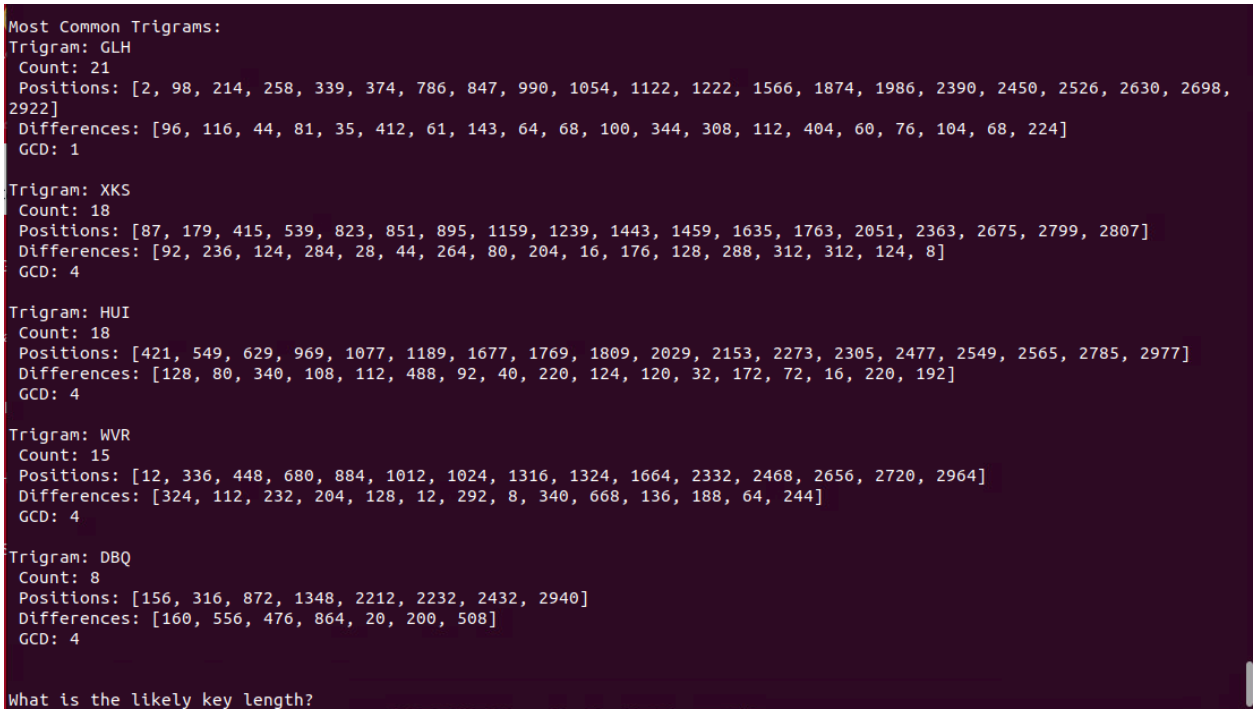
Lab 03 Template

1)

Take a screenshot of the five most common trigrams. Make sure you copy all the data including counts, distances, and common divisor.

(10 total points, 2 points each trigram with full information)



```
Most Common Trigrams:
Trigram: GLH
 Count: 21
 Positions: [2, 98, 214, 258, 339, 374, 786, 847, 990, 1054, 1122, 1222, 1566, 1874, 1986, 2390, 2450, 2526, 2630, 2698,
2922]
 Differences: [96, 116, 44, 81, 35, 412, 61, 143, 64, 68, 100, 344, 308, 112, 404, 60, 76, 104, 68, 224]
 GCD: 1

Trigram: XKS
 Count: 18
 Positions: [87, 179, 415, 539, 823, 851, 895, 1159, 1239, 1443, 1459, 1635, 1763, 2051, 2363, 2675, 2799, 2807]
 Differences: [92, 236, 124, 284, 28, 44, 264, 80, 204, 16, 176, 128, 288, 312, 312, 124, 8]
 GCD: 4

Trigram: HUI
 Count: 18
 Positions: [421, 549, 629, 969, 1077, 1189, 1677, 1769, 1809, 2029, 2153, 2273, 2305, 2477, 2549, 2565, 2785, 2977]
 Differences: [128, 80, 340, 108, 112, 488, 92, 40, 220, 124, 120, 32, 172, 72, 16, 220, 192]
 GCD: 4

Trigram: WVR
 Count: 15
 Positions: [12, 336, 448, 680, 884, 1012, 1024, 1316, 1324, 1664, 2332, 2468, 2656, 2720, 2964]
 Differences: [324, 112, 232, 204, 128, 12, 292, 8, 340, 668, 136, 188, 64, 244]
 GCD: 4

Trigram: DBQ
 Count: 8
 Positions: [156, 316, 872, 1348, 2212, 2232, 2432, 2940]
 Differences: [160, 556, 476, 864, 20, 200, 508]
 GCD: 4


What is the likely key length?
```

2)

Why do we analyze trigrams (three-character sequences) when attempting to break a Vigenère cipher? What information do the differences between their positions provide?

(10 total points, 5 points each question)

Analyzing trigrams in a ciphertext helps in breaking a Vigenere cipher because repeated trigrams are likely caused by the repeating nature of the keyword used in the cipher. The differences in their positions within the ciphertext indicate where the key is repeating. Based on this we can analyze similar trigrams and get the key characters for encryption.

3)

How does calculating the greatest common divisor (GCD) of position differences help in determining the key length?

(5 total points)

This is because the distances between the repetitions is most likely multiples of the key length and the GCD of these will mostly give us the key length.

4)

Based on your findings, what do you suspect the key length is? Justify your

answer. (10 total points, 5 points length value, 5 points justification)

Based on the findings I suspect the key length to be 4. This is because the most frequent GCD is 4 while 1 appears only once. The keyword length is typically the most common GCD among the differences in trigrams indices.

5)

Why do you assume the most frequent character is E? How does it help us with

multiple shift-by-n ciphers?

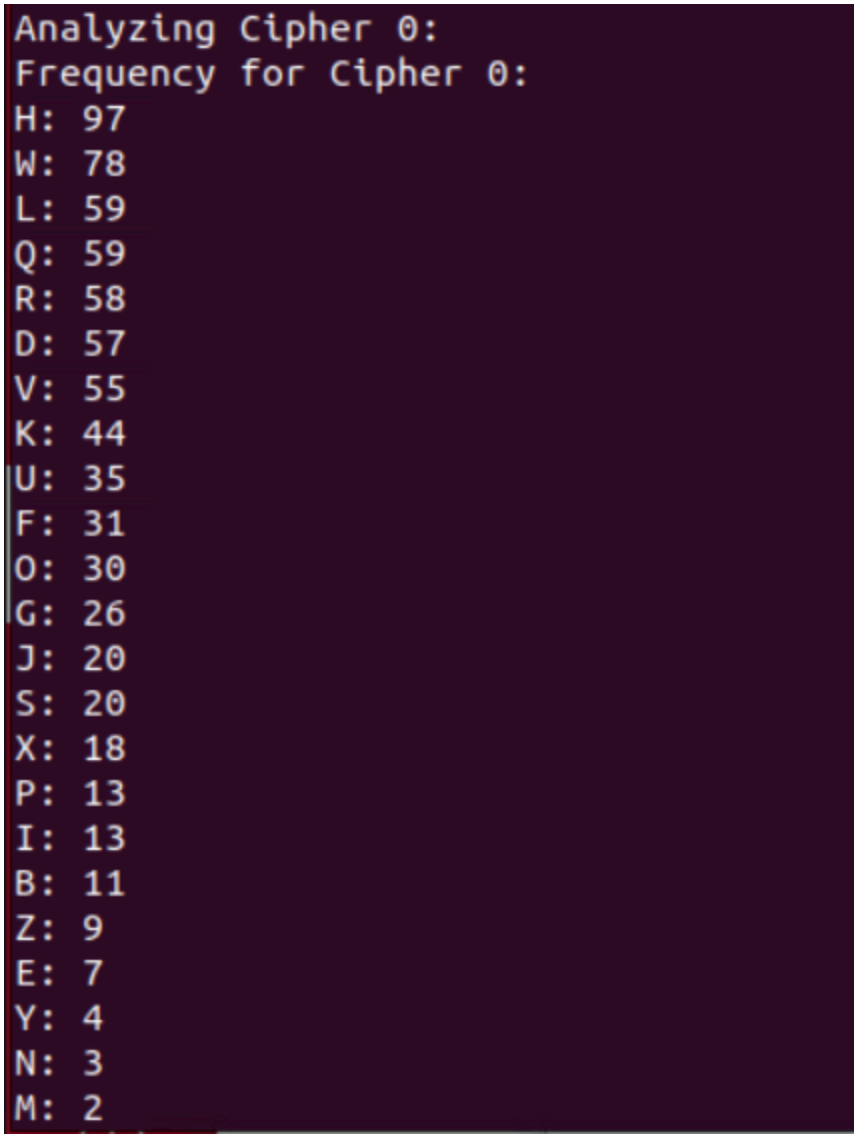
(10 total points, 5 points each question)

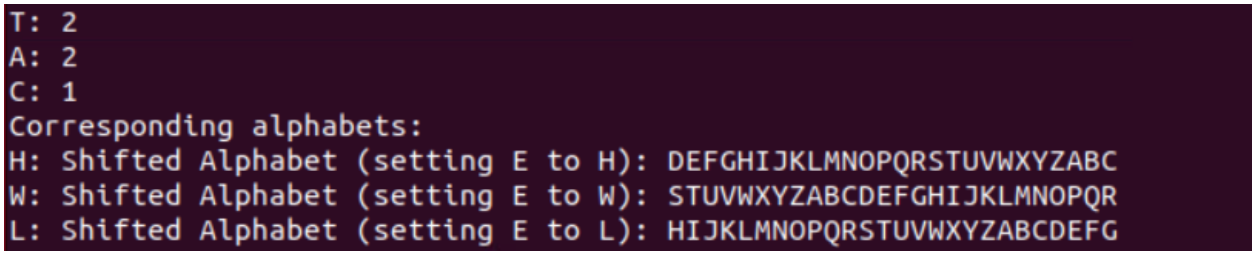
The assumption that the most frequent character in each monoalphabetic shift by n cipher corresponds to E is based on letter frequency analysis. E is the most commonly used letter in English. Each shift cipher behaves like a Caesar cipher and in that the most frequently occurring letter is E. This helps us as we can determine the shift/ key value for a segment by assuming that the most frequent letter in each shift cipher corresponds to E.

6)

Take a screenshot for each shift-by-n cipher

(10 total points)


Analyzing Cipher 0:
Frequency for Cipher 0:
H: 97
W: 78
L: 59
Q: 59
R: 58
D: 57
V: 55
K: 44
U: 35
F: 31
O: 30
G: 26
J: 20
S: 20
X: 18
P: 13
I: 13
B: 11
Z: 9
E: 7
Y: 4
N: 3
M: 2

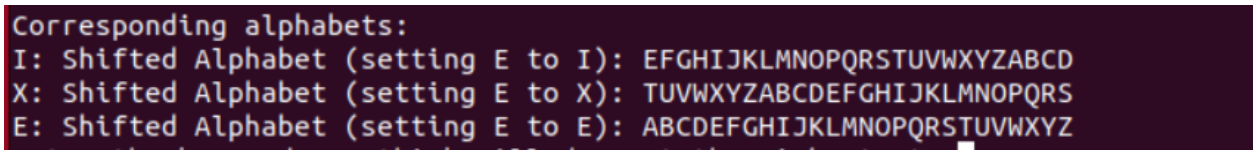

T: 2
A: 2
C: 1
Corresponding alphabets:
H: Shifted Alphabet (setting E to H): DEFGHIJKLMNOPQRSTUVWXYZABC
W: Shifted Alphabet (setting E to W): STUVWXYZABCDEFGHIJKLMNOPQR
L: Shifted Alphabet (setting E to L): HIJKLMNOPQRSTUVWXYZABCDEFG

```
Analyzing Cipher 1:
Frequency for Cipher 1:
S: 103
H: 97
C: 58
B: 56
O: 56
W: 53
G: 47
Z: 35
V: 34
F: 34
R: 29
Q: 27
I: 20
T: 17
U: 16
M: 15
K: 14
A: 13
P: 8
D: 8
J: 4
L: 3
E: 2
Y: 2
N: 1
X: 1
Corresponding alphabets:
```

```
Corresponding alphabets:
S: Shifted Alphabet (setting E to S): OPQRSTUVWXYZABCDEFGHIJKLMN
H: Shifted Alphabet (setting E to H): DEFGHIJKLMNOPQRSTUVWXYZABC
C: Shifted Alphabet (setting E to C): YZABCDEFGHIJKLMNOPQRSTUVWX
```

```
Analyzing Cipher 2:
Frequency for Cipher 2:
R: 85
G: 75
F: 70
B: 61
V: 59
N: 48
E: 46
A: 43
Y: 35
U: 35
H: 29
P: 26
Q: 18
S: 18
Z: 18
C: 15
T: 15
L: 14
I: 12
O: 10
J: 9
X: 5
K: 3
M: 2
W: 1
```

```
W: 1
D: 1
Corresponding alphabets:
R: Shifted Alphabet (setting E to R): NOPQRSTUVWXYZABCDEFGHIJKLM
G: Shifted Alphabet (setting E to G): CDEFGHIJKLMNOPQRSTUVWXYZAB
F: Shifted Alphabet (setting E to F): BCDEFGHIJKLMNOPQRSTUVWXYZA
```



7)

Decrypt the ciphertext using the potential key values you found in question 5.

Show all iterations, the final keyword, and the final plaintext.

(30 total points, 20 points for all iterations, 5 points for correct keyword, 5 points for correct plaintext)

```
Enter the keyword you think will decrypt the ciphertext: DONE
```

```
Decrypted Plaintext:
INTHEHEARTOFTHEANCIENTWORLDLIESAMYSTERYTHATHASPUZZLEDSCHOLARSANDADVENTURERSFORCENTURIESTHELEGENDOFTHELOSTCITYOFATLANTISAC
IVILIZATIONOFUNPARALLELEDTECHNOLOGYANDWEALTHSUBMERGEDUNDERTHEOCEANSDEPTHSCONTINUESTOCAPTIVATETHEIMAGINATIONOFALLWHOHEARIT
STALEACCORDINGTOTHEANCIENTTEXTSATLANTISWASAHUBOFKNOWLEDGEWHEREPHILOSOPHERSANDSCIENTISTSTHRIVEDTHECITYWASSAIDTOBEMADEOFGOL
DSILVERANDOTHERPRECIOUSMATERIALSSHININGBRIGHTLYUNDERTHESUNTHESECRETSOFATLANTISINCLUDETHEADVANCEDTECHNOLOGYTHATWASPOSSIBLY
CENTURIESAHEADOFITSTIMEINCLUDINGDEVICESTHATCOULDHARNESSTHEPOWEROFTHENATURALELEMENTSSTORIESTELLOFENERGYCRYSTALSTHATPOWERED
EVERYTHINGFROMAIRSHIPSTOTHECITYSGREATLIGHTWHICHCOULDBESEENFROMMANYMILESAWAYTHESECRYSTALSWERENOTONLYSOURCESOFPOWERBUTALSOO
FHEALINGWITHABILITIESTOCUREAILMENTSANDPROLONGLIFEINPURSUITOFTHETRUTHMANYEXPLORERSHAVESETOUTTOFINDTHERELICSOFTHISONCEGREAT
CITYTHEYTRAVELTOREMOTEISLANDSDIVEINTOTHEDEPTHSOFTHEOCEANANDSTUDYANCIENTSCRIPTSINDUSTYTOMESHOPINGTOFINDCLUESSOMEBELIEVETHA
TTHECITYCOULDBEFOUNDINTHEMEDITERRANEANWHILEOTHERSSUGGESTTHECARIBBEANOREVENLOCATIONSOFFTHECOASTSOFINDIAORJAPANTHELEGENDALS
OSPEAKSOFAGREATCATACLYSMTHATLEDTOTHECITYSDOWNFALLSOMESAYITWASAVOLCANOOTHERSAMASSIVEEARTHQUAKEANDYETOTHERSBELIEVEITWASAFLO
ODTHATCAUSEDTHECITYTOSINKINTOTHESEALEAVINGBEHINDONLYECHOESOFITSFORMERGLORYINMYTHSANDLEGENDSSCATTEREDACROSSTHEWORLDTHESEST
ORIESHAVEBEENTOLDANDRETOLDTHROUGHGENERATIONSOFTENADORNEDWITHNEWDETAILSORINTERPRETEDINDIFFERENTWAYSSCHOLARSDEBATETHECREDIB
ILITYOFTHESEACCOUNTSWITHSOMEASSERTINGTHATATLANTISWASREALPERHAPSANEXAGGERATIONOFASMALLERHISTORICALEVENTORCITYSTATEOTHERSAR
GUEITWASPURELYAPHILOSOPHICALALLEGORYCREATEDBYPLATOTODISCUSSHISTHEORIESOFCIVILIZATIONDESPITETHESKEPTICISMTHEALLUREOFATLANT
ISREMAINSSTRONGWITHITSMYSTERIESLYINGINWAITFORTHOSEBOLDENOUGHTOUNCOVERTHEMASTHESEARCHCONTINUESMODERNTECHNOLOGYAIDSINTHEQUE
STUSINGSATELLITEIMAGERYANDDEEPSEAEXPLORATIONEQUIPMENTTOSCANTHEOCEANFLOORFORSIGNSOFANCIENTHUMANSETTLEMENTSEACHNEWPIECEOFEV
IDENCEBRINGSAWAVEOFEXCITEMENTSUGGESTINGTHATPERHAPSTHESTORYOFATLANTISISMORETHANJUSTAMYTHINDEEDTHESECRETOFATLANTISWHETHERIT
BEALOSTCIVILIZATIONORAMONUMENTALLESSONFROMHISTORYCONTINUESTOINFLUENCEMODERNCULTUREANDEXPLORATIONTHEPOSSIBILITYTHATSUCHAPL
ACEONCEEXISTEDCHALLENGESOURUNDERSTANDINGOFHUMANHISTORYANDOURCAPACITYFORTECHNOLOGICALADVANCEMENTTHELEGENDOFATLANTISISAREMI
NDEROFTHEPOWEROFHUMANCURIOSITYANDTHEENDLESSPURSUITOFKNOWLEDGEWHETHERWEEVERFINDATLANTISORNOTTHEJOURNEYOFSEEKINGITTEACHESUS
ABOUTOURPASTANDOPENSOURMINDSTOTHEPOSSIBILITIESOFTHEFUTURETHESTORYOFATLANTISISNOTJUSTABOUTALOSTCITYBUTABOUTTHEQUESTFORKNOW
LEDGEANDTHEEXPLORATIONOFTHEUNKNOWNITCHALLENGESUSTOKEEPLOOKINGQUESTIONINGANDWONDERINGABOUTTHEVASTMYSTERIESOFOURWORLDTHESEC
RETOFATLANTISTHELOSTCITYREMAINSONEOFTHEGREATESTMYSTERIESOFTHEANCIENTWORLDITSSTORYECHOINGTHROUGHAGESASABEACONFORTHOSEWHOSE
EKTHETRUTHBEHINDTHEMYTHSTHEFASCINATIONWITHATLANTISWILLUNDOUBTEDLYCONTINUEINSPIRINGFUTUREGENERATIONSTOEXPLOREIMAGINEANDDRE
AMTHISTEXTINCLUDESTHEMATICREPETITIONANDISCRAFTEDTOFACILITATETHEANALYSISOFTHEVIGENERECIPHERSENCRYPTIONPATTERNS
```

The keyword was guessed in the first try based on the lab document that gives an example.

8) **What strategies can you use to refine your keyword guesses if the plaintext is not immediately recognizable?**

(5 total points)

We can look for common English words like the, and, or, if, to,etc. We can identify repeated patterns in decrypted text. If that doesn't work we could try out different combinations from the

corresponding alphabets we found in the steps before. Another thing we could try would be to rearrange the letters of the keyword based on the decrypted plaintext.

9)

Submit your documented python code as Lab03_part01.py to canvas.

(10 total points for working code. No points awarded if the code is copy/pasted from someone else.)

Submitted.