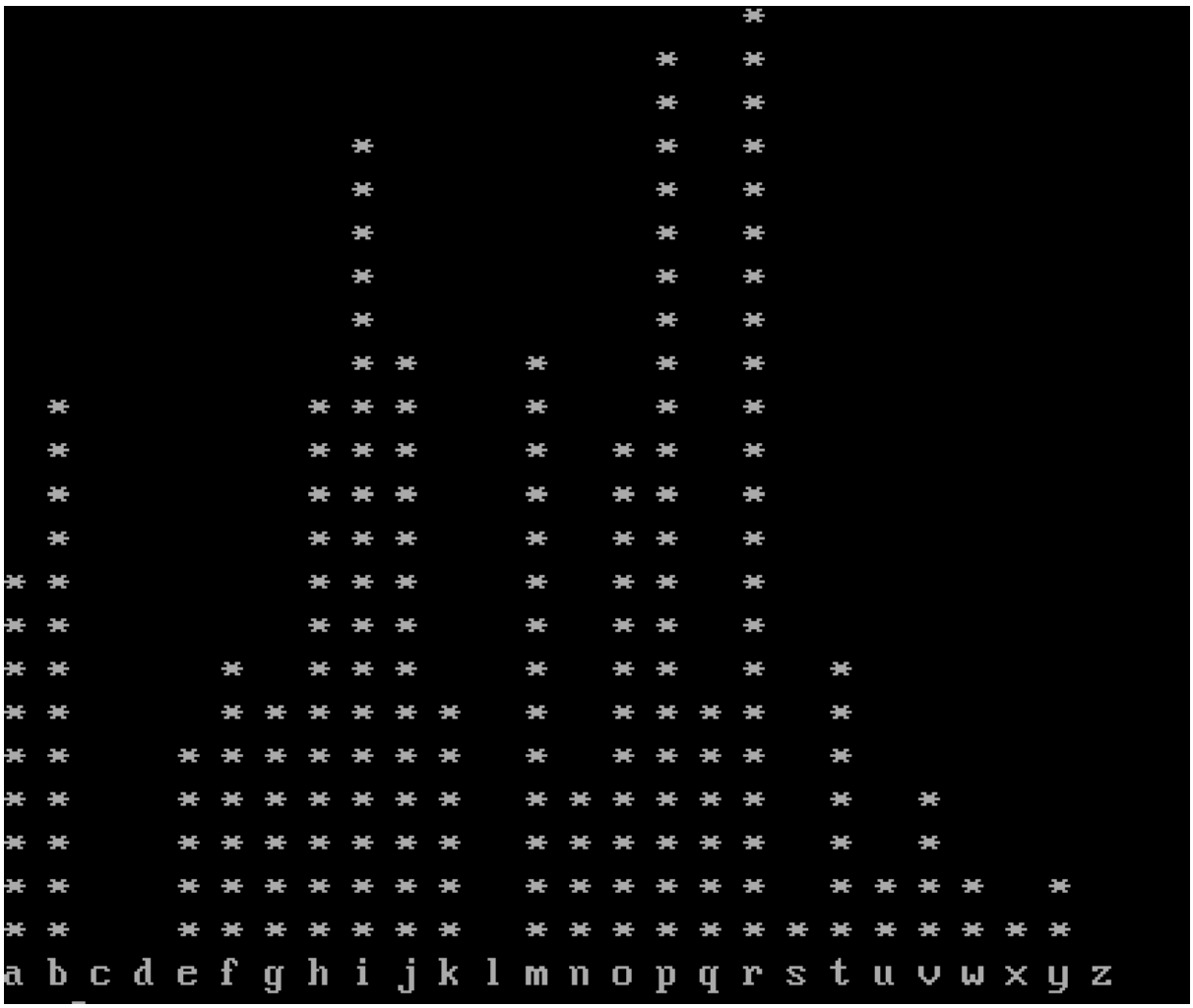
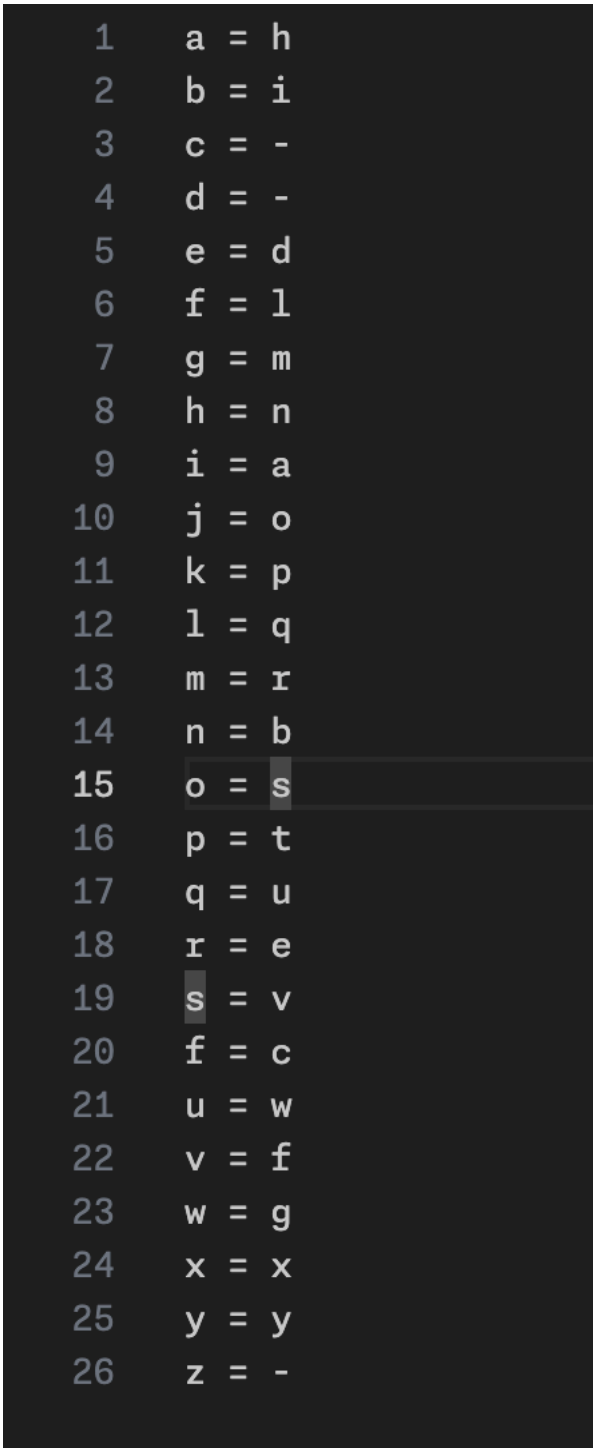
CText-1.txt

The cipher text from CText-1.txt is encrypted using monoalphabetic cipher.

- The first step that is used in decrypting CText1 is by finding which letter has the most frequency by using the function that shows the frequency distribution graph of letters in Krypto.



- From the above diagram it can be seen that 'R' is the most frequently seen character in the text file.
- By using the diagram, 'R' character is mapped to 'E' since E is the most frequent character in the alphabet. 'T', 'A', 'O', 'I', 'N', 'S', 'H' and 'R' are mapped according to what characters appear frequently after 'R'.
- After substituting the characters using Krypto, the following characters are used to decrypt the cipher text.


a = h
b = i
c = -
d = -
e = d
f = l
g = m
h = n
i = a
j = o
k = p
l = q
m = r
n = b
o = s
p = t
q = u
r = e
s = v
f = c
u = w
v = f
w = g
x = x
y = y
z = -

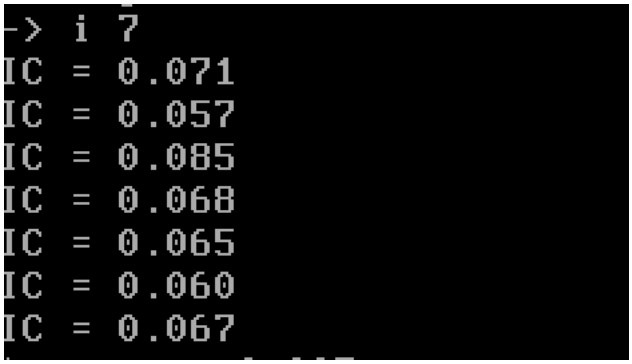
The following is the decrypted string using the above keys for CText-1

```
lectures at cambridge an intention which i was subseluently
induced to alter the substance of a considerable portion of it
has however appeared among the preliminary chapters of the
mechanical part of the encyclopedia metropolitana
altogether superfluous to examine to what extent it deserves to be
esteemed useful or essential in a representative republic or how
much more merit it may be entitled to as a defense against the
oppressions of an hereditary monarch than as a barrier to the
```

CText-2.txt

The cipher text from CText-2.txt is encrypted using Vigenère cipher.

- The first step that is used to decrypt the cipher text is to find the length of the key. To find the length of the key, an index of coincidence is needed. Index of coincidence is found by using the function to calculate the index of coincidence from Krypto.



- By using the above function, we take index of coincidence as 7 since it is the closest index of coincidence as English alphabet.
- The ciphertext is split into columns based on key length and count the frequencies of letter in each group.
- Count the shift by assuming the most frequent characters ‘E’, ‘T’ and other common letters.
- After shifting, we get QAYEQII as the encrypted key. After decrypting, we get VAMPIRE as the key for decryption.

The following is the decrypted plain text for CText-2

```
1   tyranny of popular magistrates in a popular government discussions
2   of this kind would be more curious than beneficial as all are
3   satisfied of the utility of the institution and of its friendly
4   aspect to liberty but i must acknowledge that i cannot readily
5   discern the inseparable connection between the existence of liberty
6   if after such dissolution the house of representatives again passes the
7   proposed law with or without any amendments which have been made
8   one fine day it occurred to the members of the body that they
```