 0\)) and the next one. It should be a large gap, larger than any of the others.

(d) Compute, for all \(0 \leq a \leq 25\) that are rel prime to 26, and \(b \in \{0, \ldots, 25\}\),
\[
\sum_{i=0}^{25} p_i \times p_{ai+b} \pmod{26}.
\]
Output them in order and note the distance between the first one (which should happen when \(s = 0\)) and the next one. It should be a large gap, larger than any of the others. I am most curious if its a smaller gap than the last question, or about the same.

YOU ARE NOT DONE! GOTO NEXT PAGE TO SEE WHAT YOU RUN THIS PROGRAM ON
Run the program on the following and report your results

(a) The prob vector from

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

Note that that website has percents, not probabilities. So for example the prob of an a is 0.08167.

(b) The prob vector where the first 13 entries are \( \frac{1}{13} \) and the rest are 0.

(c) The prob vector where the first 13 entries are \( \frac{1}{20} \) and the rest are \( \frac{7}{260} \).

(d) Let \( A = \frac{1}{2} + \cdots + \frac{1}{27} \). The prob vector is \( (\frac{1}{2} \times \frac{1}{A}, \frac{1}{3} \times \frac{1}{A}, \ldots, \frac{1}{27} \times \frac{1}{A}) \).

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.)

**SOLUTION TO PROBLEM FIVE**

I did option (3).

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

Kcde’a pxojlm bw Lsfarh Nzxweh nzba fylago jrdf um nfykhur!

This leaks LOTS of information: They don’t do the blocks-of-five, so spacing is a clue. They don’t get rid of punctuation. They don’t map all letters to small letters. So this is not a very good encoder. This is typical of the encryption you find on the web.