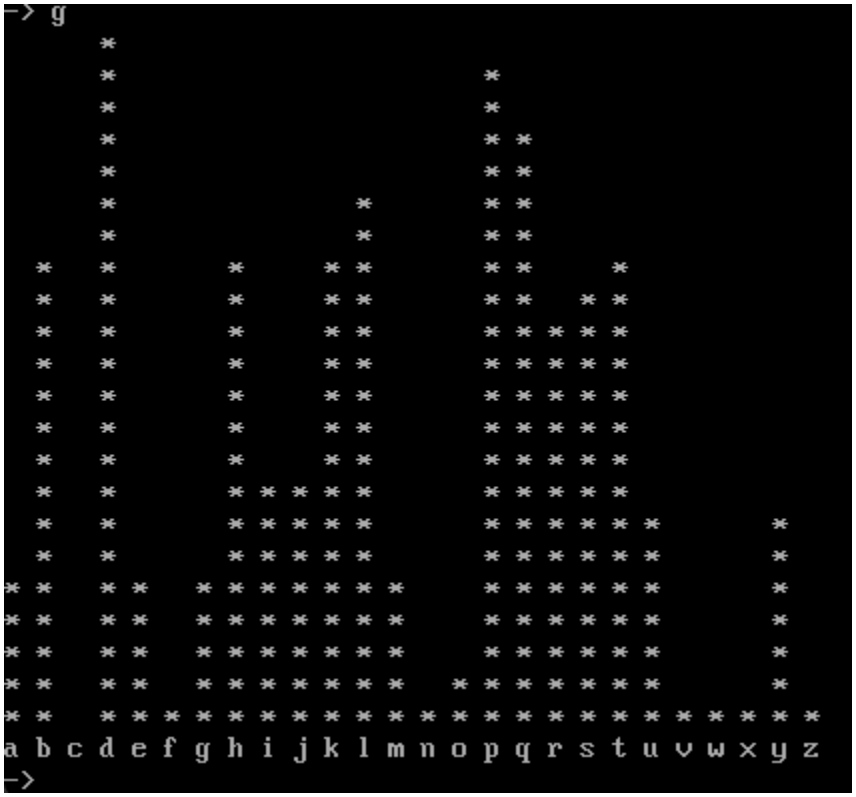
Task one

Ctext-1: monoalphabetic cipher

Cipher Text:
qpmbihy rllhdi glqj vlhrpkbr qlrfs tymbrphhy rapqprtdqbzdi oy p sjphh
mdqrdktped lg rqystphs lq gqpejdkts sdt bk p jptqbx lg ehpss nudkradi
lq sumdq rllhdi jpejp lq gbkdq eqpbkdi rqystphhbkd jptdqbphs bg jpejps
kdvdq oqdpra tad suqgprd tl dqumt pki qdjpbk iddm ukidqeqluki tady rllh
jura jlqd shlwhy pki taus phhlw pjmhd tbjd tl sustpbk rqystph
mqdrbmbtptblk pki eqlwta qdsuhtbke bk tad glqjptblk lg rlpqsdq
eqpbkdi kdpqhy rljmhdtdhy rqystphhbkd bekdlus qlrfs suosdnudkt tl
gbkph rqystphhbzptblk pki slhbibgbrptblk sura qlrfs rpk od dxaujdi oy

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:

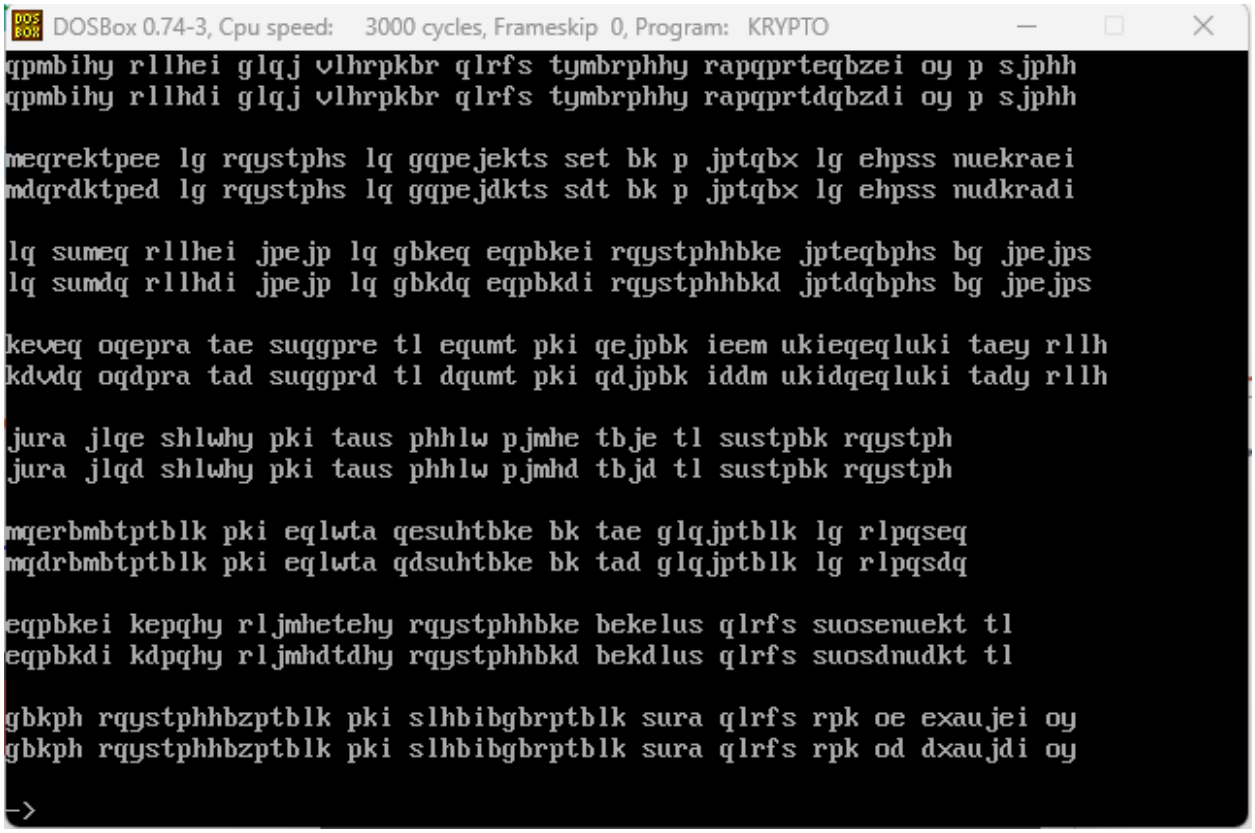


Most frequent character in the string descending order:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
p	o	r	i	d	g	e	a	b	c	f	h	j	k	l	m	n	q	s	t

u	v	w	x	y	z
u	v	w	x	y	z

‘D’ = ‘e’:



‘P’ is a single letter word most common is i or a, so try ‘p’ = ‘a’:

```
qambihy rllhei glqj vlhrakbr qlrfs tymbrahhy raaqarteqbzei oy a sjahh
qpmbihy rllhdi glqj vlhrpkbr qlrfs tymbrphhy rapqprtdqbzdi oy p sjphh

meqrektaee lg rqystahs lq gqaejekts set bk a jatqbx lg ehass nuekraei
mdqrdktped lg rqystphs lq gqpejdkts sdt bk p jptqbx lg ehpss nudkradi

lq sumeq rllhei jaeja lq gbkeq eqabkei rqystahhbke jateqbahs bg jaejas
lq sumdq rllhdi jpejp lq gbkdq eqpbkdi rqystphhbkd jptdqbphs bg jpejps

keveq oqeara tae suqgare tl equmt aki qejabk ieem ukieqeqluki taey rllh
kdvdq oqdpra tad suqgprd tl dqumt pki qdjpbk iddm ukidqeqluki tady rllh

jura jlqe shlwhy aki taus ahhlw ajmhe tbje tl sustabk rqystah
jura jlqd shlwhy pki taus phhlw pjmhd tbjd tl sustpbk rqystph

mqerbmbtatblk aki eqlwta qesuhtbke bk tae glqjatblk lg rlaqseq
mqdrbmbtptblk pki eqlwta qdsuhtbke bk tad glqjptblk lg rlpqsdq

eqabkei keaqhy rljmhetehy rqystahhbke bekelus qlrfs suosenuekt tl
eqpbkdi kdpqhy rljmhdtdhy rqystphhbkd bekdlus qlrfs suosdnudkt tl

gbkah rqystahhbzatblk aki slhbibgbratblk sura qlrfs rak oe exaujei oy
gbkph rqystphhbzptblk pki slhbibgbrptblk sura qlrfs rpk od dxaujdi oy
```

‘Tae’ most common trigram is the so ‘a’ = ‘h’

‘T’ = ‘t’

```
qambihy rllhei glqj vlhrakbr qlrfs tymbrahhy rhaqarteqbzei oy a sjahh
qpmbihy rllhdi glqj vlhrpkbr qlrfs tymbrphhy rapqprtdqbzdi oy p sjphh

meqrektaee lg rqystahs lq gqaejekts set bk a jatqbx lg ehass nuekrhei
mdqrdktped lg rqystphs lq gqpejdkts sdt bk p jptqbx lg ehpss nudkradi

lq sumeq rllhei jaeja lq gbkeq eqabkei rqystahhbke jateqbahs bg jaejas
lq sumdq rllhdi jpejp lq gbkdq eqpbkdi rqystphhbkd jptdqbphs bg jpejps

keveq oqearh the suqgare tl equmt aki qejabk ieem ukieqeqluki they rllh
kdvdq oqdpra tad suqgprd tl dqumt pki qdjpbk iddm ukidqeqluki tady rllh

jurh jlqe shlwhy aki thus ahhlw ajmhe tbje tl sustabk rqystah
jura jlqd shlwhy pki taus phhlw pjmhd tbjd tl sustpbk rqystph

mqerbmbtatblk aki eqlwth qesuhtbke bk the glqjatblk lg rlaqseq
mqdrbmbtptblk pki eqlwta qdsuhtbke bk tad glqjptblk lg rlpqsdq

eqabkei keaqhy rljmhetehy rqystahhbke bekelus qlrfs suosenuekt tl
eqpbkdi kdpqhy rljmhdtdhy rqystphhbkd bekdlus qlrfs suosdnudkt tl

gbkah rqystahhbzatblk aki slhbibgbratblk surh qlrfs rak oe exhujei oy
gbkph rqystphhbzptblk pki slhbibgbrptblk sura qlrfs rpk od dxaujdi oy
```

‘Surh’ most relatable word will be ‘such’, ‘r’ = ‘c’

```
qambihy cllhei glqj vlhcakbc qlcfs tymbcahhy chaqacteqbzei oy a sjahh
qpmbihy rllhdi glqj vlhrpkbr qlrfs tymbrphhy rapqprtdqbzdi oy p sjphh

meqcektaee lg cqystahs lq gqaejekts set bk a jatqbx lg ehass nuekchei
mdqrdktped lg rqystphs lq gqpejdkts sdt bk p jptqbx lg ehpss nudkradi

lq sumeq cllhei jaeja lq gbkeq eqabkei cqystahhbke jateqbahs bg jaejas
lq sumdq rllhdi jpejp lq gbkdq eqpbkdi rqystphhbkd jptdqbphs bg jpejps

keveq oqeach the suqgace tl equmt aki qejabk ieem ukieqeqluki they clll
kdvdq oqdpra tad suqgprd tl dqumt pki qdjpbk iddm ukidqeqluki tady rlll

juch jlqe shlwhy aki thus ahhlw ajmhe tbje tl sustabk cqystah
jura jlqd shlwhy pki taus phhlw pjmhd tbjd tl sustpbk rqystph

mqecbmbtatblk aki eqlwth qesuhtbke bk the glqjatblk lg claqseq
mqdrbmbtptblk pki eqlwta qdsuhtbke bk tad glqjptblk lg rlpqsdq

eqabkei keaqhy cljmhetehy cqystahhbke bekelus qlcfs suosenuekt tl
eqpbkdi kdpqhy rljmhdtdhy rqystphhbkd bekdlus qlrfs suosdnudkt tl

gbkah cqystahhbzatblk aki slhbibgbcatblk such qlcfs cak oe exhujei oy
gbkph rqystphhbzptblk pki slhbibgbrptblk sura qlrfs rpk od dxaujdi oy
```

‘Aki’ most common trigram that starts with a is ‘and’, ‘k’ = ‘n’, ‘i’ = ‘d:

```
qambdhy cllhed glqj vlhcanbc qlcfs tymbcahhy chaqacteqbzed oy a sjahh
qpmbihy rllhdi glqj vlhrpkbr qlrfs tymbrphhy rapqprtdqbzdi oy p sjphh

meqcentaee lg cqystahs lq gqaejents set bn a jatqbx lg ehass nuenched
mdqrdktped lg rqystphs lq gqpejdkts sdt bk p jptqbx lg ehpss nudkradi

lq sumeq cllhed jaeja lq gbneq eqabned cqystahhbne jateqbahs bg jaejas
lq sumdq rllhdi jpejp lq gbkdq eqpbkdi rqystphhbkd jptdqbphs bg jpejps

neveq oqeach the suqgace tl equmt and qejabn deem undeqeqlund they cllh
kdvdq oqdpra tad suqgprd tl dqumt pki qdjpbk iddm ukidqeqluki tady rllh

juch jlqe shlwhy and thus ahhlw ajmhe tbje tl sustabn cqystah
jura jlqd shlwhy pki taus phhlw pjmhd tbjd tl sustpbk rqystph

mqecbmbtatbln and eqlwth qesuhtbne bn the glqjatbln lg claqseq
mqdrbmbtptblk pki eqlwta qdsuhtbke bk tad glqjptblk lg rlpqsdq

eqabned neaqhy cljmhetehy cqystahhbne benelus qlcfs suosenuent tl
eqpbkdi kdpqhy rljmhdtdhy rqystphhbkd bekdlus qlrfs suosdnudkt tl

gbnah cqystahhbzatbln and slhbdbgbcatbln such qlcfs can oe exhujed oy
gbkph rqystphhbzptblk pki slhbibgbrptblk sura qlrfs rpk od dxaujdi oy
```

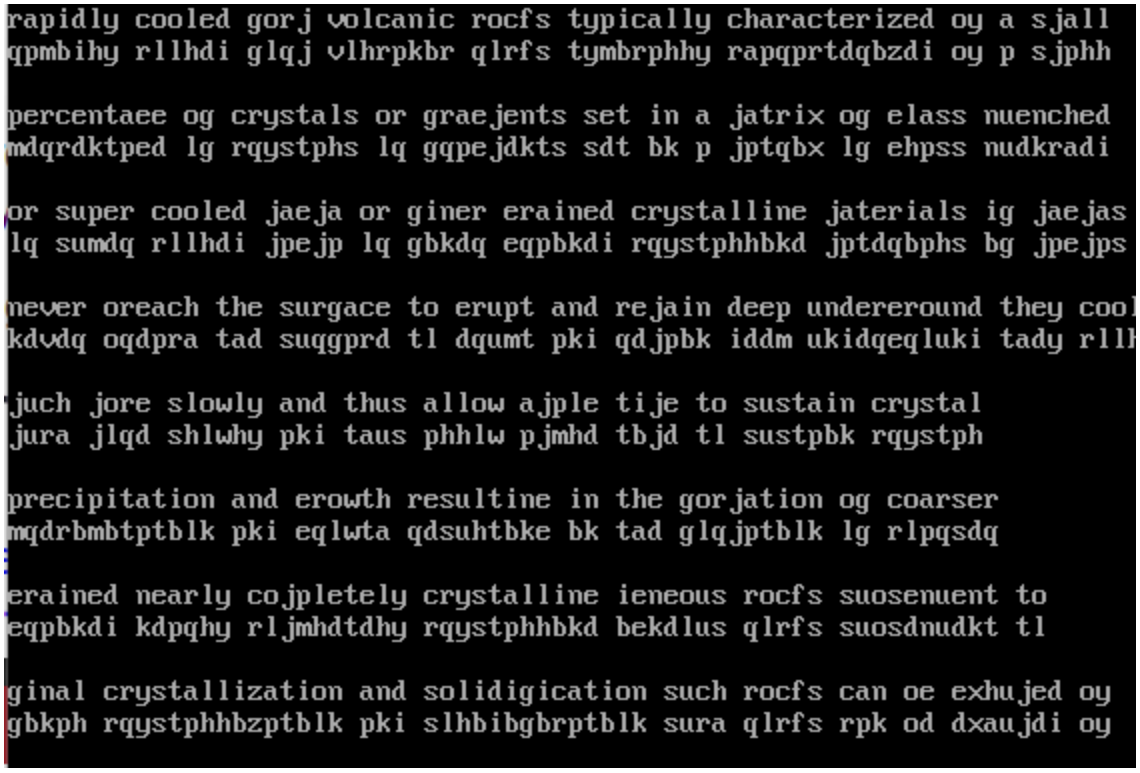
Chaqacteqbzed most relatable word is characterized, q = r, b = i , z =z

```
ramidhy cllhed glrj vlhcanic rlcfs tymicahhy characterized oy a sjahh
qpmbihy rllhdi glqj vlhrpkbr qlrfs tymbrphhy rapqprtdqbzdi oy p sjphh

mercentaee lg crystahs lr graejents set in a jatrix lg ehass nuenched
mdqrdktped lg rqystphs lq gqpejdkts sdt bk p jptqbx lg ehpss nudkradi

lr sumer cllhed jaeja lr giner erained crystahhine jateriahs ig jaejas
lq sumdq rllhdi jpejp lq gbkdq eqpbkdi rqystphhbkd jptdqbphs bg jpejps

never oreach the surgace tl erumt and rejain deem undererlund they cllh
kdvdq oqdpra tad suqgprd tl dqumt pki qdjpbk iddm ukidqeqluki tady rllh

juch jlre shlwhy and thus ahhlw ajmhe tije tl sustain crystah
jura jlqd shlwhy pki taus phhlw pjmhd tbjd tl sustpbk rqystph

mrecimitatiln and erlwth resuhtine in the glrjatiln lg clarser
mqdrbmbtptblk pki eqlwta qdsuhtbke bk tad glqjptblk lg rlpqsdq

erained nearhy cljmhetehy crystahhine ienelus rlcfs suosenuent tl
eqpbkdi kdpqhy rljmhdtdhy rqystphhbkd bekdlus qlrfs suosdnudkt tl

ginah crystahhizatiln and slhidigicatiln such rlcfs can oe exhujed oy
gbkph rqystphhbzptblk pki slhbibgbrptblk sura qlrfs rpk od dxaujdi oy
```

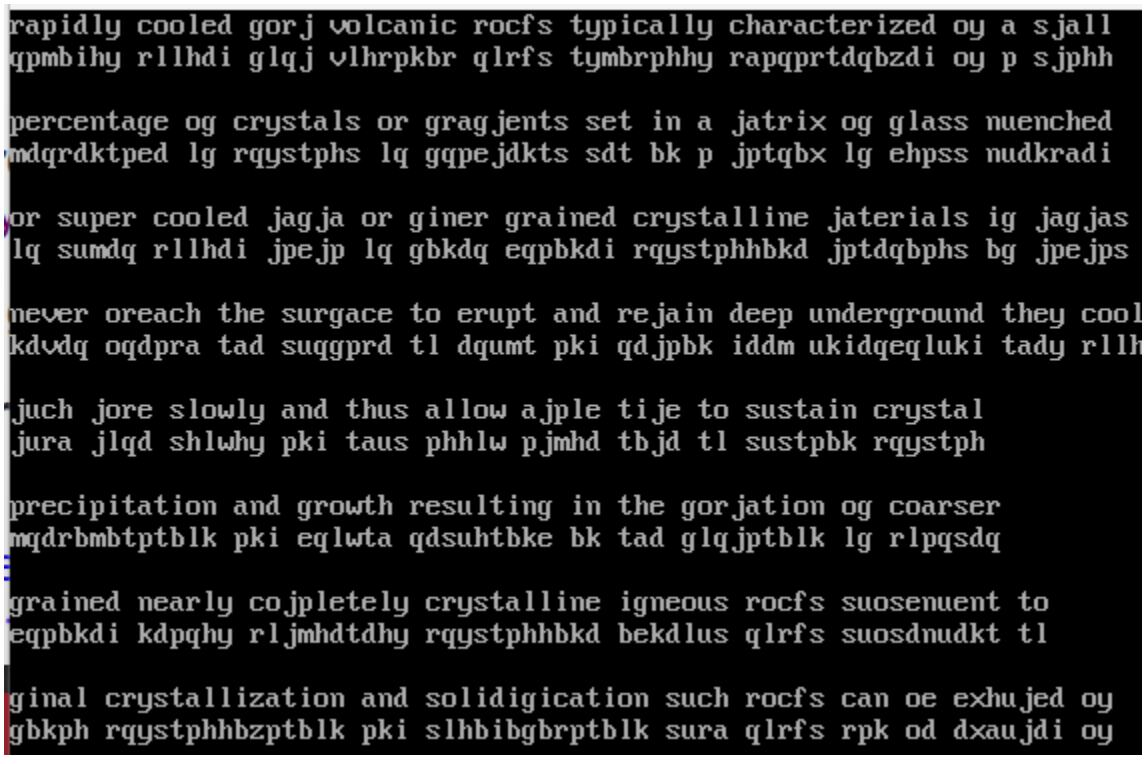
Tymicahhy the most relatable word is typically, m = p, h = l:

```
rapidly cllled glrj vllcanic rlcfs typically characterized oy a sjall
qpmbihy rllhdi glqj vlhrpkbr qlrfs tymbrphhy rapqprtdqbzdi oy p sjphh

percentaee lg crystals lr graejents set in a jatrix lg elass nuenched
mdqrdktped lg rqystphs lq gqpejdkts sdt bk p jptqbx lg ehpss nudkradi

lr super cllled jaeja lr giner erained crystalline jaterials ig jaejas
lq sumdq rllhdi jpejp lq gbkdq eqpbkdi rqystphhbkd jptdqbphs bg jpejps

never oreach the surgace tl erupt and rejain deep undererlund they clll
kdvdq oqdpra tad suqgprd tl dqumt pki qdjpbk iddm ukidqeqluki tady rllh

juch jlre sllwly and thus alllw ajple tije tl sustain crystal
jura jlqd shlwhy pki taus phhlw pjmhd tbjd tl sustpbk rqystph

precipitatiln and erlwth resultine in the glrjatiln lg clarser
mqdrbmbtptblk pki eqlwta qdsuhtbke bk tad glqjptblk lg rlpqsdq

erained nearly cljpletely crystalline ienelus rlcfs suosenuent tl
eqpbkdi kdpqhy rljmhdtdhy rqystphhbkd bekdlus qlrfs suosdnudkt tl

ginal crystallizatiln and sllidigicatiln such rlcfs can oe exhujed oy
gbkph rqystphhbzptblk pki slhbibgbrptblk sura qlrfs rpk od dxaujdi oy
```

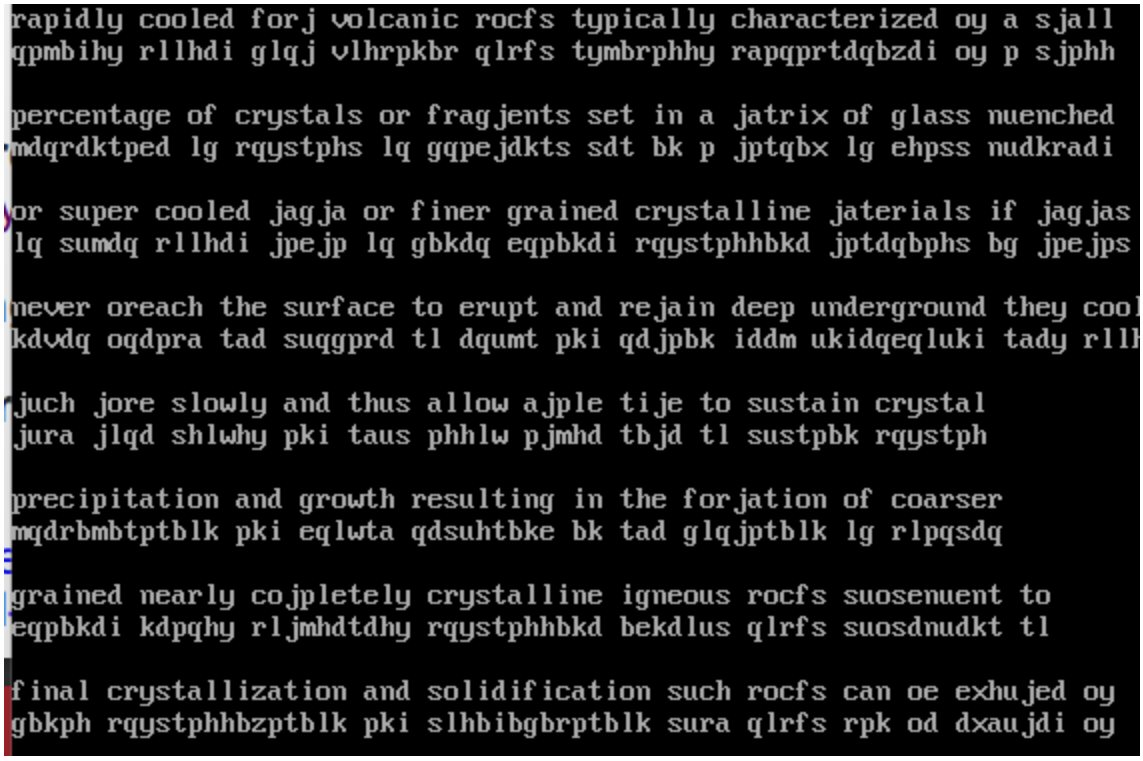
Vllcanic most relatable word is volcanic, l = o:



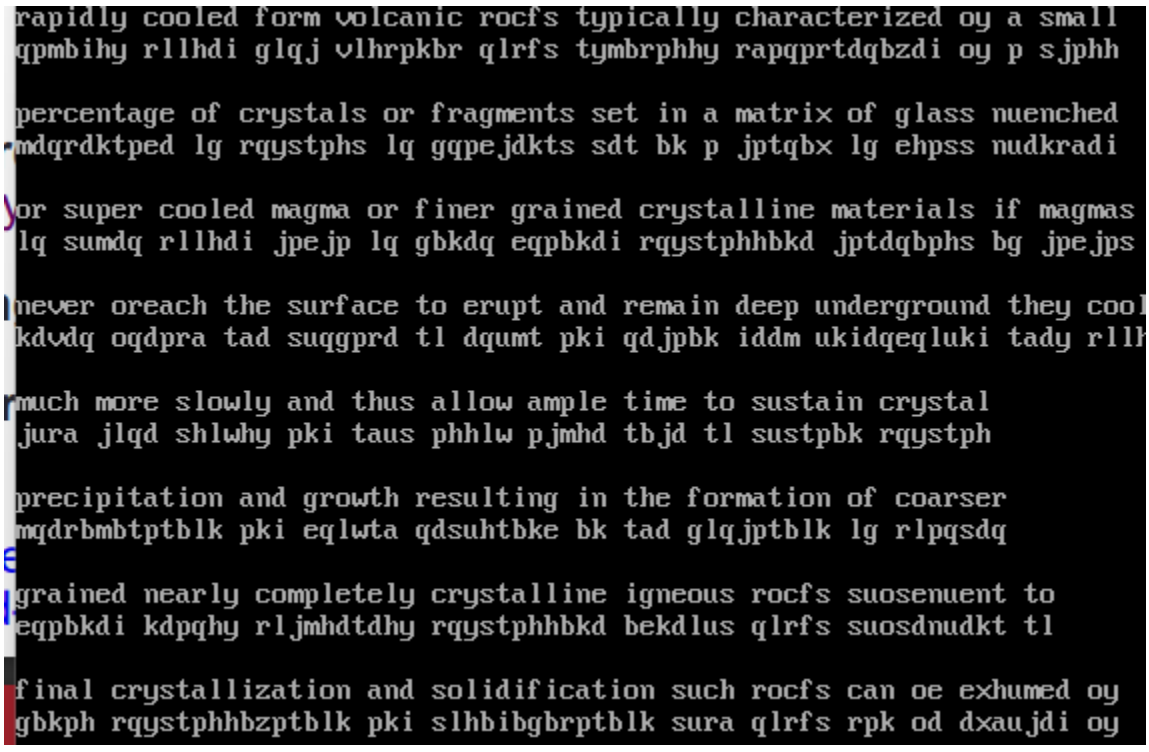
Percentaee most relatable word is percentage, e = g:



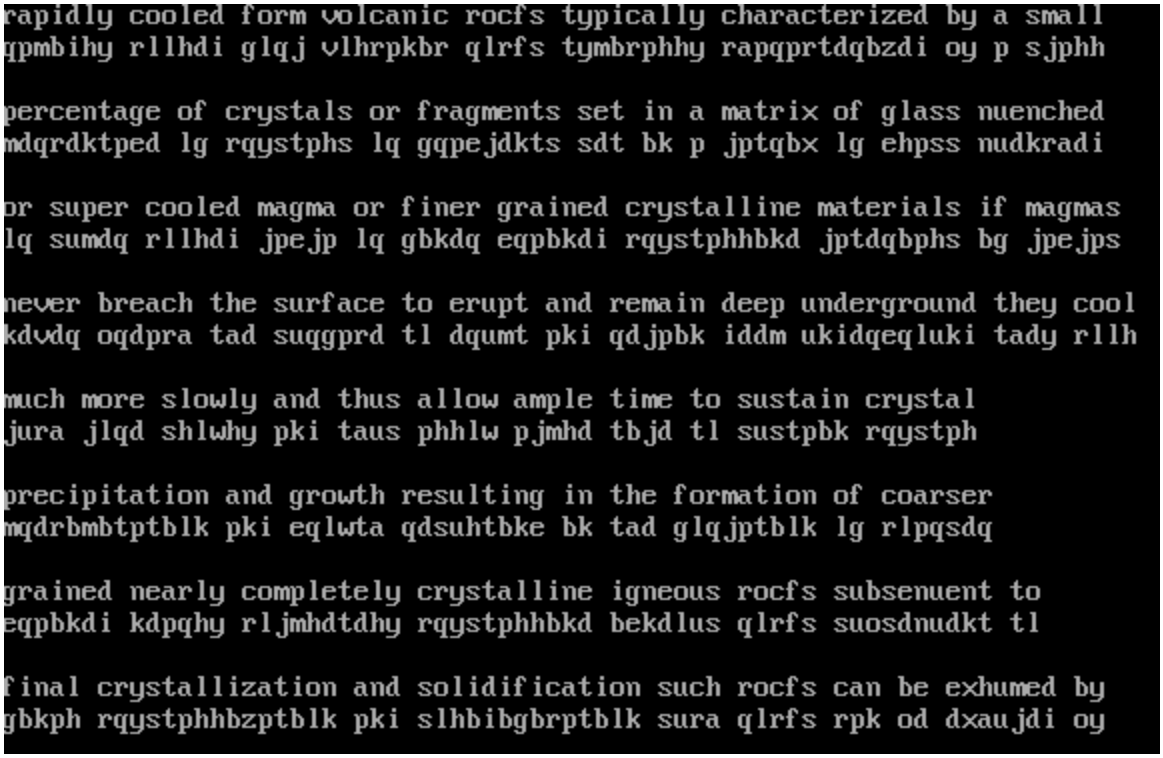
Percentage og crystals, og = of, g = f:



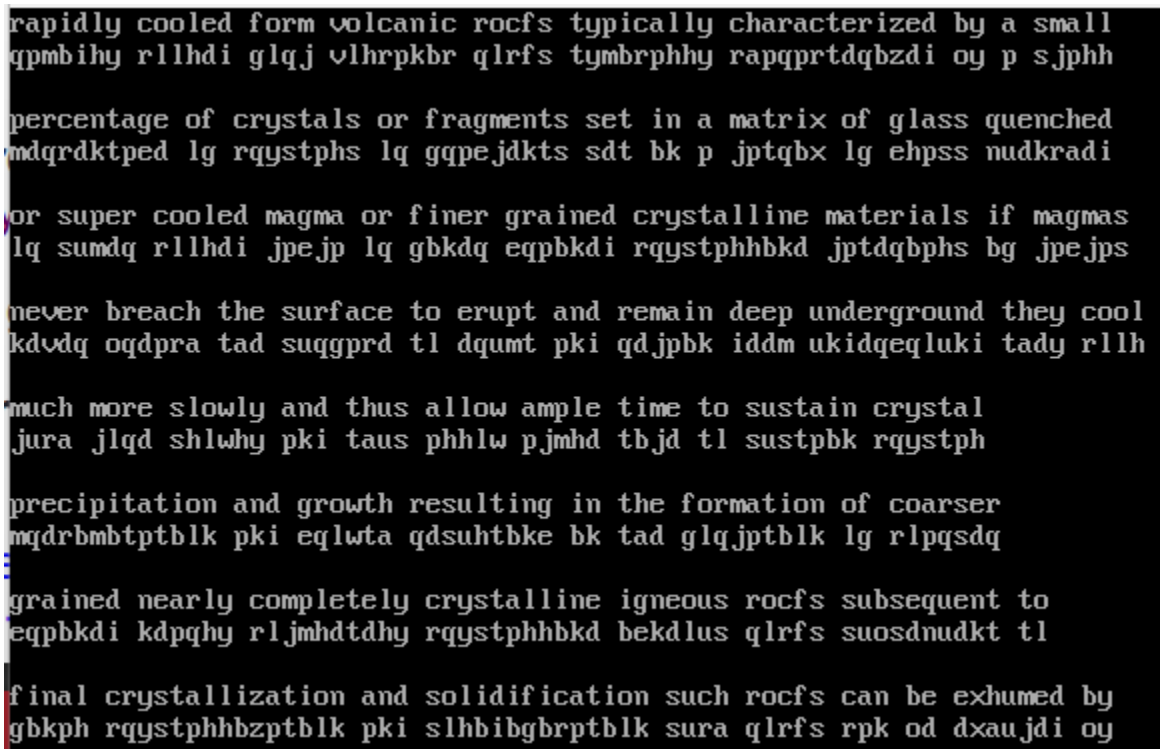
Fragjents relatable word is fragments, j = m:



Characterized oy a small, oy = by, o = b:



Nuenched most relatable word is quenched, n = q:



Rocfs most relatable word is rocks, f = k:

rapidly cooled form volcanic rocks typically characterized by a small
qpmbihy rllhdi glqj vlhrpkbr qlrfs tymbrphhy rapqprtdqbzdi oy p sjphh

percentage of crystals or fragments set in a matrix of glass quenched
mdqrdktped lg rqystphs lq gqpejdkts sdt bk p jptqbx lg ehpss nudkradi

or super cooled magma or finer grained crystalline materials if magmas
lq sumdq rllhdi jpejp lq gbkdq eqpbkdi rqystphhbkd jptdqbphs bg jpejps

never breach the surface to erupt and remain deep underground they cool
kdvdq oqdpra tad suqgprd tl dqumt pki qdjpbk iddm ukidqeqluki tady rllh

much more slowly and thus allow ample time to sustain crystal
jura jlqd shlwhy pki taus phhlw pjmhd tbjd tl sustpbk rqystph

precipitation and growth resulting in the formation of coarser
mqdrbmbtptblk pki eqlwta qdsuhtbke bk tad glqjptblk lg rlpqsdq

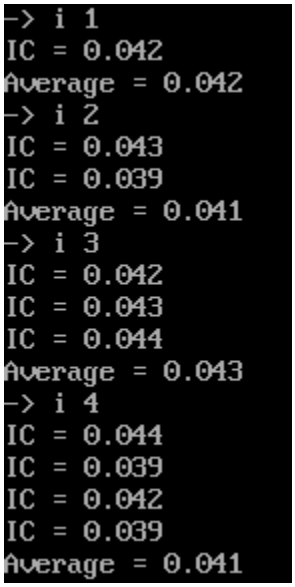
grained nearly completely crystalline igneous rocks subsequent to
eqpbkdi kdpqhy rljmhdtdhy rqystphhbkd bekdlus qlrfs suosdnudkt tl

final crystallization and solidification such rocks can be exhumed by
gbkph rqystphhbzptblk pki slhbibgbrptblk sura qlrfs rpk od dxaujdi oy

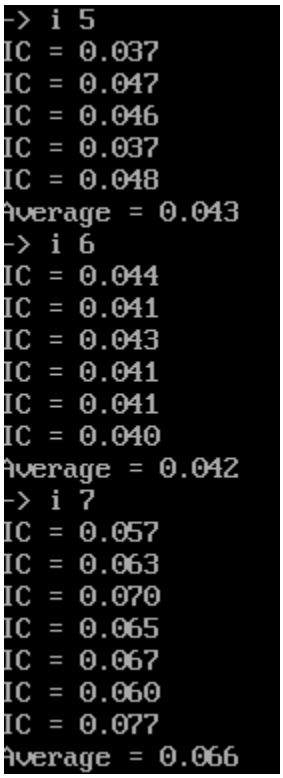
Ctext-2: Vigenère cipher

Checking the index of coincidence based on length:

Length 1 to 4:



Length: 5 to 7:

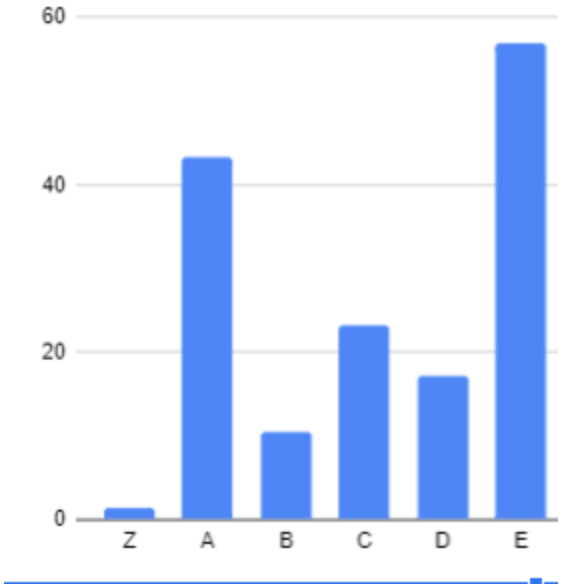


Length 8:

```
-> i 8
IC = 0.044
IC = 0.037
IC = 0.034
IC = 0.042
IC = 0.041
IC = 0.042
IC = 0.043
IC = 0.036
Average = 0.040
->
```

As you can see from the outcome the average IC of length 7 is more than 0.65 , but the average IC of length 8 & 6 is less than 0.65 .Therefore the keyword length should be 7.

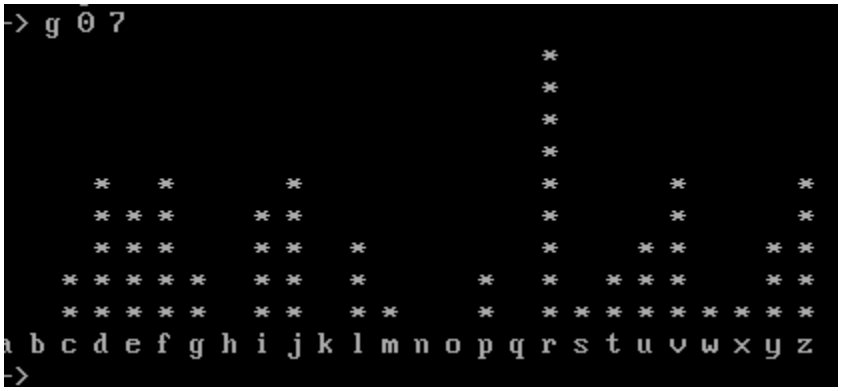
We will use the frequency of letter of the alphabet in the English language but starting from Z to E only.



Z = low, A = high, B = low, C & D = medium, E = high.

-> g i 7, i=0, 1, 2, 3, 4, 5, 6 to give the seven sub alphabets.
In this group, the most frequently used letter is “A”. Making assumption that this letter “A” (in ciphertext) is actually letter ‘e’ (in plaintext), we then check the rest to verify that the corresponding letters are sensible.

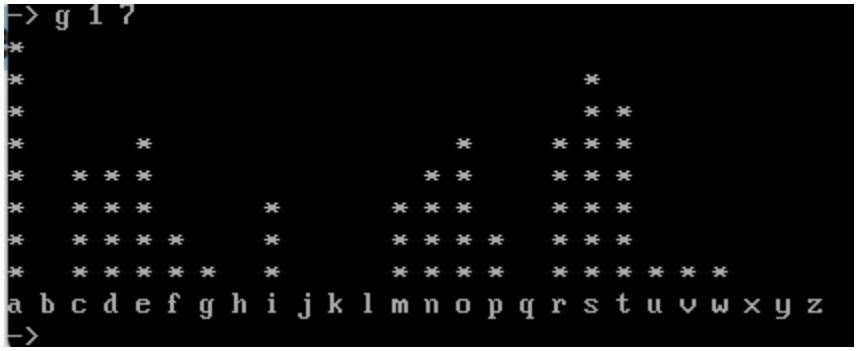
-> g 0 7



Based on the graph for the first sub alphabet:
QRSTUV frequency looks similar to the frequency of english.

Comparing side by side it looks similar, therefore the first sub alphabet is ‘R’

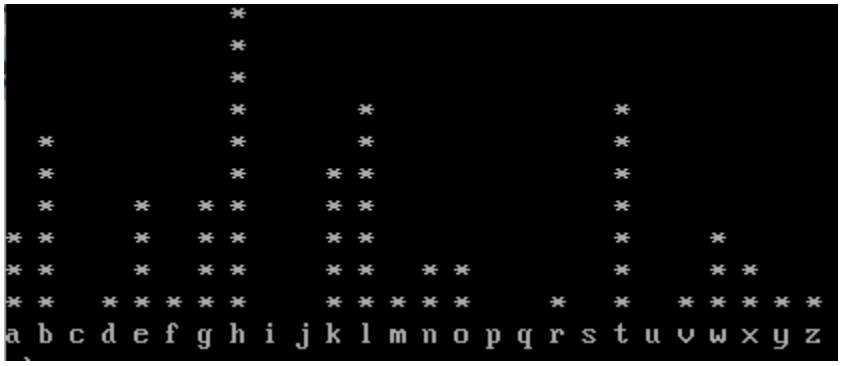
-> g 1 7



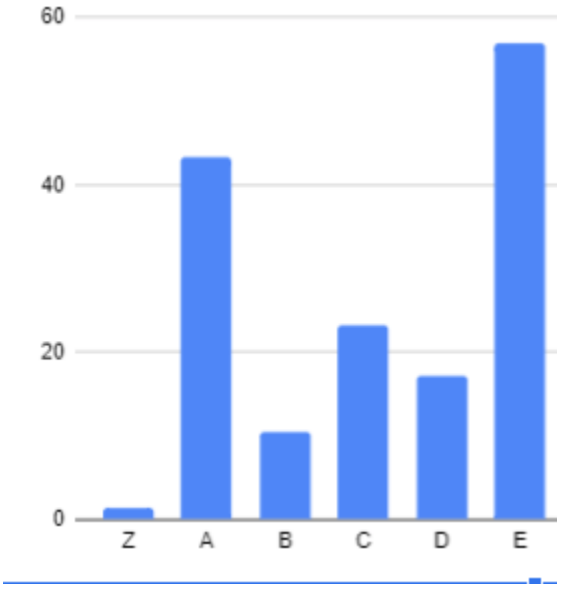
Based on the graph for the second sub alphabet:
ZABCDE frequency looks similar to the frequency of english.

Comparing side by side it looks similar, therefore the first sub alphabet is ‘A’

-> g 2 7



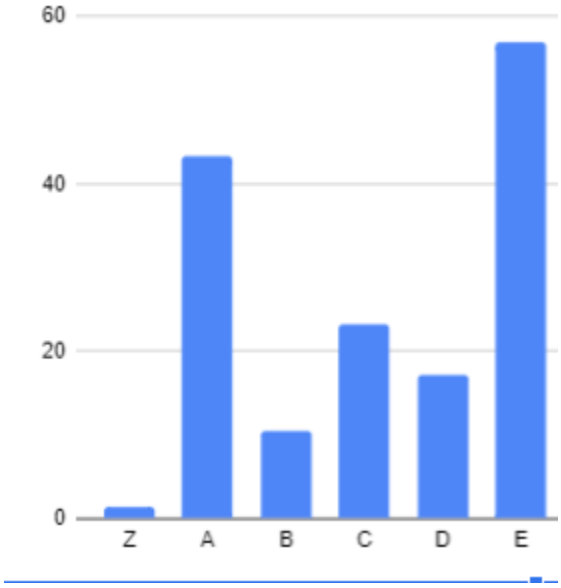
Based on the graph for the third sub alphabet:
ZABCDE -> Z = low, A = high but B = higher than A, therefore unlikely.
DEFGHI-> E is the lowest, therefore unlikely
JKLMNO-> L supposedly is B is the highest, therefore unlikely
However, STUVWX frequency looks similar to the frequency of english.



Comparing side by side it looks similar, therefore the first sub alphabet is ‘T’

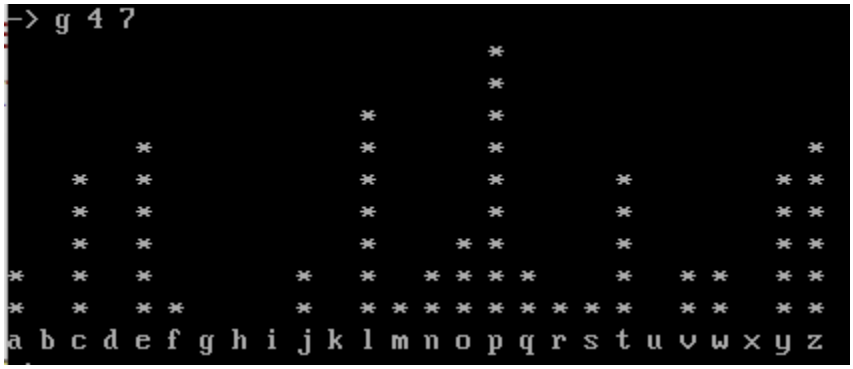
-> g 3 7

Based on the graph for the forth sub alphabet:
ABCDEF -> F supposedly E is the lowest.
DEFGHI-> E is the lowest, therefore unlikely
FGHIJK & JKLMNO-> G or K supposedly is B is the highest therefore unlikely
However, STUVWX frequency looks similar to the frequency of english.

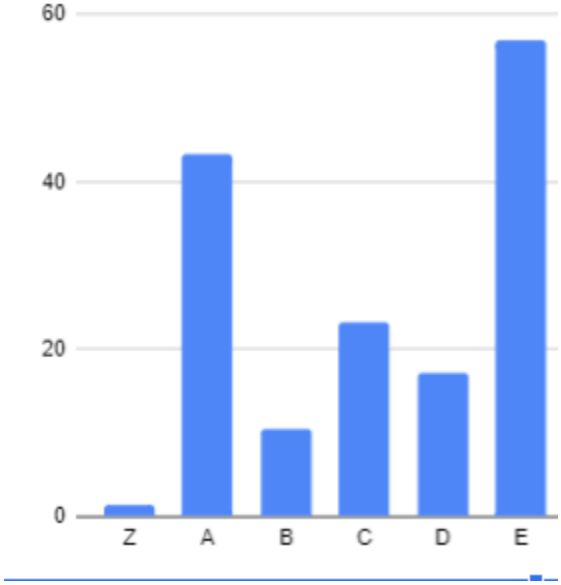


Comparing side by side it looks similar, therefore the first sub alphabet is ‘T’

-> g 4 7

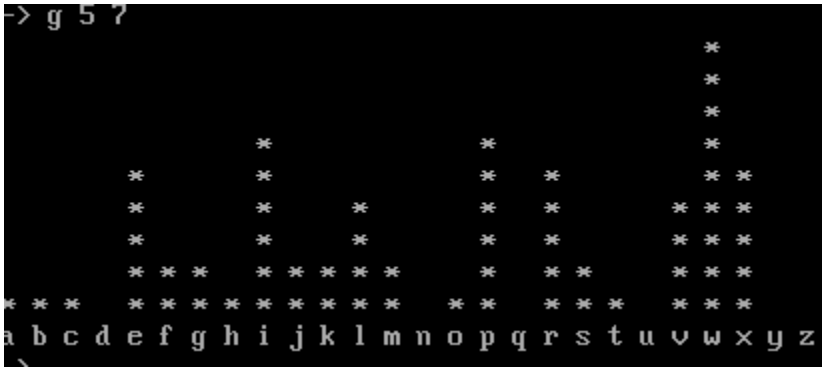


Based on the graph for the fifth sub alphabet:
KLMNOP frequency looks similar to the frequency of english.

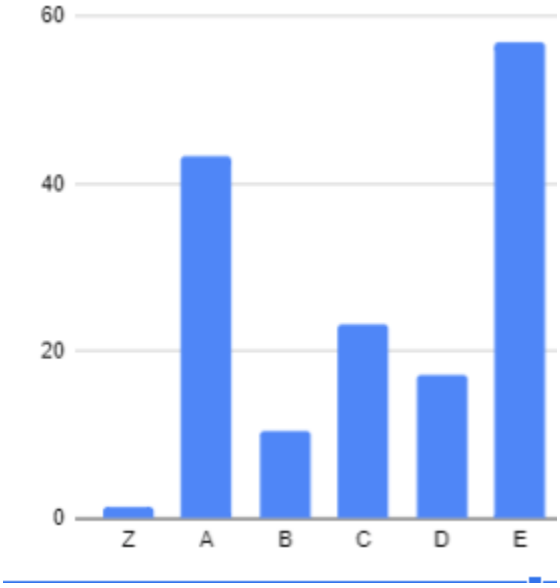


Comparing side by side it looks similar, therefore the first sub alphabet is ‘L’

-> g 5 7

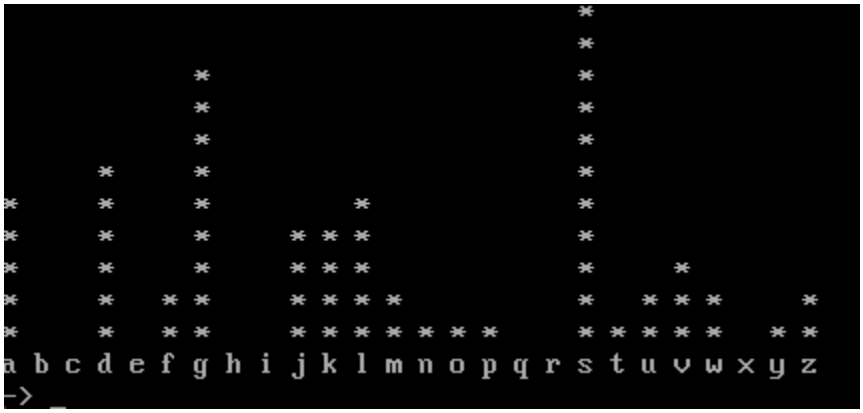


Based on the graph for the fifth sub alphabet:
HIJKLM -> J supposedly B is the same as C & D, therefore unlikely
QRSTUV-> S supposedly E is lowest, therefore unlikely
UVWXYZ-> W supposedly is B is the highest therefore unlikely
However, DEFGHI frequency looks similar to the frequency of english.

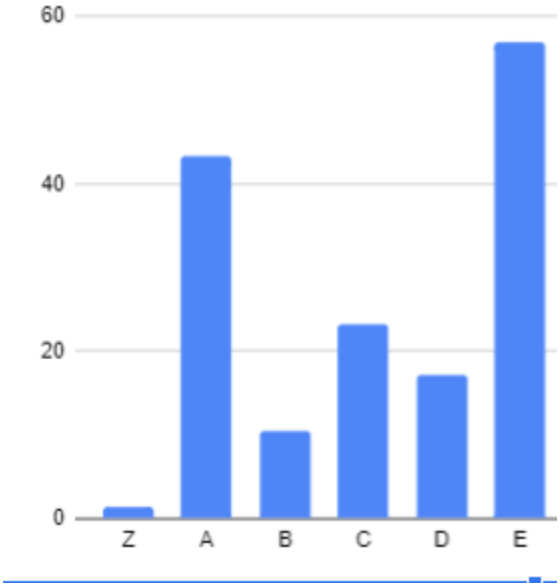


Comparing side by side it looks similar, therefore the first sub alphabet is ‘E’

-> g 6 7



Based on the graph for the fifth sub alphabet:
CDEFGH -> H supposedly E is the lowest, therefore unlikely
IJKLMN-> N supposedly E is lowest, therefore unlikely
However, RSTUVW frequency looks similar to the frequency of english.



Comparing side by side it looks similar, therefore the first sub alphabet is ‘S’

Therefore the keyword is: RATTLES