Name: HAY MUNN HNIN WAI

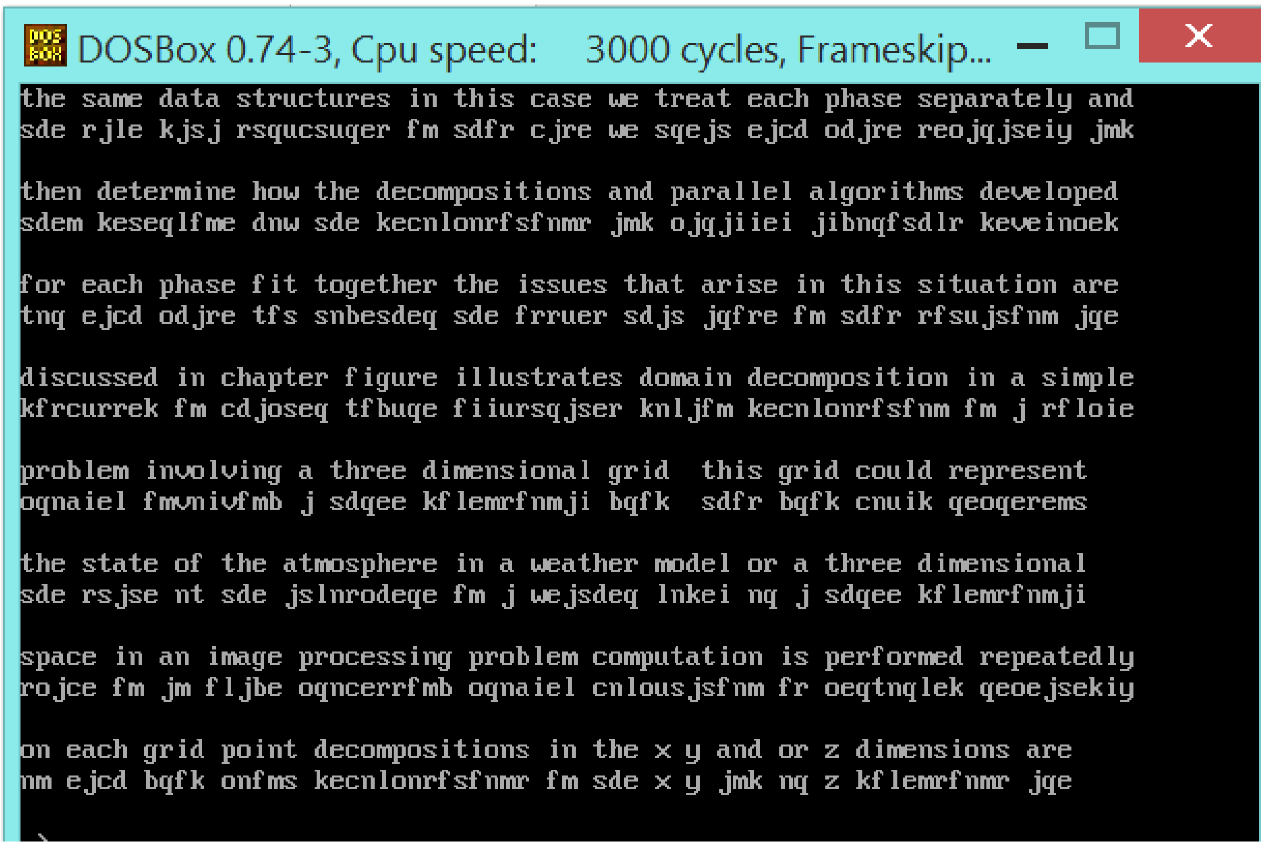
UOW ID: 6573277

CSCI361 Assignment -1

Task-1

Mono Alphabetic Cipher

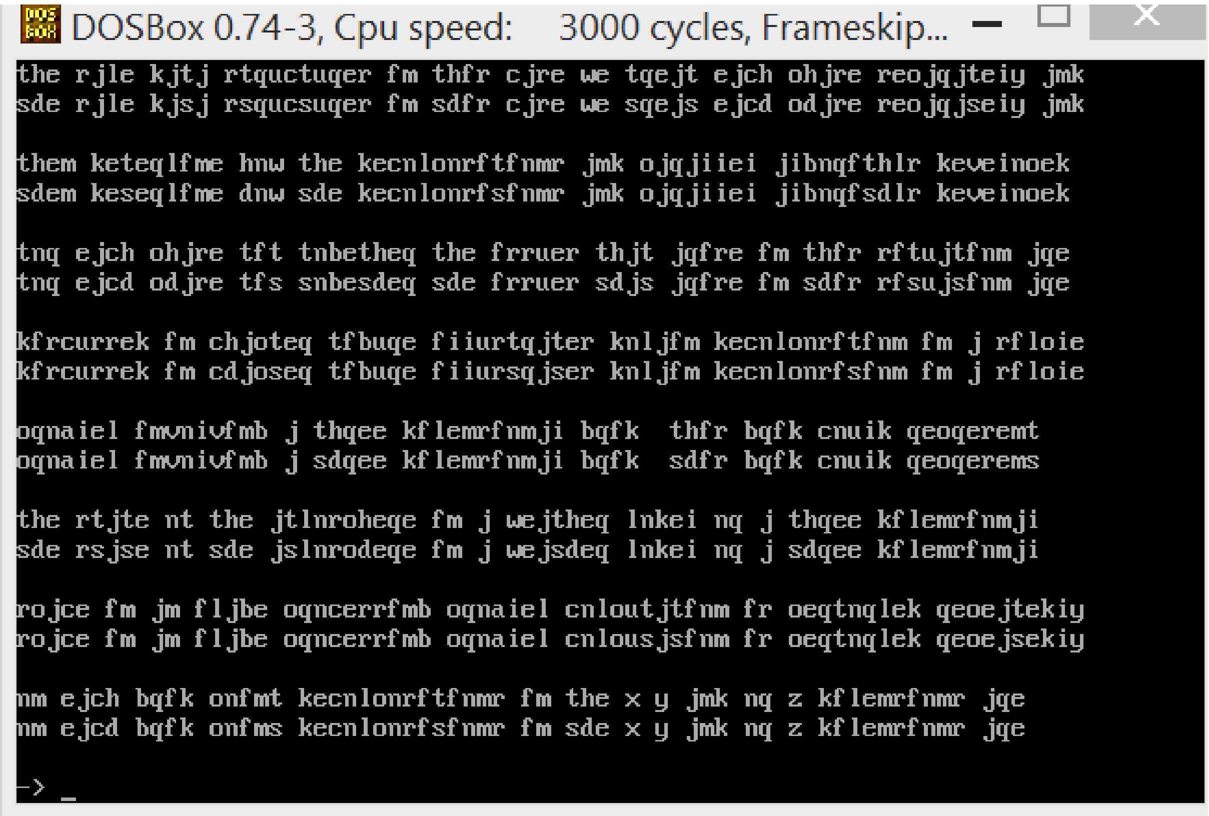
CText-1 Decryption Using KRYPTO.Exe



```
the same data structures in this case we treat each phase separately and
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

then determine how the decompositions and parallel algorithms developed
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

for each phase fit together the issues that arise in this situation are
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

discussed in chapter figure illustrates domain decomposition in a simple
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

problem involving a three dimensional grid  this grid could represent
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the state of the atmosphere in a weather model or a three dimensional
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

space in an image processing problem computation is performed repeatedly
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

on each grid point decompositions in the x y and or z dimensions are
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe
```

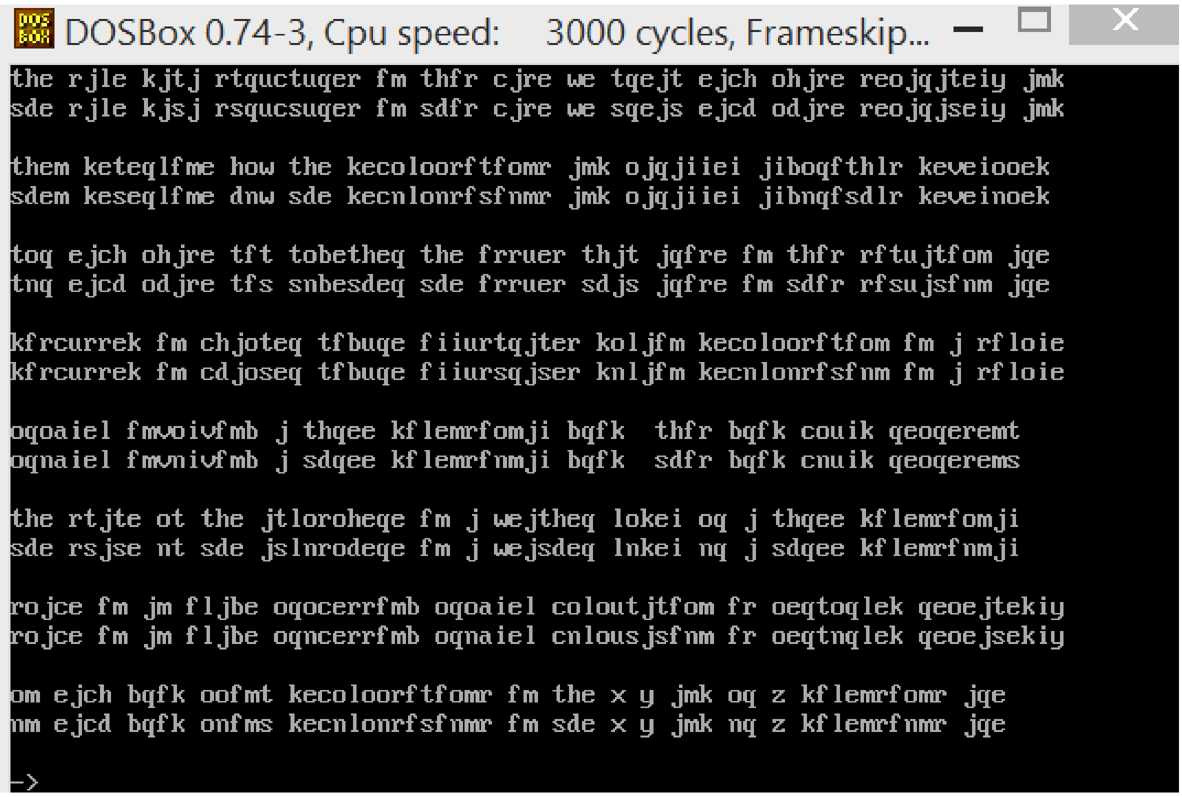
I used KRYPTO.EXE read CText-1 file by using DOSBox. Initially, I find the index of coincidence to guess which language is used in this Cipher Text-1. Then, I find the frequency of which letter appears most and **most frequent English trigrams.** Firstly, I got (Frequency/length) of "sde" → 9.

I assume this "SDE" can be the word "the" and I substitute these 3 words "the"→ to" SDE".



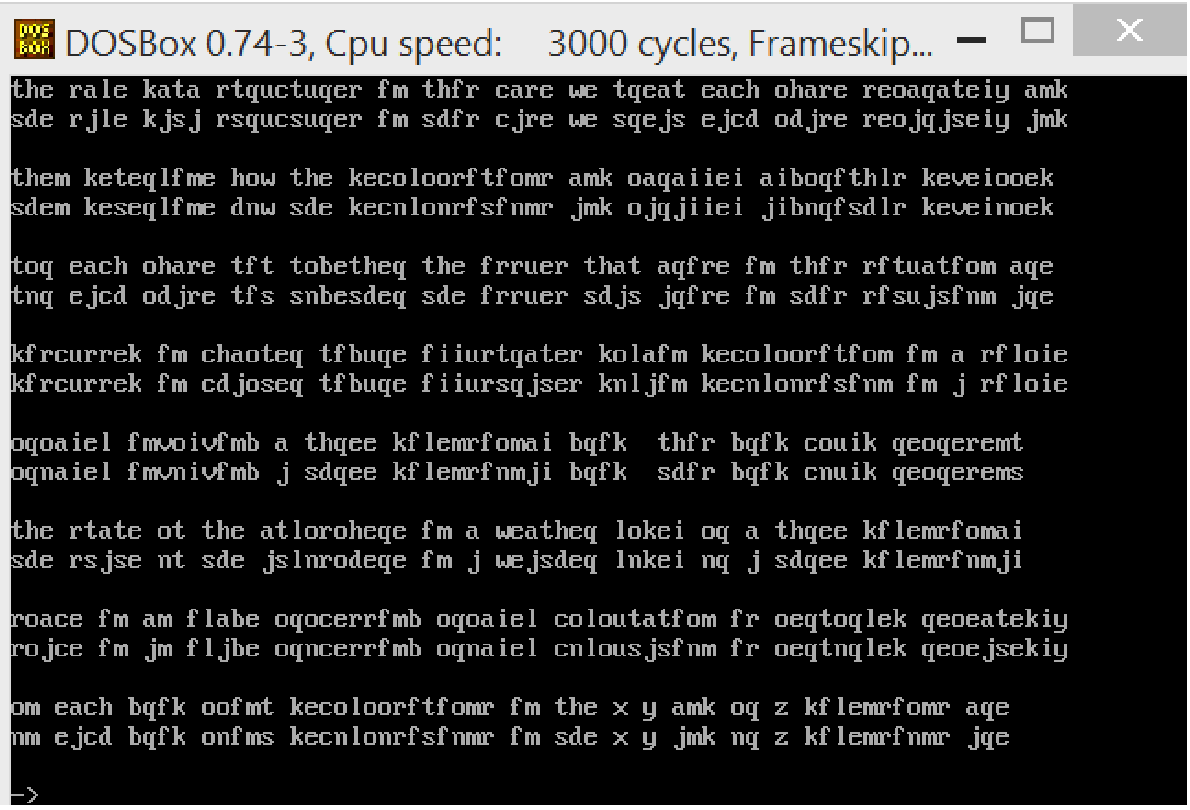
```
the rjle kjtj rtquctuqer fm thfr cjre we tqejt ejch ohjre reojqjteiy jmk
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

them keteqlfme hnw the kecnlonrftfnmr jmk ojqjiiei jibnqfthlr keveinoek
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

tnq ejch ohjre tft tnbetheq the frruer thjt jqfre fm thfr rftujtfnm jqe
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

kfrcurrek fm chjoteq tfbuqe fiiurtqjter knljfm kecnlonrftfnm fm j rfloie
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

oqnaiel fmvnivfmb j thqee kflemrfnmji bqfk  thfr bqfk cnuik qeoqeremt
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the rtjte nt the jtlnroheqe fm j wejtheq lnkei nq j thqee kflemrfnmji
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

rojce fm jm fljbe oqncerrfmb oqnaiel cnloutjtfnm fr oeqtnqlek qeoejtekiy
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

nm ejch bqfk onfmt kecnlonrftfnmr fm the x y jmk nq z kflemrfnmr jqe
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe

-> _
```

Next, I can successively guess words “hnw” → and substitute “ N to o “.



```
the rjle kjtj rtquctuqer fm thfr cjre we tqejt ejch ohjre reojqjteiy jmk
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

them keteqlfme how the kecoloorftfomr jmk ojqjiiei jiboqfthlr keveiooek
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

toq ejch ohjre tft tobetheq the frruer thjt jqfre fm thfr rftujtfom jqe
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

kfrcurrek fm chjoteq tfbuqe fiiurtqjter koljfm kecoloorftfom fm j rfloie
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

oqoaiel fmvoivfmb j thqee kflemrfomji bqfk  thfr bqfk couik qeoqeremt
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the rtjte ot the jtloroheqe fm j wejtheq lokei oq j thqee kflemrfomji
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

rojce fm jm fljbe oqocerrfmb oqoaiel coloutjtfom fr oeqtoqlek qeoejtekiy
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

om ejch bqfk oofmt kecoloorftfomr fm the x y jmk oq z kflemrfomr jqe
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe

->
```

Then, I can guess words like "ejch" → Substitute Jto a.



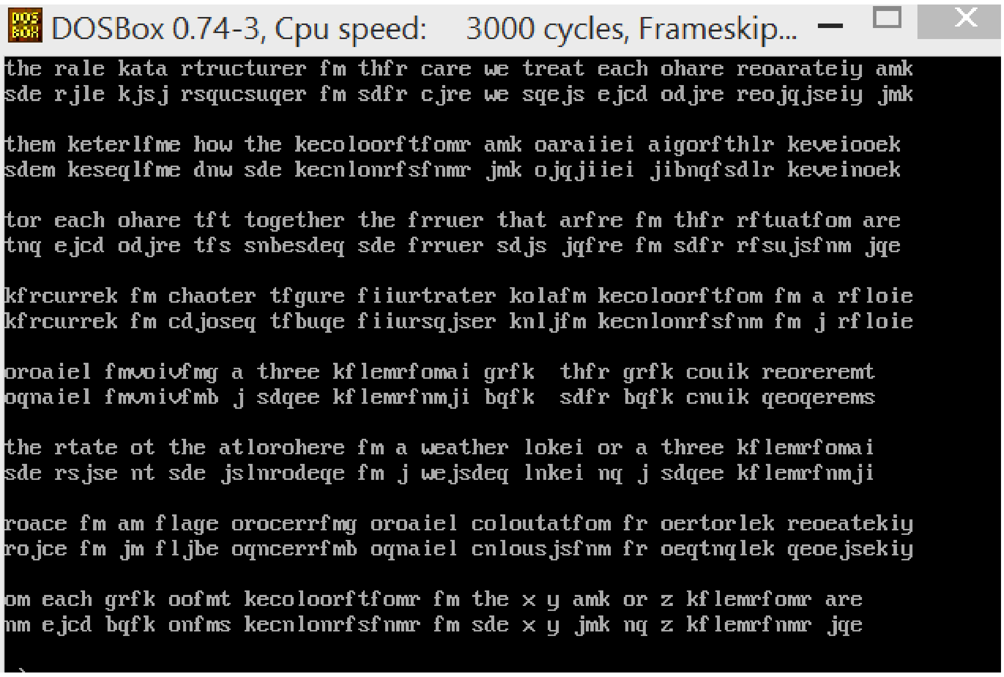
```
the rale kata rtqructuqer fm thfr care we tqeat each ohare reoaqateiy amk
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

them keteqlfme how the kecoloorftfomr amk oaqaiiei aiboqfthlr keveiooek
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

toq each ohare tft tobetheq the frruer that aqfre fm thfr rftuatfom aqe
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

kfrcurrek fm chaoteq tfbuqe fiiurtqater kolafm kecoloorftfom fm a rfloie
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

oqoaiel fmvoivfmb a thqee kflemrfomai bqfk  thfr bqfk couik qeoqeremt
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the rtate ot the atloroheqe fm a weatheq lokei oq a thqee kflemrfomai
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

roace fm am flabe oqocerrfmb oqoaiel coloutatfom fr oeqtoqlek qeoeatekiy
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

om each bqfk oofmt kecoloorftfomr fm the x y amk oq z kflemrfomr aqe
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe

->
```

Continuously, I can guess other words from spelling such as

" tqeat" →"treat" . Substitute Q to r.

"tobetheq" → "together", Substitute B to g.

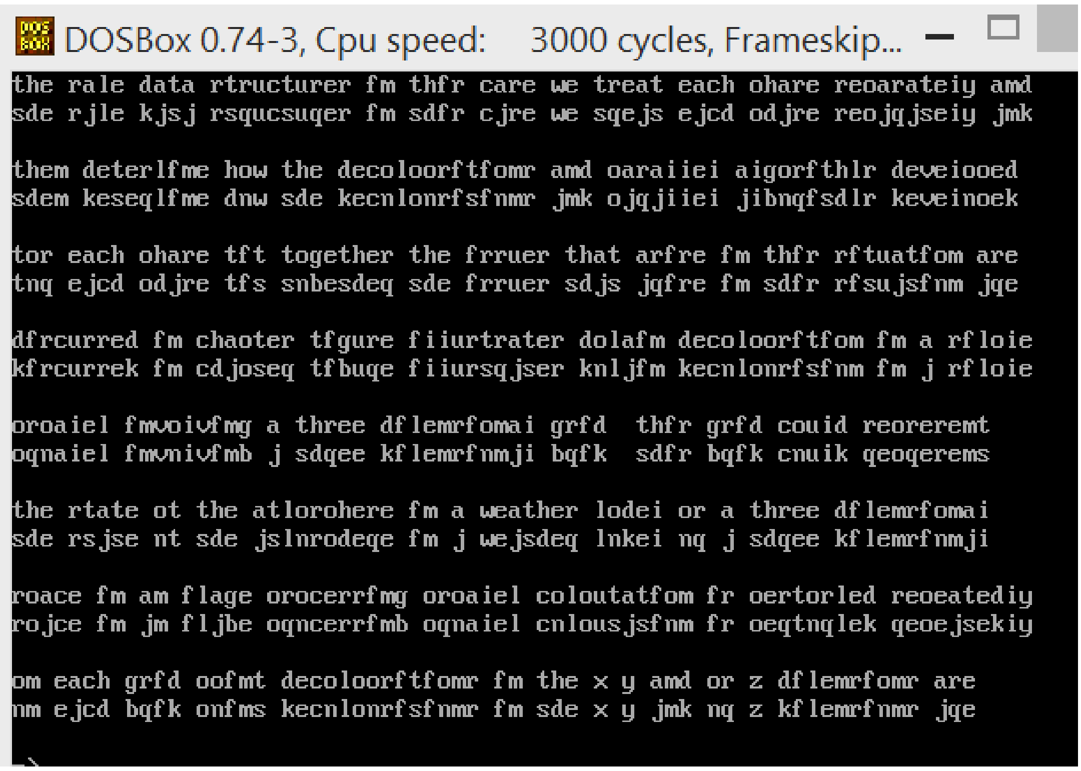
"thqee" → "three"



```
the rale kata rtructurer fm thfr care we treat each ohare reoarateiy amk
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

them keterlfme how the kecoloorftfomr amk oaraiiei aigorfthlr keveiooek
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

tor each ohare tft together the frruer that arfre fm thfr rftuatfom are
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

kfrcurrek fm chaoter tfgure fiiurtrater kolafm kecoloorftfom fm a rfloie
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

oroaiel fmvoivfmg a three kflemrfomai grfk  thfr grfk couik reoreremt
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the rtate ot the atlorohere fm a weather lokei or a three kflemrfomai
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

roace fm am flage orocerrfmg oroaiel coloutatfom fr oertorlek reoeatekiy
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

om each grfk oofmt kecoloorftfomr fm the x y amk or z kflemrfomr are
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe
```

From this, I continuously can guess other words such as:

"kata" → "data", Substitute K to d

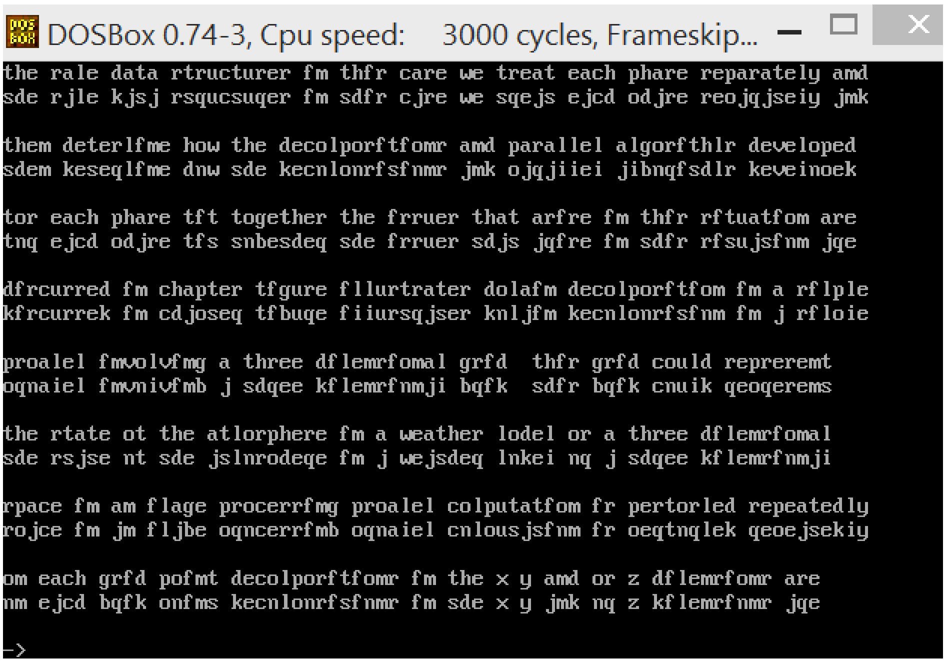


```
the rale data rtructurer fm thfr care we treat each ohare reoarateiy amd
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

them deterlfme how the decoloorftfomr amd oaraiiei aigorfthlr deveiooed
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

tor each ohare tft together the frruer that arfre fm thfr rftuatfom are
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

dfrcurred fm chaoter tfgure fiiurtrater dolafm decoloorftfom fm a rfloie
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

oroaiel fmvoivfmg a three dflemrfomai grfd  thfr grfd couid reoreremt
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the rtate ot the atlorohere fm a weather lodei or a three dflemrfomai
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

roace fm am flage orocerrfmg oroaiel coloutatfom fr oertorled reoeatediy
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

om each grfd oofmt decoloorftfomr fm the x y amd or z dflemrfomr are
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe
```

After this , I Can guess "deveiooed" → "developed"

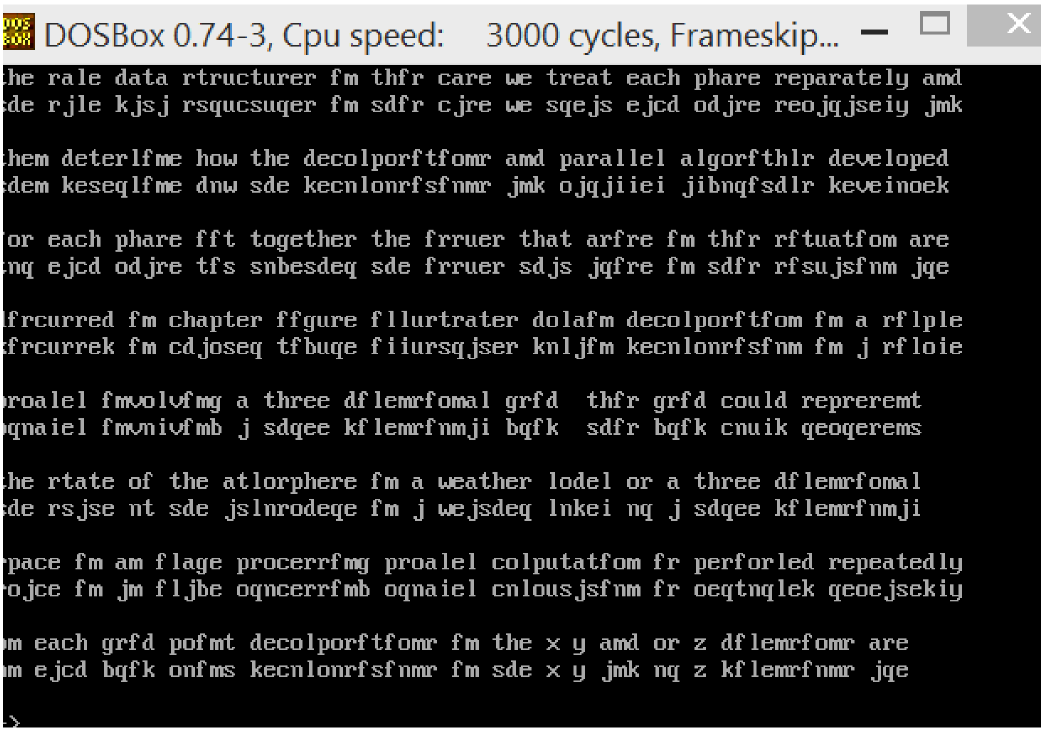
Substitute I to L

Substitute O to p



```
the rale data rtructurer fm thfr care we treat each phare reparately amd
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

them deterlfme how the decolporftfomr amd parallel algorfthlr developed
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

tor each phare tft together the frruer that arfre fm thfr rftuatfom are
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

dfrcurred fm chapter tfgure fllurtrater dolafm decolporftfom fm a rflple
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

proalel fmvolvfmg a three dflemrfomal grfd  thfr grfd could repreremt
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the rtate ot the atlorphere fm a weather lodel or a three dflemrfomal
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

rpace fm am flage procerrfmg proalel colputatfom fr pertorled repeatedly
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

om each grfd pofmt decolporftfomr fm the x y amd or z dflemrfomr are
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe

->
```

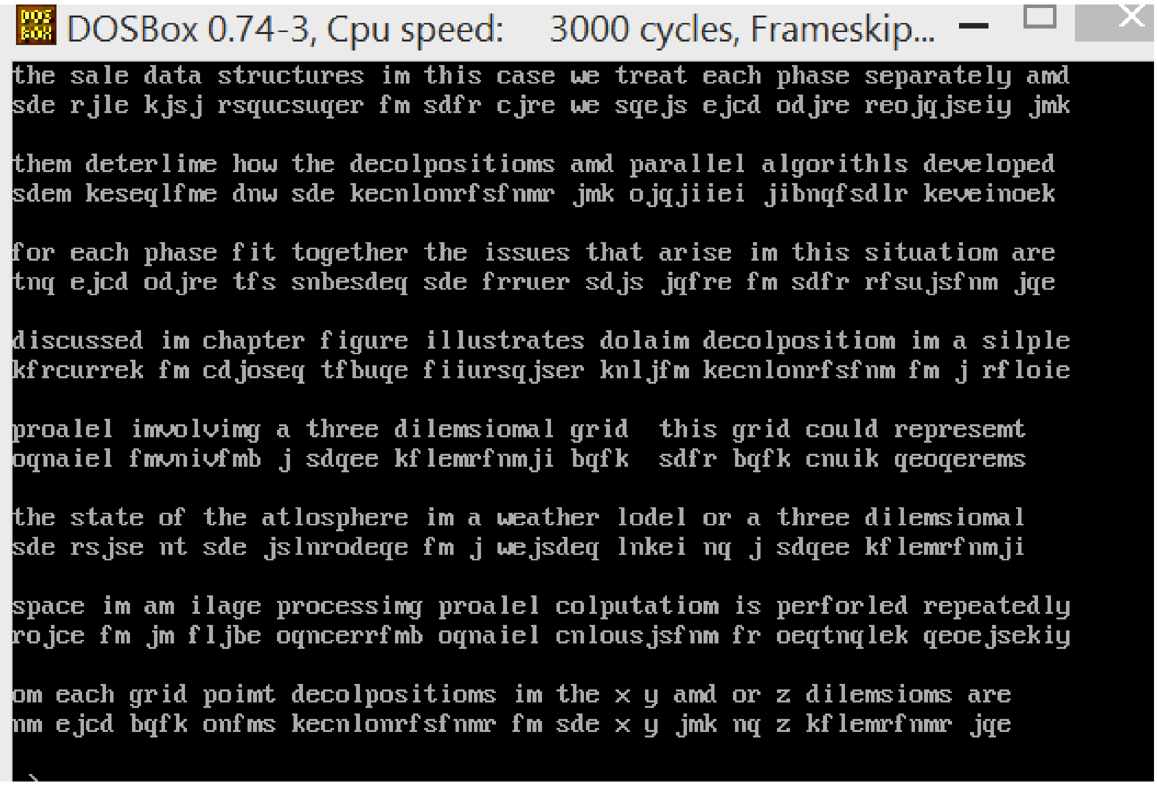
“tor” → “for” Substitute T to f



```
he rale data rtructurer fm thfr care we treat each phare reparately amd
de rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

hem deterlfme how the decolporftfomr amd parallel algorfthlr developed
dem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

or each phare fft together the frruer that arfre fm thfr rftuatfom are
nq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

lfrcurred fm chapter ffgure fllurtrater dolafm decolporftfom fm a rflple
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

roalel fmvolvfmg a three dflemrfomal grfd  thfr grfd could reprerernt
qnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

he rtate of the atlorphere fm a weather lodel or a three dflemrfomal
de rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

pace fm am flage procerrfmg proalel colputatfom fr perforled repeatedly
ojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

m each grfd pofmt decolporftfomr fm the x y amd or z dflemrfomr are
m ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe

>
```

Now, I can easily guess” fft “ → “fit “, Substitute F to i

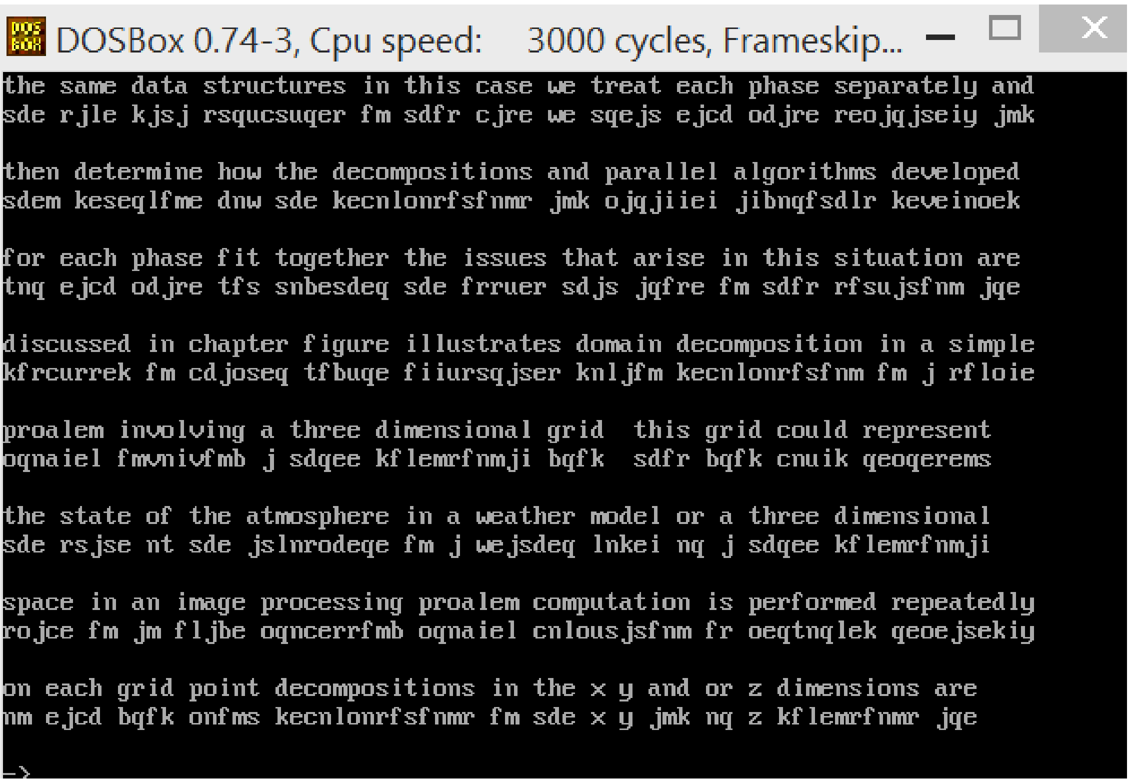
“phare “ → “phase” Substitute R to s



```
the sale data structures im this case we treat each phase separately amd
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

them deterlime how the decolpositioms amd parallel algorithls developed
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

for each phase fit together the issues that arise im this situatiom are
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

discussed im chapter figure illustrates dolaim decolpositiom im a silple
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

proalel imvolvimg a three dilemsiomal grid  this grid could represemt
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the state of the atlosphere im a weather lodel or a three dilemsiomal
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

space im am ilage processimg proalel colputatiom is perforled repeatedly
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

om each grid poimt decolpositioms im the x y amd or z dilemsioms are
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe

>
```

From the above result, I can guess “dilemsiomal” →”dimensional”

Substitute L to m, M to n. Finally, I got the Decrypted Message as below.



```
the same data structures in this case we treat each phase separately and
sde rjle kjsj rsqucsuqer fm sdfr cjre we sqejs ejcd odjre reojqjseiy jmk

then determine how the decompositions and parallel algorithms developed
sdem keseqlfme dnw sde kecnlonrfsfnmr jmk ojqjiiei jibnqfsdlr keveinoek

for each phase fit together the issues that arise in this situation are
tnq ejcd odjre tfs snbesdeq sde frruer sdjs jqfre fm sdfr rfsujsfnm jqe

discussed in chapter figure illustrates domain decomposition in a simple
kfrcurrek fm cdjoseq tfbuqe fiiursqjser knljfm kecnlonrfsfnm fm j rfloie

proalem involving a three dimensional grid  this grid could represent
oqnaiel fmvnivfmb j sdqee kflemrfnmji bqfk  sdfr bqfk cnuik qeoqerems

the state of the atmosphere in a weather model or a three dimensional
sde rsjse nt sde jslnrodeqe fm j wejsdeq lnkei nq j sdqee kflemrfnmji

space in an image processing proalem computation is performed repeatedly
rojce fm jm fljbe oqncerrfmb oqnaiel cnlousjsfnm fr oeqtnqlek qeoejsekiy

on each grid point decompositions in the x y and or z dimensions are
nm ejcd bqfk onfms kecnlonrfsfnmr fm sde x y jmk nq z kflemrfnmr jqe

->
```

To generate the Encryption Key, I wrote down A to Z and substitute each Cipher together with the Plain Text that I got from the above process. From this, I notice how this CText-1 is generated. It is using a Keyword → JACKET and **this was substituted from plain text Initial letter “abcdef”** and the rest of the letters are One-To-One Mapping with English Alphabet sequence without duplicate with pervious substituted words.

Kindly see the below Encryption Key as below:

Mono Alphabetic Cipher Encryption Key

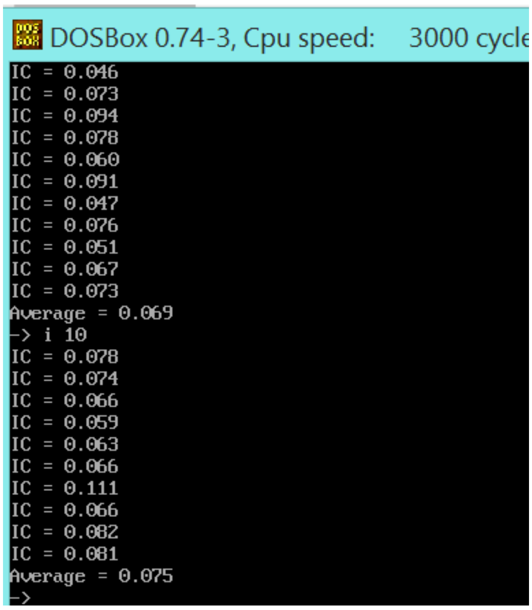
Plain Text	**Cipher Text**
a	**J**
b	**A**
c	**C**
d	**K**
e	**E**
f	**T**
g	B
h	D
i	F
j	G
k	H
l	I
m	L
n	M
o	N
p	O
q	P
r	Q
s	R
t	S
u	U
v	V
w	W
x	X
y	Y
z	Z

Vigenere Cipher (CText-02)

For CText-02, firstly I tried to find the index of coincidence. I try from 0 to 5, I got average value i= 0.076 for <I 5> , which is very close to properties range of English Language

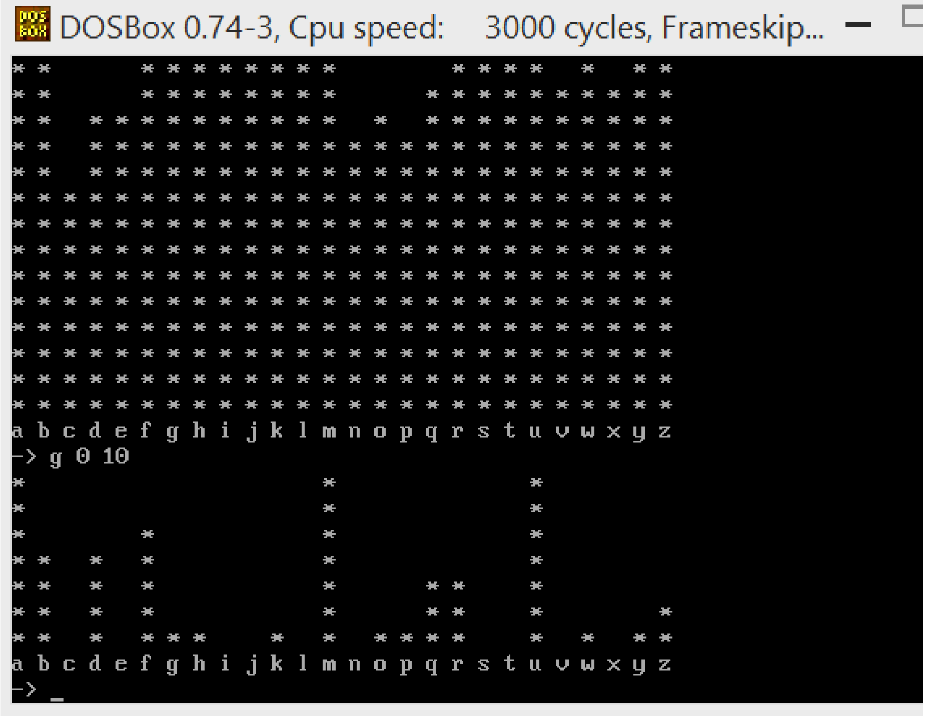
(0.066895). So, I tried to print graph < g 0 5 > and try first. But when i tried with Frequency Distribution for the Language. I cannot correctly guess the Keyword for index < I 5> .

I continue to find index find until < I 12>. And I found that at index < I 10> the average value is = 0.075 as below:



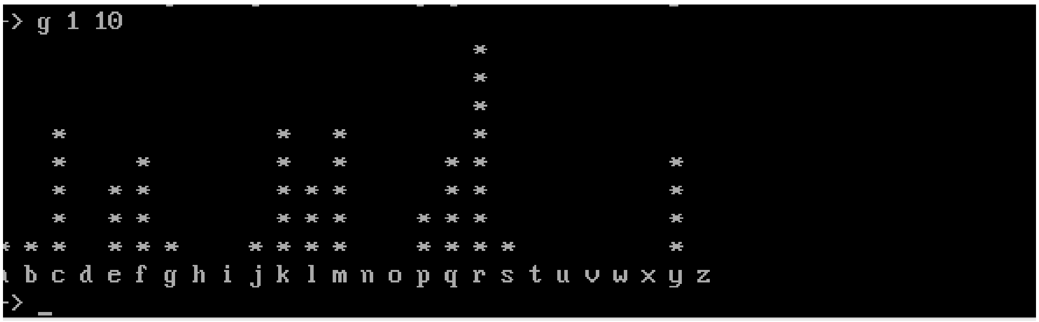
```
IC = 0.046
IC = 0.073
IC = 0.094
IC = 0.078
IC = 0.060
IC = 0.091
IC = 0.047
IC = 0.076
IC = 0.051
IC = 0.067
IC = 0.073
Average = 0.069
-> i 10
IC = 0.078
IC = 0.074
IC = 0.066
IC = 0.059
IC = 0.063
IC = 0.066
IC = 0.111
IC = 0.066
IC = 0.082
IC = 0.081
Average = 0.075
->
```

I try to print graph < g 0 10> as below:



```
* *       * * * * * * * *         * * * *   *   * *
* *       * * * * * * * *       * * * * * * * * * *
* *   * * * * * * * * * *   *   * * * * * * * * * *
* *   * * * * * * * * * * * * * * * * * * * * * * *
* *   * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * *
a b c d e f g h i j k l m n o p q r s t u v w x y z
-> g 0 10
*                       *               *
*                       *               *
*         *             *               *
* *   *   *             *               *
* *   *   *             *       * *     *
* *   *   *             *       * *     *         *
* *   *   * * *     *   *   * * * *     *   *   * *
a b c d e f g h i j k l m n o p q r s t u v w x y z
-> _
```

From the above graph < g 0 10> I try to find the Frequency Distribution order according to this order “(Highest Frequency) etaoinsrhldcumfpgwybvkxjqz (Lowest Frequency) “. I look at the lower frequency order and count letter” A”, see each letter’s Frequency Distribution order from graph is fixed or not. When I count Letter” m” as “A”, the graph seems to be correct and match with the frequency distribution. **Hence, I guess First Keyword letter can be – “M”.**



```
-> g 1 10
                                  *
                                  *
                                  *
    *               *   *         *
    *     *         *   *       * *             *
    *   * *         * * *       * *             *
    *   * *         * * *     * * *             *
* * *   * * *     * * * *     * * * *           *
a b c d e f g h i j k l m n o p q r s t u v w x y z
-> _
```

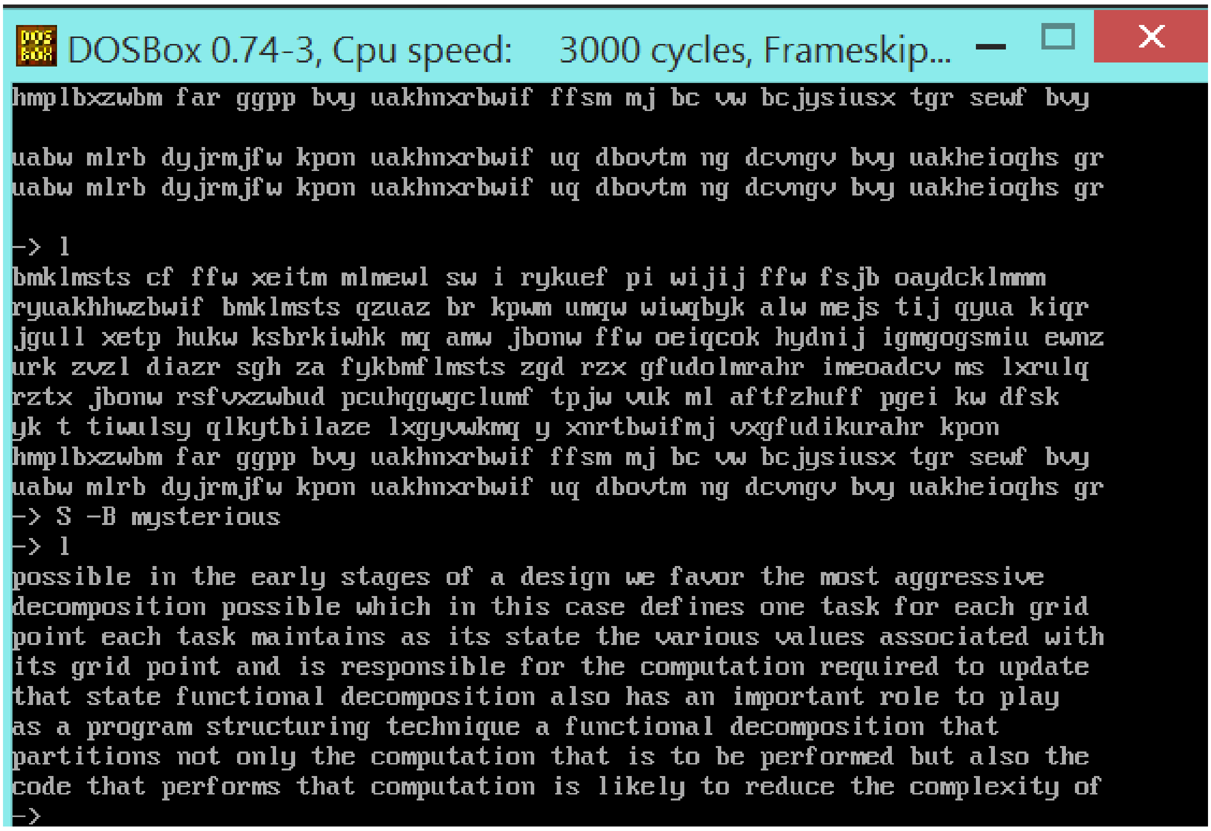
For graph <g 1 10>, same with previous method, I look at the lower frequency order and count letter” A” and see each letter’s Frequency Distribution order from graph is fixed or not. I look at the Frequency Distribution order according to this

“(Highest Frequency) etaoinsrhldcumfpgwybvkxjqz (Lowest Frequency) “ . I check Is the frequency distribution for a language fixed. From the graph, if count “A” from “Y”, **I guess Second Keyword letter can be – “Y”.**

I continue with the above-mentioned methods for the rest of the graphs

< g 2 10> to <g 9 10>. By applying the same methods,

I guess Keyword is = “MYSTERIOUS”. I substituted to Block and got Plain Text result as below:



```
hmplbxzwbm far ggpp bvy uakhnxrbwif ffsm mj bc vw bcjysiusx tgr sewf bvy

uabw mlrb dyjrmjfw kpon uakhnxrbwif uq dbovtm ng dcvngv bvy uakheioqhs gr
uabw mlrb dyjrmjfw kpon uakhnxrbwif uq dbovtm ng dcvngv bvy uakheioqhs gr

-> l
bmklmsts cf ffw xeitm mlmewl sw i rykuef pi wijij ffw fsjb oaydcklmmm
ryuakhhwzbwif bmklmsts qzuaz br kpwm umqw wiwqbyk alw mejs tij qyua kiqr
jgull xetp hukw ksbrkiwhk mq amw jbonw ffw oeiqcok hydnij igmgogsmiu ewnz
urk zvzl diazr sgh za fykbmflmsts zgd rzx gfudolmrahr imeoadcv ms lxrulq
rztx jbonw rsfvxzwbud pcuhqgwgclumf tpjw vuk ml aftfzhuff pgei kw dfsk
yk t tiwulsy qlkytbilaze lxgyvwkmq y xnrtbwifmj vxgfudikurahr kpon
hmplbxzwbm far ggpp bvy uakhnxrbwif ffsm mj bc vw bcjysiusx tgr sewf bvy
uabw mlrb dyjrmjfw kpon uakhnxrbwif uq dbovtm ng dcvngv bvy uakheioqhs gr
-> S -B mysterious
-> l
possible in the early stages of a design we favor the most aggressive
decomposition possible which in this case defines one task for each grid
point each task maintains as its state the various values associated with
its grid point and is responsible for the computation required to update
that state functional decomposition also has an important role to play
as a program structuring technique a functional decomposition that
partitions not only the computation that is to be performed but also the
code that performs that computation is likely to reduce the complexity of
->
```