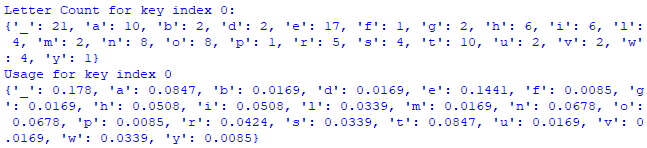
Kevin Zhang

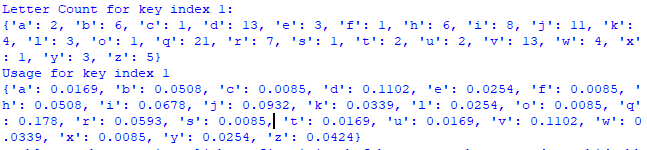
CSC5270

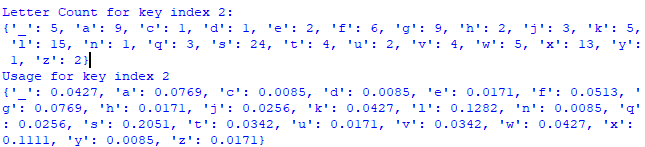
HW1

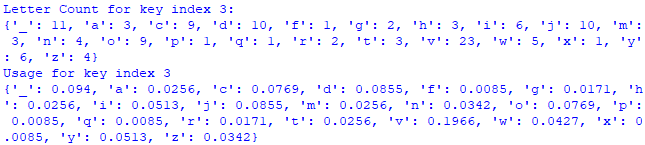
Question 2

1. Key: ARTW  
     
   Message: the\_art\_of\_war\_teaches\_us\_to\_rely\_not\_on\_tHE\_likelihood\_of\_the\_Enemy\_not\_coming\_but\_on\_our\_own\_readiness\_to\_recEive\_him\_not\_on\_the\_chance\_of\_his\_not\_attacking\_but\_ratHEr\_on\_tHE\_fact\_that\_we\_Have\_made\_our\_position\_unassailable\_the\_end\_and\_aim\_of\_spying\_in\_all\_its\_five\_varietiEs\_is\_knowledge\_of\_the\_enemy\_and\_this\_knowledge\_can\_only\_be\_derived\_in\_the\_first\_instancE\_from\_the\_converted\_spy\_hence\_it\_is\_essEntial\_that\_the\_convErted\_spy\_be\_treated\_with\_tHE\_utmost\_libErality  
     
   The first step to decode this passage was to find the key length. I used two tactics. The latter tactic was something I used when I was stuck and needed to confirm the key length again.   
   A close up of text on a white background

   Description automatically generated  
   For the first tactic, I evaluated the reoccurrences of letters. I wrote the text multiple times, each time slightly offset. Then, I looked for the number of letters in each row that matched the first row. Notably, two rows had a much greater number of matching letters than the other rows. Row 5 had 5 matching letters and row 9 had 3 matching letters. The rows were 4 rows apart, suggesting the key length was 4.  
     
   The second tactic I used to confirm key length was to check for reoccurring letter combinations and their distance apart. Some reoccurring combinations include:  
     
   vors: 48 letters apart  
   vods: 40 letters apart  
   lvod: 40 letters apart  
   sohv: 68 letters apart  
   qlce: 68 letter apart  
     
   The greatest common factor of all of those letter distances was 4, once again suggesting that the key size was 4.  
     
   Once I found the key size, I needed to find out how much every four letters of the ciphertext had been shifted. I ran a script that would do a frequency analysis on the parts of the text that were shifted by key letter 0, key letter 1, key letter 2, and key letter 3. Results of the frequency analysis follow.  
     
   Key letter 0:   
     
   A screenshot of a cell phone

   Description automatically generated  
     
   Key letter 1:  
     
   A screenshot of a cell phone

   Description automatically generated  
     
   Key letter 2:  
     
     
   A screenshot of a cell phone

   Description automatically generated  
     
   Key letter 3:  
     
   A screenshot of a cell phone

   Description automatically generated  
     
   All graphs showed the distribution of letters. Each graph also had one column that was significantly higher than the rest. The highest column must represent the most common character, the space “\_”. Thus, I calculated how much each graph was shifted from “\_” and used that information to find the key letter.  
     
   Key letter 0 shifted 0 spaces. The corresponding letter is A.  
   Key letter 1 shifted 17 spaces. The corresponding letter is R.  
   Key letter 2 shifted 19 spaces. The corresponding letter is T.  
   Key letter 3 shifted 22 spaces. The corresponding letter is W.  
     
   Thus, the key is ARTW.
2. Breaking the vigenere cipher requires two main steps: finding the key length and then finding each key letter. The most important part is the key length because once that is found, the vigenere cipher is just multiple simple Caesar ciphers. Because the vigenere key is a repeated value, the ciphertext will also have repeated values, which can give insight into the key length.   
     
   After finding the key length, each part of the ciphertext is just segmented Caesar ciphers, which can be decoded with brute force, since there are only 25 meaningful shifts for a Caesar cipher. Alternatively, frequency analysis can be used to show the frequency of letters compared to the normal frequency of letters. This process can reveal how much the ciphertext has been shifted.