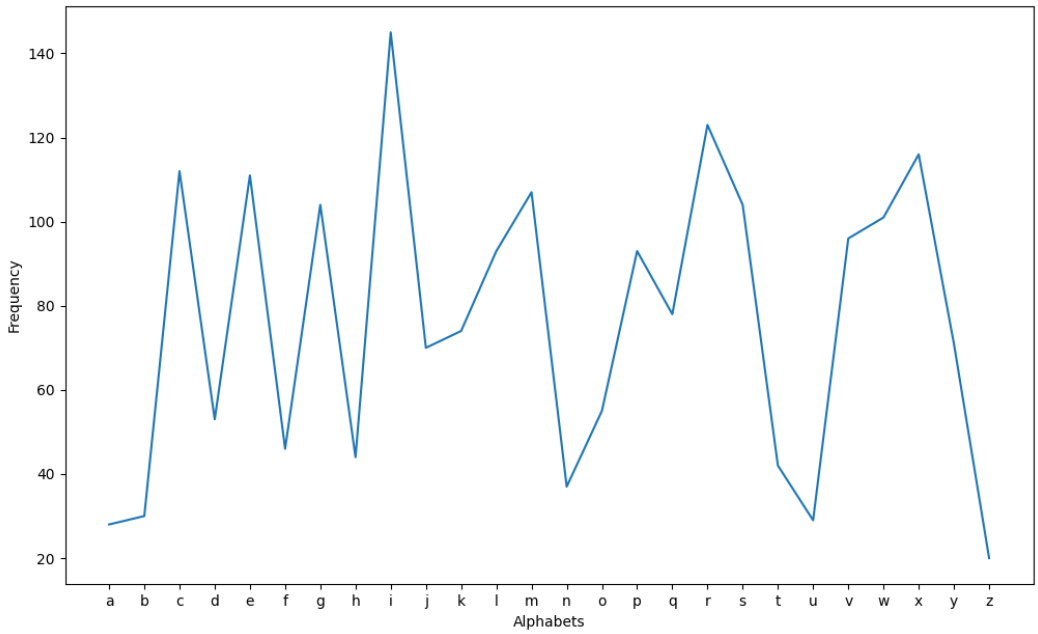
ECE 458 Asg 1

Harry Ryu
Rick Du

Exercise 1 Part 1B

Frequency List: [28. 30. 112. 53. 111. 46. 104. 44. 145. 70. 74. 93. 107. 37. 55. 93. 78. 123. 104. 42. 29. 96. 101. 116. 71. 20.]

Graph:



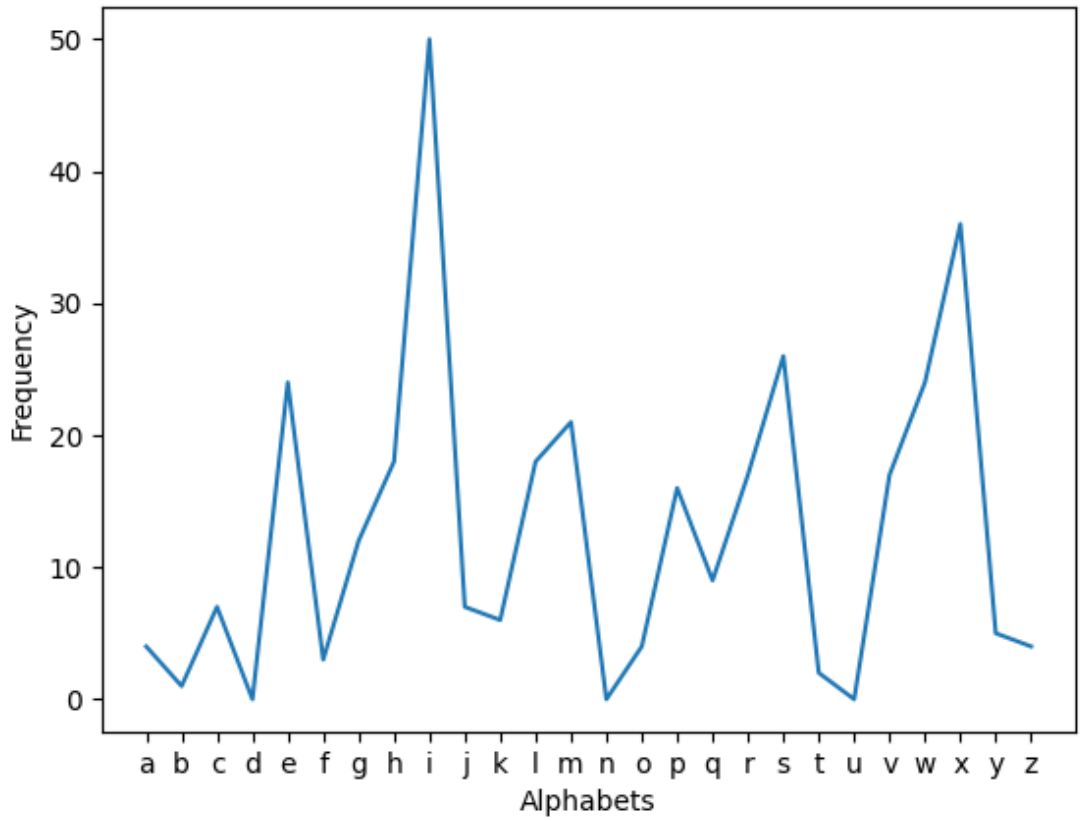
Observations: The graph indicates that the letter with the highest frequency in the entire ciphertext is “i”, which is most likely the letter “e” when decrypted.

Exercise 1 Part 2B

Frequency list (2D array of 4 x 26): [
[4. 1. 7. 0. 24. 3. 12. 18. 50. 7. 6. 18. 21. 0. 4. 16. 9. 17. 26. 2. 0. 17. 24. 36. 5. 4.]
[2. 0. 23. 10. 15. 8. 47. 6. 8. 25. 23. 1. 0. 19. 7. 15. 26. 6. 0. 27. 25. 22. 9. 2. 5. 0.]
[6. 0. 9. 1. 20. 3. 7. 12. 42. 8. 4. 19. 26. 0. 2. 19. 9. 24. 25. 7. 0. 22. 30. 28. 6. 1.]
[0. 17. 22. 36. 11. 4. 9. 0. 4. 0. 27. 7. 16. 14. 38. 7. 9. 14. 20. 1. 0. 11. 9. 21. 27. 6.]

```
 [ 7.  0.  6.  0. 39.  8. 16.  8. 41. 11.  7. 20. 16.  0.  4. 17.  9. 20.
  23.  2.  0. 22. 16. 28.  8.  2.]
 [ 9. 12. 45.  6.  2. 20. 13.  0.  0. 19.  7. 28. 28.  4.  0. 19. 16. 42.
  10.  3.  4.  2. 13.  1. 20.  7.]
]
```

Graph:



Observations: The distribution is different from the previous graph, as the current graph only represents a small chunk of the original graph. However, this chunk of graph also indicates that the most frequent letter is “i”.

Exercise 1 Part 3

The key is “ecekey”

Exercise 1 Part 4

welocometothesecuritycourseofecetherestofthistextisjustrandomstufffromtheinternetthecolorofanimalsisbynomeansamatterofchanceitdependsonmanyconsiderationsbutinthemajorityofcasestendstoprotecttheanimalfromdangerbyrenderingitlessconspicuousperhapsitmaybesaidthatifcoloringismainlyprotectivethereoughttobebutfewbrightlycoloredanimalstherearehowevernotafewcasesinwh

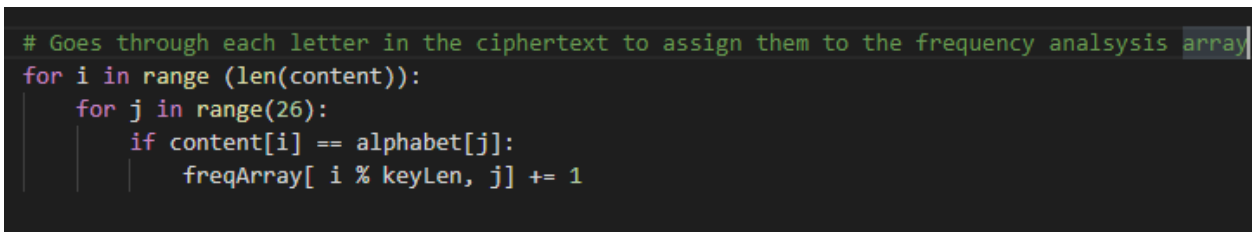
ichvividcolorsarethemselvesprotectivethekingfisheritselfthoughsobrightlycoloredisbynomeansea
sytoseetheblueharmonizeswiththewaterandthebirdasitdartsalongthestreamlooksalmostlikeaflash
ofsunlightdesertanimalsaregenerallythecolorofthedesertthusforinstancethelionteantelopeandth
ewilddonkeyareallsandcoloredindeedsayscanontristraminthedesertwhereneithertreesbrushwood
norevenundulationofthesurfaceaffordtheslightestprotectiontoitsfoesamodificationofcolorassimilat
edtothatofthesurroundingcountryisabsolutelynecessaryhencewithoutexceptiontheupperplumage
ofeverybirdandalsothefurofallthesmallermammalsandtheskinofallthesnakesandlizardsisofoneunif
ormsandcolorthenextpointisthecolorofthematurecaterpillarssomeofwhicharebrownthisprobablym
akesthecaterpillarevenmoreconspicuousamongthegreenleavesthanwouldotherwisebethecaselet
usseethenwhetherthehabitsoftheinsectwillthrowanylightupontheriddlewhatwouldyoudoifyouwere
abigcaterpillarwhylikemostotherdefenselesscreaturesyouwouldfeedbynightandlieconcealedbyda
ysodothesecaterpillarswhenthemorninglightcomestheycreepdownthestemofthefoodplantandlieco
ncealedamongthethickherbageanddrysticksandleavesnearthegroundanditisobviousthatundersuc
hcircumstancesthebrowncolorreallybecomesaprotectionitmightindeedbearguedthatthecaterpillar
shavingbecomebrownconcealedthemselvesonthegroundandthatwewerereversingthestateofthing
sbutthisisnotsobecausewhilewemaysayasageneralrulethatlargecaterpillarsfeedbynightandliecon
cealedbydayitisbynomeansalwaysthecasethattheyarebrownsomeofthemstillretainingthegreencol
orwemaythenconcludethatthehabitofconcealingthemselvesbydaycamefirstandthatthebrowncolori
salateradaptation

Exercise 2 Question 1

One method to obtain the key length is to scan through the entire given ciphertext to search for repeating consecutive letters. Then based on the distance (d) between each repeating group of those repeating consecutive letters, the length of the key will be one of the common divisors of this distance d. Try out each one of the different divisors as the key length to be used for frequency analysis until one is obtained that results in the decrypted plaintext making sense, thus this is the key length we wanted to obtain.

Exercise 2 Question 2

1. Obtain the key length as described by exercise 2 question 1. Search for common repeating consecutive letters and based on the distance between them obtain the common divisors, and proceed with the following steps with each of the common divisor.
2. Apply frequency analysis on the ciphertext, where the number of chunks equals the value of the common divisor picked.


```
# Goes through each letter in the ciphertext to assign them to the frequency analsysis array
for i in range (len(content)):
    for j in range(26):
        if content[i] == alphabet[j]:
            freqArray[ i % keyLen, j] += 1
```

3. The letter “e” is the most commonly used alphabet. The letter in the ciphertext with the highest frequency is most likely “e”. Use the difference between the ciphertext and “e” to obtain the key.
4. Apply the key on the ciphertext by subtracting the ciphertext letters with the key to obtain a plaintext. If the plaintext makes sense, then we have successfully cracked the ciphertext using the correct key. Otherwise go back to step 1. and repeat until the right plaintext is obtained.

```python
# Excercise 1 Part 3
# Takes the frequency array from the previous function and obtain the key through frequency analysis assuming "e" is the most frequent letter
def decryptKey(freqArray):

    # Initalize key string
    key = ""

    # Loops through each chunk
    for i in range(len(freqArray)):
        # Obtain the alphabet with the highest frequency
        maxFreqIndex = np.argmax(freqArray[i])
        # Obtain key value assuming "e" has the highest occurence
        key += alphabet[(maxFreqIndex + 26 - 4) % 26 ]

    print(key)
    return key
```