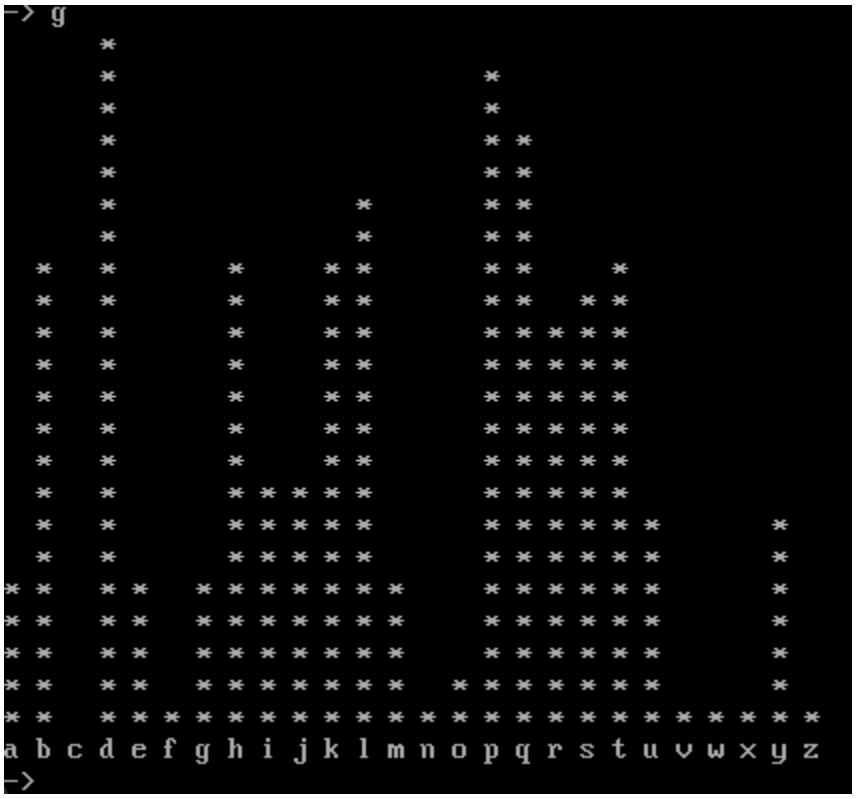
Report two- Task 4

In your report, describe the statistical properties of Ctext-3 and discuss how they compare them with those of Ctext-1 and Ctext-2, remembering that Ctext-1 and Ctext-3 are associated with the same plaintext. Include a comparative graph of the letter frequency distributions. Write your report in a file called Report2.pdf.

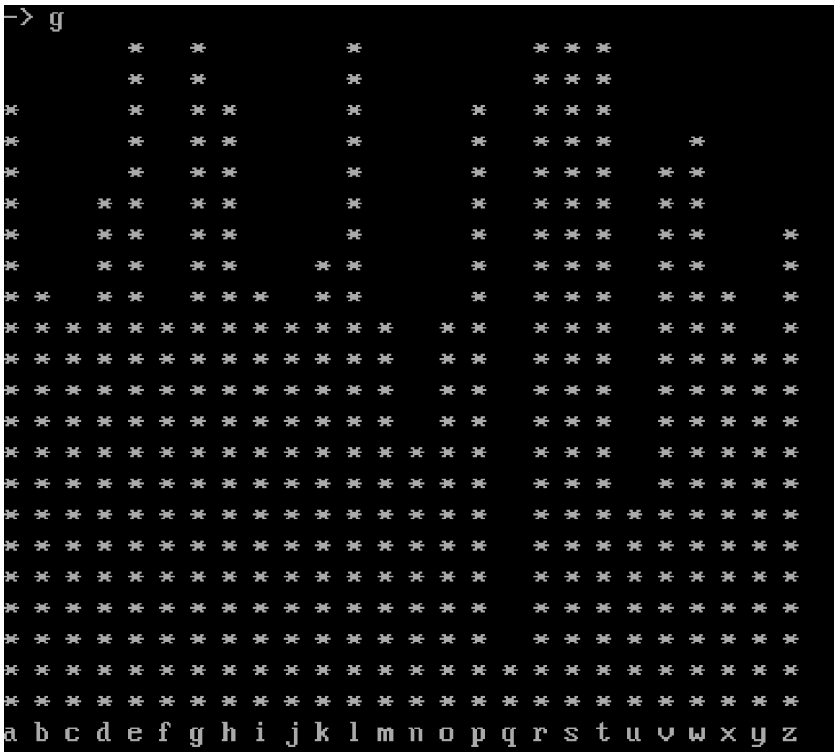
Ctext-1 Frequency distribution graph:



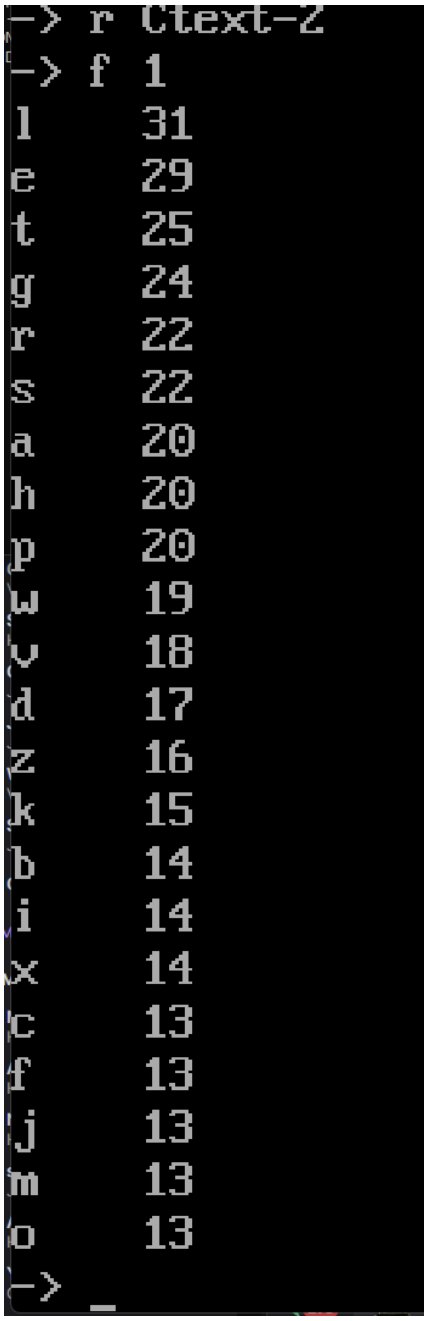
Most frequent character in the string descending order:

```
-> f 1
d    45
p    43
q    38
l    34
t    31
b    30
h    30
k    30
s    29
r    27
j    17
i    16
u    15
y    14
a    11
e    11
g    11
m    10
o     5
f     3
w     3
n     2
->
```

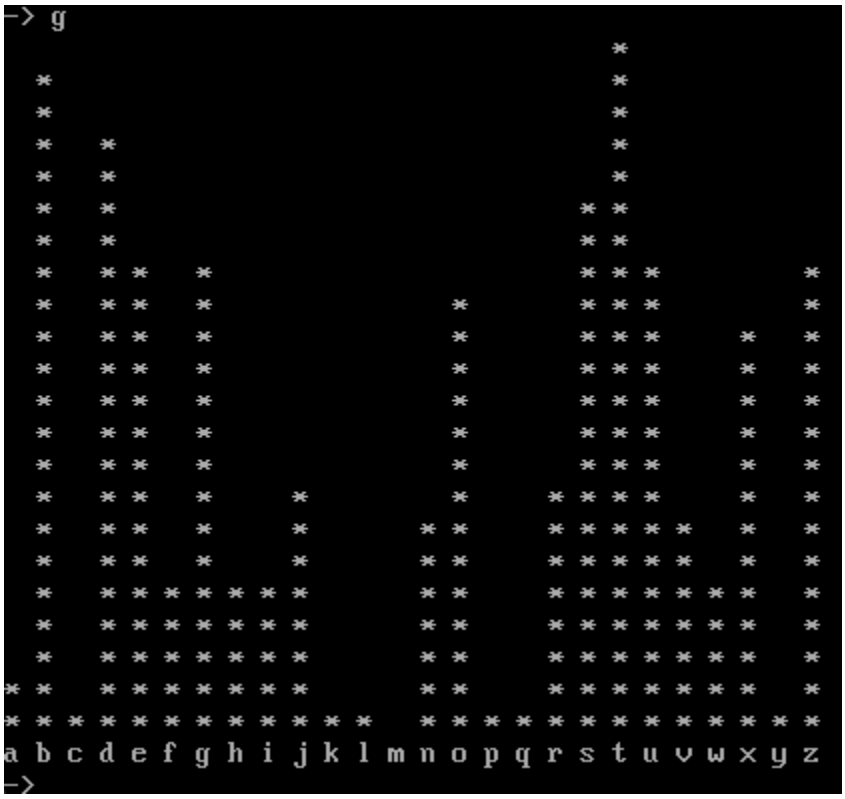
Ctext-2 Frequency distribution graph:

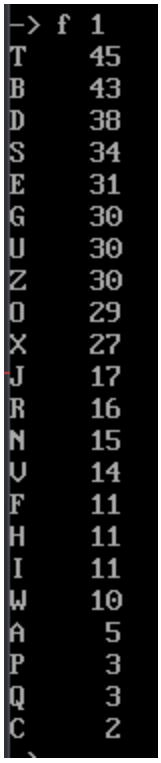


Most frequent character in the string descending order:



Ctext- 3 Frequency distribution graph:





Ctext-3(kamasutra) and Ctext-1(substitution) is using monoalphabetic cipher, a monoalphabetic cipher uses the same mapping for each letter of the plaintext to the corresponding letter in the ciphertext. This makes the cipher vulnerable to frequency analysis, as the frequency distribution of letters in the ciphertext will be similar to that of the plaintext. Whereas Ctext-2(Vigenere) is using polyalphabetic cipher, in a polyalphabetic cipher, each letter in the plaintext is replaced by a different letter or symbol, and the mapping between the plaintext and ciphertext letters changes for each block of the text. This makes it more difficult for an attacker to crack the cipher, since frequency analysis, which is a common method for breaking monoalphabetic ciphers, becomes less effective.

So, to summarize, the main difference between a polyalphabetic cipher and a monoalphabetic cipher is the number of alphabets used to encrypt the plaintext, with polyalphabetic cipher being more secure due to its changing mappings.

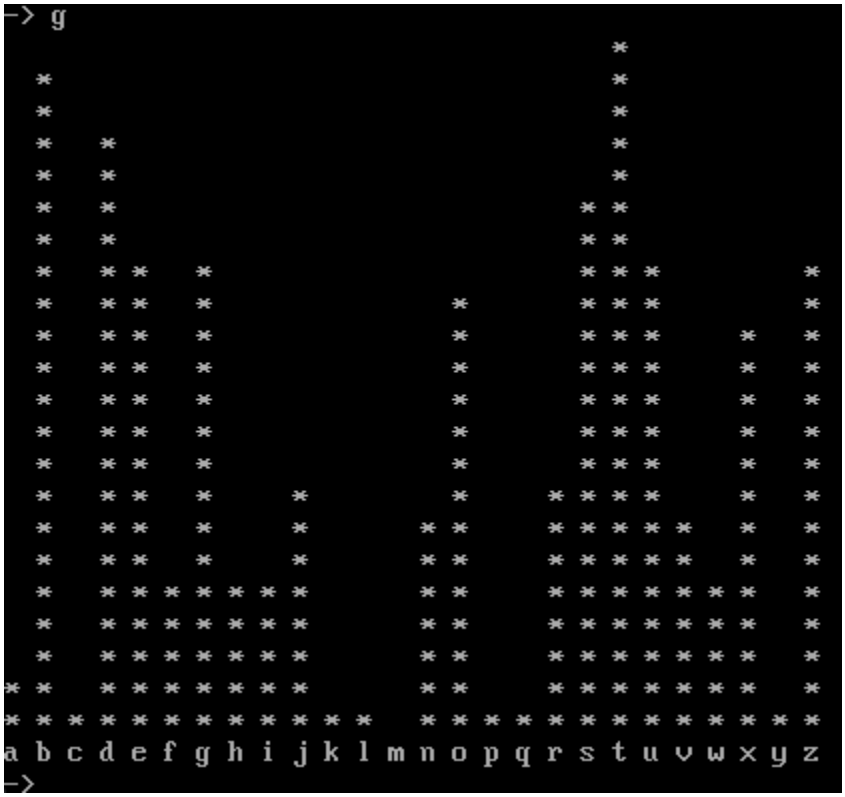
Discuss a way to decrypt the Kama Sutra cipher without using the key. Show your argument by decrypting the ciphertext Ctext-3 assuming that you don't know the key. The discussion will need to be written in the same file Report2.pdf.

Using statistical analysis

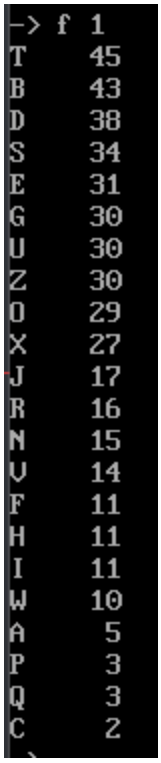
Cipher Text:
DBWGRZV XSSZTR FSDJ YSZXBUGX DSXQO EVWGXBZZV
XHBDBXETDGLTR AV B OJBZZ WTDXTUEBIT SF
XDVOEBZO SD FDBIJTUEO OTE GU B JBEDGC SF
IZBOO KNTUXHTR SD ONWTD XSSZTR JBIJB SD FGUTD
IDBGUTR XDVOEBZZGUT JBETDGBZO GF JBIJBO UTYTD
ADTBXH EHT ONDFBXT ES TDNWE BUR DTJBGU RTTW
NURTDIDSNUR EHTV XSSZ JNXH JSDT OZSPZV BUR
EHNO BZZSP BJWZT EGJT ES ONOEBGU XDVOEBZ WDTXGWGEBEGSU BUR
IDSPEH DTONZEGUI GU EHT FSDJBEGSU SF XSBDOTD IDBGUTR UTBDZV
XSJWZTETZV XDVOEBZZGUT GIUTSNO DSXQO ONAOTKNTUE ES FGUBZ
XDVOEBZZGLBEGSU
BUR OSZGRGFGXBEGSU ONXH DSXQO XBU AT TCHNJTR AV

Plain Text:
rapidly cooled form volcanic rocks typically characterized by a small
percentage of crystals or fragments set in a matrix of glass quenched
or super cooled magma or finer grained crystalline materials if magmas
never breach the surface to erupt and remain deep underground they cool
much more slowly and thus allow ample time to sustain crystal
precipitation and growth resulting in the formation of coarser
grained nearly completely crystalline igneous rocks subsequent to
final crystallization and solidification such rocks can be exhumed by

Frequency distribution graph:



Most frequent character in the string descending order:



NUOSKQCXVYBARDJMPWETGIFHZL

N	O	K	C	V	B	R	J	P	E	G	F	Z
U	S	Q	X	Y	A	D	M	W	T	I	H	L

‘T’ = ‘E’:
‘E’ = ‘T’:

```
XDVOTBZO SD FDBIJEUTO OET GU B JBTDGC SF
XDVOEBZO SD FDBIJTUEO OTE GU B JBEDGC SF

IZBOO KNEUXHER SD ONWED XSSZER JBIJB SD FGUED
IZBOO KNTUXHTR SD ONWTD XSSZTR JBIJB SD FGUTD

IDBGUER XDVOTBZZGUE JBTEDGBZO GF JBIJBO UEYED
IDBGUTR XDVOEBZZGUT JBETDGBZO GF JBIJBO UTYTD

ADEBXH THE ONDFBXE TS EDNWT BUR DEJBGU REEW
ADTBXH EHT ONDFBXT ES TDNWE BUR DTJBGU RTTW

NUREDIDSNUR THEV XSSZ JNXH JSDE OZSPZV BUR
NURTDIDSNUR EHTV XSSZ JNXH JSDT OZSPZV BUR

THNO BZZSP BJWZE TGJE TS ONOTBGU XDVOTBZ WDEXGWGTBTGSU BUR
EHNO BZZSP BJWZT EGJT ES ONOEBGU XDVOEBZ WDTXGWGEBEGSU BUR

IDSPTH DEONZTGUI GU THE FSDJBTGSU SF XSBDOED IDBGUER UEBDZV
IDSPEH DTONZEGUI GU EHT FSDJBEGSU SF XSBDOTD IDBGUTR UTBDZV

XSJWZETEZV XDVOTBZZGUE GIUESNO DSXQO ONAOEKNEUT TS FGUBZ XDVOTBZZGLBTGSU
XSJWZTETZV XDVOEBZZGUT GIUTSNO DSXQO ONAOTKNTUE ES FGUBZ XDVOEBZZGLBEGSU

BUR OSZGRGFGXBTGSU ONXH DSXQO XBU AE ECHNJER AV->
```

‘B’ = ‘A’

‘A’ = ‘B’

```
XDVOTAZO SD FDAIJEUTO OET GU A JATDGC SF
XDVOEBZO SD FDBIJTUEO OTE GU B JBEDGC SF

IZAOO KNEUXHER SD ONWED XSSZER JAIJA SD FGUED
IZBOO KNTUXHTR SD ONWTD XSSZTR JBIJB SD FGUTD

IDAGUER XDVOTAZZGUE JATEDGAZO GF JAIJAO UEYED
IDBGUTR XDVOEBZZGUT JBETDGBZO GF JBIJBO UTYTD

BDEAXH THE ONDFAXE TS EDNWT AUR DEJAGU REEW
ADTBXH EHT ONDFBXT ES TDNWE BUR DTJBGU RTTW

NUREDIDSNUR THEV XSSZ JNXH JSDE OZSPZV AUR
NURTDIDSNUR EHTV XSSZ JNXH JSDT OZSPZV BUR

THNO AZZSP AJWZE TGJE TS ONOTAGU XDVOTAZ WDEXGWGTATGSU AUR
EHNO BZZSP BJWZT EGJT ES ONOEBGU XDVOEBZ WDTXGWGEBEGSU BUR

IDSPTH DEONZTGUI GU THE FSDJATGSU SF XSADOED IDAGUER UEADZV
IDSPEH DTONZEGUI GU EHT FSDJBEGSU SF XSBDOTD IDBGUTR UTBDZV

XSJWZETEZV XDVOTAZZGUE GIUESNO DSXQO ONBOEKNEUT TS FGUAZ XDVOTAZZGLATGSU
XSJWZTETZV XDVOEBZZGUT GIUTSNO DSXQO ONAOTKNTUE ES FGUBZ XDVOEBZZGLBEGSU

AUR OSZGRGFGXATGSU ONXH DSXQO XAU BE ECHNJER BV->
```

‘F’ = remains the same
‘H’ = remains the same
‘F’ = ‘H’
‘S’ = ‘O’

```
XDVOTAZD OD FDAIJEUTO OET GU A JATDGC OF
XDVOEBZD SD FDBIJTUEO OTE GU B JBEDGC SF

IZAOO KNEUXHER OD ONWED XOOZER JAIJA OD FGUED
IZBOO KNTUXHTR SD ONWTD XSSZTR JBIJB SD FGUTD

IDAGUER XDVOTAZZGUE JATEDGAZD GF JAIJAO UEYED
IDBGUTR XDVOEBZZGUT JBETDGBZD GF JBIJBO UTYTD

BDEAXH THE ONDFAXE TO EDNWT AUR DEJAGU REEW
ADTBXH EHT ONDFBXT ES TDNWE BUR DTJBGU RTTW

NUREDIDONUR THEV XOOZ JNXH JODE OZDPZV AUR
NURTDIDSNUR EHTV XSSZ JNXH JSDT OZSPZV BUR

THNO AZZDP AJWZE TGJE TO ONOTAGU XDVOTAZ WDEXGWGTATGOU AUR
EHNO BZZSP BJWZT EGJT ES ONOEBGU XDVOEBZ WDTXGWGEBEGSU BUR

IDOPTH DEONZTGUI GU THE FODJATGOU OF XOADOED IDAGUER UEADZV
IDSPEH DTONZEGUI GU EHT FSDJBEGSU SF XSBDOTD IDBGUTR UTBDZV

XOJWZETEZV XDVOTAZZGUE GIUEONO DOXQO ONBOEKNEUT TO FGUAZ XDVOTAZZGLATGOU
XSJWZTETZV XDVOEBZZGUT GIUTSNO DSXQO ONAOTKNTUE ES FGUBZ XDVOEBZZGLBEGSU

AUR OOZGRGFGXATGOU ONXH DOXQO XAU BE ECHNJER BV->
```

Other than of is or
‘D’ = ‘R’

```
XRVOTAZD OR FRAIJEUTO OET GU A JATRGC OF
XDVOEBZD SD FDBIJTUEO OTE GU B JBEDGC SF

IZAOO KNEUXHED OR ONWER XOOZED JAIJA OR FGUER
IZBOO KNTUXHTR SD ONWTD XSSZTR JBIJB SD FGUTD

IRAGUED XRVOTAZZGUE JATERGAZD GF JAIJAO UEYER
IDBGUTR XDVOEBZZGUT JBETDGBZD GF JBIJBO UTYTD

BREAXH THE ONRFAXE TO ERNWT AUD REJAGU DEEW
ADTBXH EHT ONDFBXT ES TDNWE BUR DTJBGU RTTW

NUDERIRONUD THEV XOOZ JNXH JORE OZDPZV AUD
NURTDIDSNUR EHTV XSSZ JNXH JSDT OZSPZV BUR

THNO AZZDP AJWZE TGJE TO ONOTAGU XRVOTAZ WREXGWGTATGOU AUD
EHNO BZZSP BJWZT EGJT ES ONOEBGU XDVOEBZ WDTXGWGEBEGSU BUR

IROPTH REONZTGUI GU THE FORJATGOU OF XDAROER IRAGUED UEARZV
IDSPEH DTONZEGUI GU EHT FSDJBEGSU SF XSBDOTD IDBGUTR UTBDZV

XOJWZETEZV XRVOTAZZGUE GIUEONO ROXQO ONBOEKNEUT TO FGUAZ XRVOTAZZGLATGOU
XSJWZTETZV XDVOEBZZGUT GIUTSNO DSXQO ONAOTKNTUE ES FGUBZ XDVOEBZZGLBEGSU

AUD OOZGDGFGXATGOU ONXH ROXQO XAU BE ECHNJED BV->
```

…etc