Name: HAY MUNN HNIN WAI

UOW ID: 6573277

CSCI361 Assignment -1

Task-2 (Kamasutra Cipher Decryption)

Decrypt CText-3 Using KRYPTO.Exe without knowing Keys

Firstly, I read CText-3.txt that I generated from Task-2 and try to find the Frequency first.

As I know that Kamasutra Cipher is also a Monoalphabetic cipher, so language statistics also can appear in the ciphertext without confusion included in the cipher .

After I print out 'Ctext-3' with DOSBox and its Frequency, I got result as below:

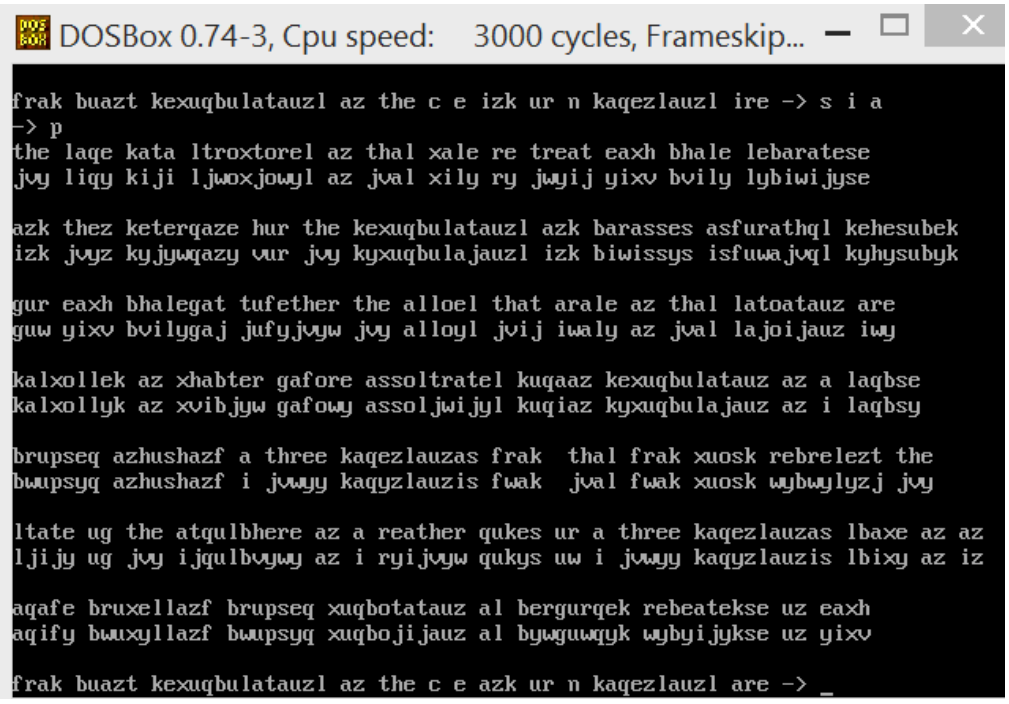
```
fwak buazj kyxuqbulajauzl az jvy c e izk uw n kaqyzlauzl iwy -> l
jvy liqy kiji ljwoxjowyl az jval xily ry jwyij yixv bvily lybiwijyse
izk jvyz kyjywqazy vur jvy kyxuqbulajauzl izk biwissys isfuwajvql kyhysubyk
guw yixv bvilygaj jufyjvyw jvy alloyl jvij iwaly az jval lajoijauz iwy
kalxollyk az xvibjyw gafowy assoljwijyl kuqiaz kyxuqbulajauz az i laqbsy
bwupsyq azhushazf i jvwyy kaqyzlauzis fwak  jval fwak xuosk wybwylyzj jvy
ljijy ug jvy ijqulbvywy az i ryijvyw qukys uw i jvwyy kaqyzlauzis lbixy az iz
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv
fwak buazj kyxuqbulajauzl az jvy c e izk uw n kaqyzlauzl iwy -> _
```

```
DOSBox 0.74-3, Cpu speed:    3000 cycles, Frameskip...
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv
fwak buazj kyxuqbulajauzl az jvy c e izk uw n kaqyzlauzl iwy -> f 3
jvy     9
auz     8
ijy     5
jau     5
azj     4
laj     4
uqb     4
xuq     4
yij     4
yka     4
zla     4
aja     3
aqy     3
azi     3
bul     3
bwu     3
fwa     3
ijv     3
ily     3
ixv     3
izk     3
jva     3
-> _
```

I assume the highest frequency words "jvy " to Most frequency English words → "the" and do the Substitution to these 3 letters.

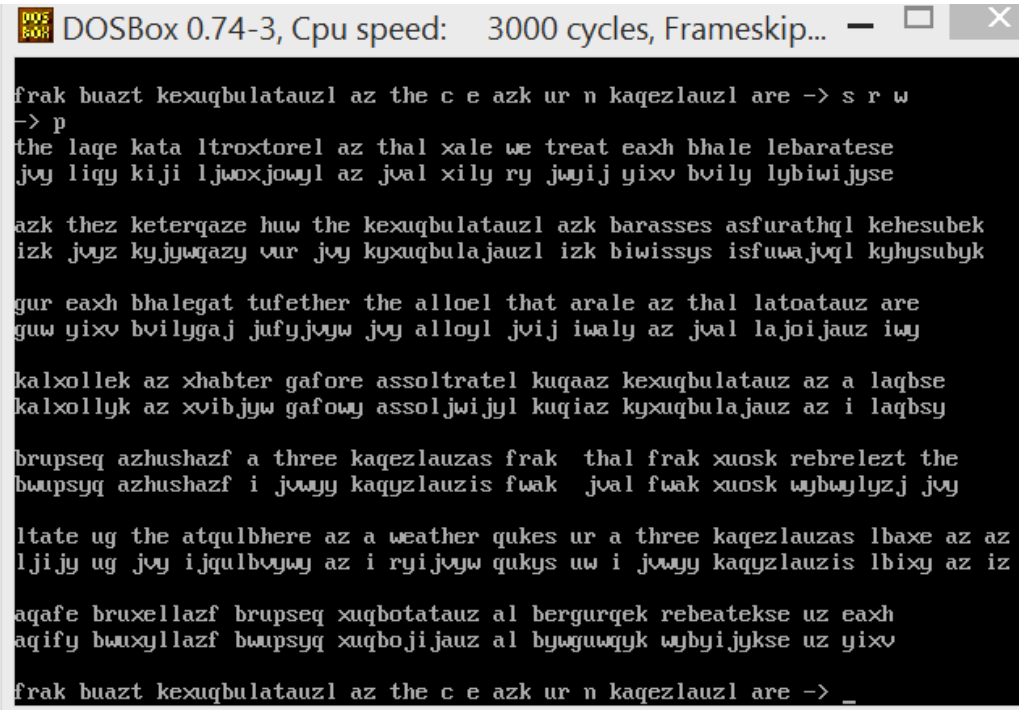
After substituted, next I can guess some words like "i " can be → Letter "a".

I got result like this:



From the above cipher, I can guess "reather " → to word "weather"

So, I Substitute "r " with "w" .



From this, I can guess “kata” → to “data” , “eaxh” to → “each” , “huw” to → “how”

I got result:

```
DOSBox 0.74-3, Cpu speed:    3000 cycles, Frameskip...

frad buazt decuqbulatauzl az the c e azd ur n daqezlauzl are -> s u o
-> p
the laqe data ltroctorel az thal cale we treat each bhale lebaratese
jvy liqy kiji ljwoxjowyl az jval xily ry jwyij yixv bvily lybiwijyse

azd thez deterqaze how the decoqbolataozl azd barasses asforathql dehesobed
izk jvyz kyjywqazy vur jvy kyxuqbulajauzl izk biwissys isfuwajvql kyhysubyk

gor each bhalegat tofether the alloel that arale az thal latoataoz are
guw yixv bvilygaj jufyjvyw jvy alloyl jvij iwaly az jval lajoijauz iwy

dalcolled az chabter gafore assoltratel doqaaz decoqbolataoz az a laqbse
kalxollyk az xvibjyw gafowy assoljwijyl kuqiaz kyxuqbulajauz az i laqbsy

bropseq azhoshazf a three daqezlaozas frad  thal frad coosd rebrelezt the
bwupsyq azhushazf i jvwyy kaqyzlauzis fwak  jval fwak xuosk wybwylyzj jvy

ltate og the atqolbhere az a weather qodes or a three daqezlaozas lbace az az
ljijy ug jvy ijqulbvywy az i ryijvyw qukys uw i jvwyy kaqyzlauzis lbixy az iz

aqafe brocellazf bropseq coqbotataoz al bergorqed rebeatedse oz each
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv

frad boazt decoqbolataozl az the c e azd or n daqezlaozl are -> _
```

Continue, I can guess “ tofether” → “together” , “gor”→ “for” ,”oz” → “on”

```
DOSBox 0.74-3, Cpu speed:    3000 cycles, Frameskip...

grad boazt decoqbolataozl az the c e azd or n daqezlaozl are -> s z n
-> p
the laqe data ltroctorel an thal cale we treat each bhale lebaratese
jvy liqy kiji ljwoxjowyl az jval xily ry jwyij yixv bvily lybiwijyse

and then deterqane how the decoqbolataonl and barasses asgorathql dehesobed
izk jvyz kyjywqazy vur jvy kyxuqbulajauzl izk biwissys isfuwajvql kyhysubyk

for each bhalefat together the alloel that arale an thal latoataon are
guw yixv bvilygaj jufyjvyw jvy alloyl jvij iwaly az jval lajoijauz iwy

dalcolled an chabter fagore assoltratel doqaan decoqbolataon an a laqbse
kalxollyk az xvibjyw gafowy assoljwijyl kuqiaz kyxuqbulajauz az i laqbsy

bropseq anhoshang a three daqenlaonas grad  thal grad coosd rebrelent the
bwupsyq azhushazf i jvwyy kaqyzlauzis fwak  jval fwak xuosk wybwylyzj jvy

ltate of the atqolbhere an a weather qodes or a three daqenlaonas lbace an an
ljijy ug jvy ijqulbvywy az i ryijvyw qukys uw i jvwyy kaqyzlauzis lbixy az iz

aqage brocellang bropseq coqbotataon al berforqed rebeatedse on each
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv

grad boant decoqbolataonl an the c e and or n daqenlaonl are ->
```

Next, I can guess “deterqane” → “determine”

```
DOSBox 0.74-3, Cpu speed:    3000 cycles, Frameskip...
grad boant decoqbolataonl an the c e and or n daqenlaonl are -> s q m
-> s a i
-> p
the lame data ltroctorel in thil cale we treat each bhale lebaratese
jvy liqy kiji ljwoxjowyl az jval xily ry jwyij yixv bvily lybiwijyse

and then determine how the decombolitionl and barasses asgorithml dehesobed
izk jvyz kyjywqazy vur jvy kyxuqbulajauzl izk biwissys isfuwajvql kyhysubyk

for each bhalefit together the illoel that arile in thil litoation are
guw yixv bvilygaj jufyjvyw jvy alloyl jvij iwaly az jval lajoijauz iwy

dilcolled in chabter figore issoltratel domain decombolition in a limbse
kalxollyk az xvibjyw gafowy assoljwijyl kuqiaz kyxuqbulajauz az i laqbsy

bropsem inhoshing a three dimenlionas grid  thil grid coosd rebrelent the
bwupsyq azhushazf i jvwyy kaqyzlauzis fwak  jval fwak xuosk wybwylyzj jvy

ltate of the atmolbhere in a weather modes or a three dimenlionas lbace in an
ljijy ug jvy ijqulbvywy az i ryijvyw qukys uw i jvwyy kaqyzlauzis lbixy az iz

image brocelling bropsem combotation il berformed rebeatedse on each
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv

grid boint decombolitionl in the c e and or n dimenlionl are -> _
```

Next, I can Substitute “lame” → “same”

```
DOSBox 0.74-3, Cpu speed:    3000 cycles, Frameskip...

grid boint decombolitionl in the c e and or n dimenlionl are -> s l s
-> p
the same data stroctores in this case we treat each bhase sebaratese
jvy liqy kiji ljwoxjowyl az jval xily ry jwyij yixv bvily lybiwijyse

and then determine how the decombositions and barasses asgorithms dehesobed
izk jvyz kyjywqazy vur jvy kyxuqbulajauzl izk biwissys isfuwajvql kyhysubyk

for each bhasefit together the issoes that arise in this sitoation are
guw yixv bvilygaj jufyjvyw jvy alloyl jvij iwaly az jval lajoijauz iwy

discossed in chabter figore issostrates domain decombosition in a simbse
kalxollyk az xvibjyw gafowy assoljwijyl kuqiaz kyxuqbulajauz az i laqbsy

bropsem inhoshing a three dimensionas grid  this grid coosd rebresent the
bwupsyq azhushazf i jvwyy kaqyzlauzis fwak  jval fwak xuosk wybwylyzj jvy

state of the atmosbhere in a weather modes or a three dimensionas sbace in an
ljijy ug jvy ijqulbvywy az i ryijvyw qukys uw i jvwyy kaqyzlauzis lbixy az iz

image brocessing bropsem combotation is berformed rebeatedse on each
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv

grid boint decombositions in the c e and or n dimensions are ->
```

Next, I guess “stroctores” → “structures” , “bhase” → “phase” , “asgorithms” → “algorithms”

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip...

```
grid point decompositions in the c e and or n dimensions are -> s s l
-> p
the same data stroctores in this case we treat each phase separatele
jvy liqy kiji ljwoxjowyl az jval xily ry jwyij yixv bvily lybiwijyse

and then determine how the decompositions and parallel algorithms deheloped
izk jvyz kyjywqazy vur jvy kyxuqbulajauzl izk biwissys isfuwajvql kyhysubyk

for each phasefit together the issoes that arise in this sitoation are
guw yixv bvilygaj jufyjvyw jvy alloyl jvij iwaly az jval lajoijauz iwy

discossed in chapter figore illostrates domain decomposition in a simple
kalxollyk az xvibjyw gafowy assoljwijyl kuqiaz kyxuqbulajauz az i laqbsy

proplem inholhing a three dimensional grid  this grid coold represent the
bwupsyq azhushazf i jvwyy kaqyzlauzis fwak  jval fwak xuosk wybwylyzj jvy

state of the atmosphere in a weather model or a three dimensional space in an
ljijy ug jvy ijqulbvywy az i ryijvyw qukys uw i jvwyy kaqyzlauzis lbixy az iz

image processing proplem compotation is performed repeatedle on each
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv

grid point decompositions in the c e and or n dimensions are -> _
```

Next, I can guess “sitoation” → “situation

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip...

```
grid point decompositions in the c e and or n dimensions are -> s o u
-> p
the same data structures in this case we treat each phase separatele
jvy liqy kiji ljwoxjowyl az jval xily ry jwyij yixv bvily lybiwijyse

and then determine how the decompositions and parallel algorithms deheloped
izk jvyz kyjywqazy vur jvy kyxuqbulajauzl izk biwissys isfuwajvql kyhysubyk

for each phasefit together the issues that arise in this situation are
guw yixv bvilygaj jufyjvyw jvy alloyl jvij iwaly az jval lajoijauz iwy

discussed in chapter figure illustrates domain decomposition in a simple
kalxollyk az xvibjyw gafowy assoljwijyl kuqiaz kyxuqbulajauz az i laqbsy

proplem inholhing a three dimensional grid  this grid could represent the
bwupsyq azhushazf i jvwyy kaqyzlauzis fwak  jval fwak xuosk wybwylyzj jvy

state of the atmosphere in a weather model or a three dimensional space in an
ljijy ug jvy ijqulbvywy az i ryijvyw qukys uw i jvwyy kaqyzlauzis lbixy az iz

image processing proplem computation is performed repeatedle on each
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv

grid point decompositions in the c e and or n dimensions are -> _
```

Next, I can successively guess “separatele” → “separately” , “deheloped” → “developed” ,

“proplem” → “problem”

Finally, I got the Plain-Text as below:

```
state of the atmosphere in a weather model or a three dimensional space in an
ljijy ug jvy ijqulbvywy az i ryijvyw qukys uw i jvwyy kaqyzlauzis lbixy az iz

image processing problem computation is performed repeatedly on each
aqify bwuxyllazf bwupsyq xuqbojijauz al bywguwqyk wybyijykse uz yixv

grid point decompositions in the x y and or z dimensions are -> l
the same data structures in this case we treat each phase separately
and then determine how the decompositions and parallel algorithms developed
for each phasefit together the issues that arise in this situation are
discussed in chapter figure illustrates domain decomposition in a simple
problem involving a three dimensional grid  this grid could represent the
state of the atmosphere in a weather model or a three dimensional space in an
image processing problem computation is performed repeatedly on each
grid point decompositions in the x y and or z dimensions are -> _
```

To Conclude, I notice that without knowing the key to decrypt the Kamasutra cipher, it takes more times than earlier Task-1 Monoalphabetic Cipher. Without the key is difficult to decrypt because of 26! = 403 septillion of combination of key can be produce uniquely.

But if we know this Cipher is Encrypted with Kamasutra Cipher, we can simply look up the letters that are paired up and decrypt the message.

Kindly see the below Encryption Key-Pair as below:

Task-2 (Kamasutra Alphabetic Cipher) Encryption Key

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