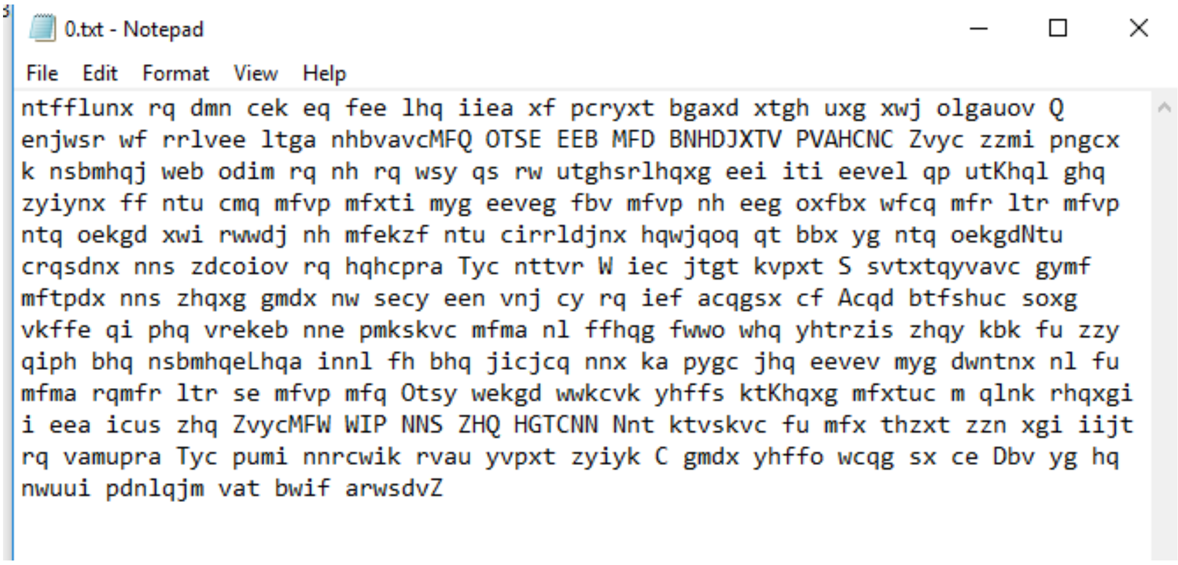
ASSIGNMENT 1

Khaled Alblowy n9292608

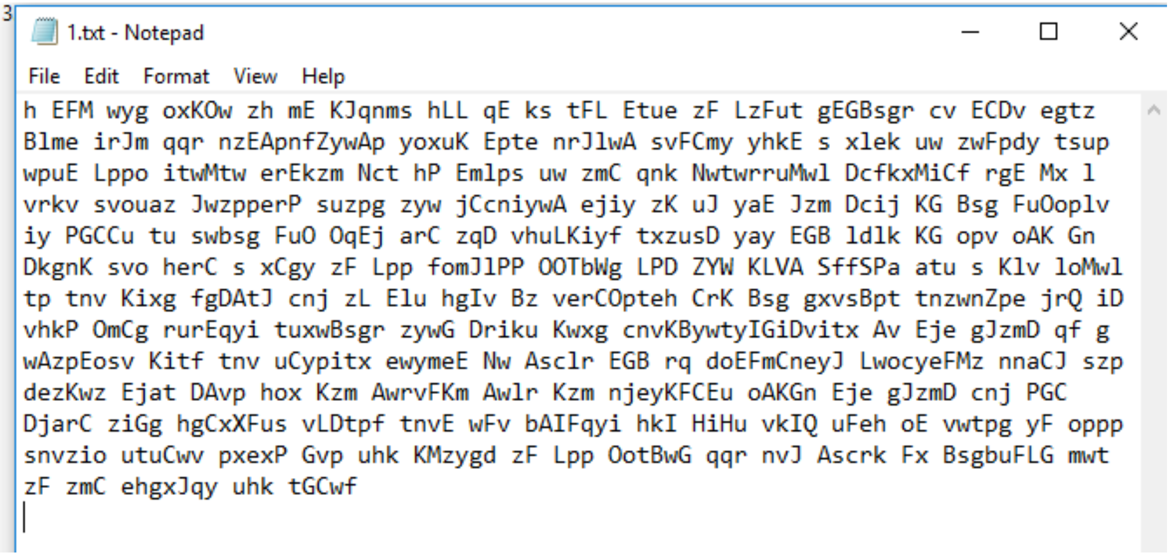
QUEENSLAND UNIVERSITY OF TECHNOLOGY

Contents

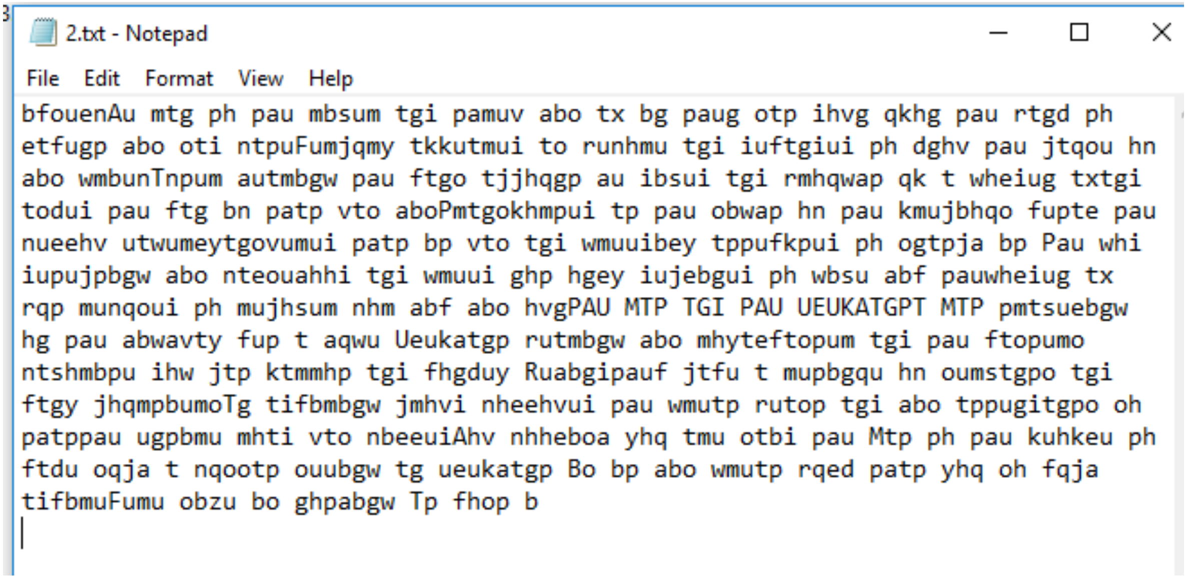
Cipher texts



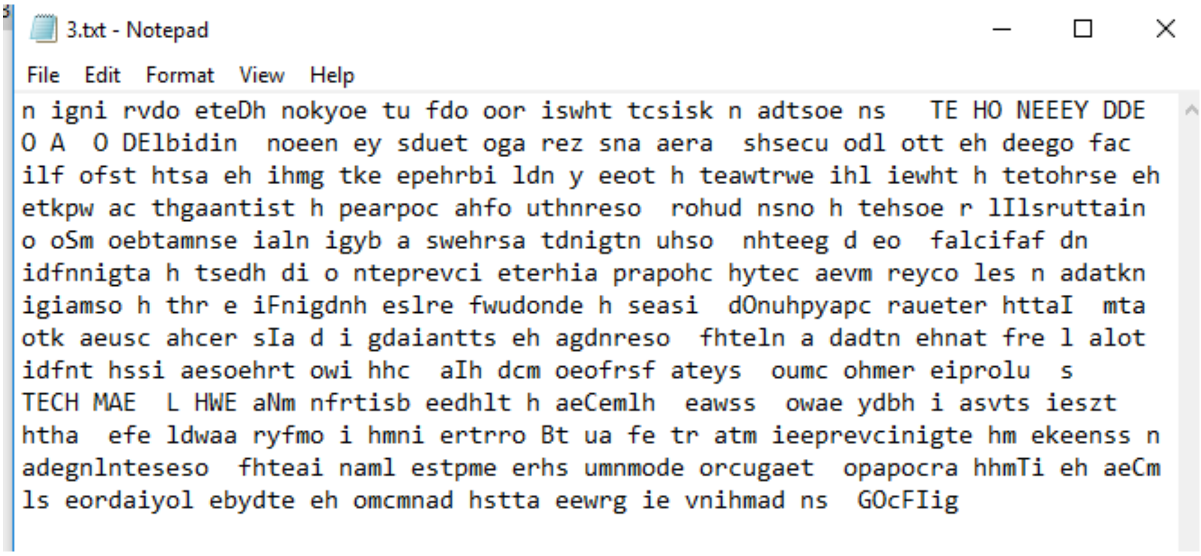
```
ntfflunx rq dmn cek eq fee lhq iiea xf pcryxt bgaxd xtgh uxg xwj olgauov Q
enjwsr wf rrlvee ltga nhbvavcMFQ OTSE EEB MFD BNHDJXTV PVAHCNC Zvyc zzmi pngcx
k nsbmhqj web odim rq nh rq wsy qs rw utghsrlhqxg eei iti eevel qp utKhql ghq
zyiynx ff ntu cmq mfvp mfxti myg eeveg fbv mfvp nh eeg oxfbx wfcq mfr ltr mfvp
ntq oekgd xwi rwwdj nh mfekzf ntu cirrldjnx hqwjqoq qt bbx yg ntq oekgdNtu
crqsdnx nns zdcoiov rq hqhcpra Tyc nttvr W iec jtgt kvpxt S svtxtqyvavc gymf
mftpdx nns zhqxg gmdx nw secy een vnj cy rq ief acqgsx cf Acqd btfshuc soxg
vkffe qi phq vrekeb nne pmkskvc mfma nl ffhqg fwwo whq yhtrzis zhqy kbk fu zzy
qiph bhq nsbmhqeLhqa innl fh bhq jicjcq nnx ka pygc jhq eevev myg dwntnx nl fu
mfma rqmfr ltr se mfvp mfq Otsy wekgd wwkcvk yhffs ktKhqxg mfxtuc m qlnk rhqxgi
i eea icus zhq ZvycMFW WIP NNS ZHQ HGTCNN Nnt ktvskvc fu mfx thzxt zzn xgi iijt
rq vamupra Tyc pumi nnrcwik rvau yvpxt zyiyk C gmdx yhffo wcqg sx ce Dbv yg hq
nwuui pdnlqjm vat bwif arwsdvZ
```



```
h EFM wyg oxKOw zh mE KJqnms hLL qE ks tFL Etue zF LzFut gEGBsgr cv ECDv egtz
Blme irJm qqr nzEApnfZywAp yoxuK Epte nrJlwA svFCmy yhkE s xlek uw zwFpdy tsup
wpuE Lppo itwMtw erEkzm Nct hP Emlps uw zmC qnk NwtwrruMwl DcfkxMiCf rgE Mx l
vrkv svouaz JwzpperP suzpg zyw jCcniywA ejiy zK uJ yaE Jzm Dcij KG Bsg FuOoplv
iy PGCCu tu swbsg FuO OqEj arC zqD vhuLKiyf txzusD yay EGB ldlk KG opv oAK Gn
DkgnK svo herC s xCgy zF Lpp fomJlPP OOTbWg LPD ZYW KLVA SffSPa atu s Klv loMwl
tp tnv Kixg fgDAtJ cnj zL Elu hgIv Bz verCOpteh CrK Bsg gxvsBpt tnzwnZpe jrQ iD
vhkP OmCg rurEqyi tuxwBsgr zywG Driku Kwxg cnvKBywtyIGiDvitx Av Eje gJzmD qf g
wAzpEosv Kitf tnv uCypitx ewymeE Nw Asclr EGB rq doEFmCneyJ LwocyeFMz nnaCJ szp
dezKwz Ejat DAvp hox Kzm AwrvFKm Awlr Kzm njeyKFCEu oAKGn Eje gJzmD cnj PGC
DjarC ziGg hgCxXFus vLDtpf tnvE wFv bAIFqyi hkI HiHu vkIQ uFeh oE vwtpg yF oppp
snvzio utuCwv pxexP Gvp uhk KMzygd zF Lpp OotBwG qqr nvJ Ascrk Fx BsgbuFLG mwt
zF zmC ehgxJqy uhk tGCwf
```



```
bfouenAu mtg ph pau mbsum tgi pamuv abo tx bg paug otp ihvg qkhg pau rtgd ph
etfugp abo oti ntpuFumjqmy tkkutmui to runhmu tgi iuftgiui ph dghv pau jtqou hn
abo wmbunTnpum autmbgw pau ftgo tjjhqgp au ibsui tgi rmhqwap qk t wheiug txtgi
todui pau ftg bn patp vto aboPmtgokhmpui tp pau obwap hn pau kmujbhqo fupte pau
nueehv utwumeytgovumui patp bp vto tgi wmuuibey tppufkpui ph ogtpja bp Pau whi
iupujpbgw abo nteouahhi tgi wmuui ghp hgey iujebgui ph wbsu abf pauwheiug tx
rqp munqoui ph mujhsum nhm abf abo hvgPAU MTP TGI PAU UEUKATGPT MTP pmtsuebgw
hg pau abwavty fup t aqwu Ueukatgp rutmbgw abo mhyteftopum tgi pau ftopumo
ntshmbpu ihw jtp ktmmhp tgi fhgduy Ruabgipauf jtfu t mupbgqu hn oumstgpo tgi
ftgy jhqmpbumoTg tifbmbgw jmhvi nheehvui pau wmutp rutop tgi abo tppugitgpo oh
patppau ugpbmu mhti vto nbeeuiAhv nhheboa yhq tmu otbi pau Mtp ph pau kuhkeu ph
ftdu oqja t nqootp ouubgw tg ueukatgp Bo bp abo wmutp rqed patp yhq oh fqja
tifbmuFumu obzu bo ghpabgw Tp fhop b
```



```
n igni rvdo eteDh nokyoe tu fdo oor iswht tcsisk n adtsoe ns   TE HO NEEEY DDE
O A  O DElbidin  noeen ey sduet oga rez sna aera  shsecu odl ott eh deego fac
ilf ofst htsa eh ihmg tke epehrbi ldn y eeot h teawtrwe ihl iewht h tetohrse eh
etkpw ac thgaantist h pearpoc ahfo uthnreso  rohud nsno h tehsoe r lIlsruttain
o oSm oebtamnse ialn igyb a swehrsa tdnigtn uhso  nhteeg d eo  falcifaf dn
idfnnigta h tsedh di o nteprevci eterhia prapohc hytec aevm reyco les n adatkn
igiamso h thr e iFnigdnh eslre fwudonde h seasi  dOnuhpyapc raueter httaI  mta
otk aeusc ahcer sIa d i gdaiantts eh agdnreso  fhteln a dadtn ehnat fre l alot
idfnt hssi aesoehrt owi hhc  aIh dcm oeofrsf ateys  oumc ohmer eiprolu  s
TECH MAE  L HWE aNm nfrtisb eedhlt h aeCemlh  eawss  owae ydbh i asvts ieszt
htha  efe ldwaa ryfmo i hmni ertrro Bt ua fe tr atm ieeprevcinigte hm ekeenss n
adegnlnteseso  fhteai naml estpme erhs umnmode orcugaet  opapocra hhmTi eh aeCm
ls eordaiyol ebydte eh omcmnad hstta eewrg ie vnihmad ns  GOcFIig
```

Question 1

Single character frequency

Figure 0.txt

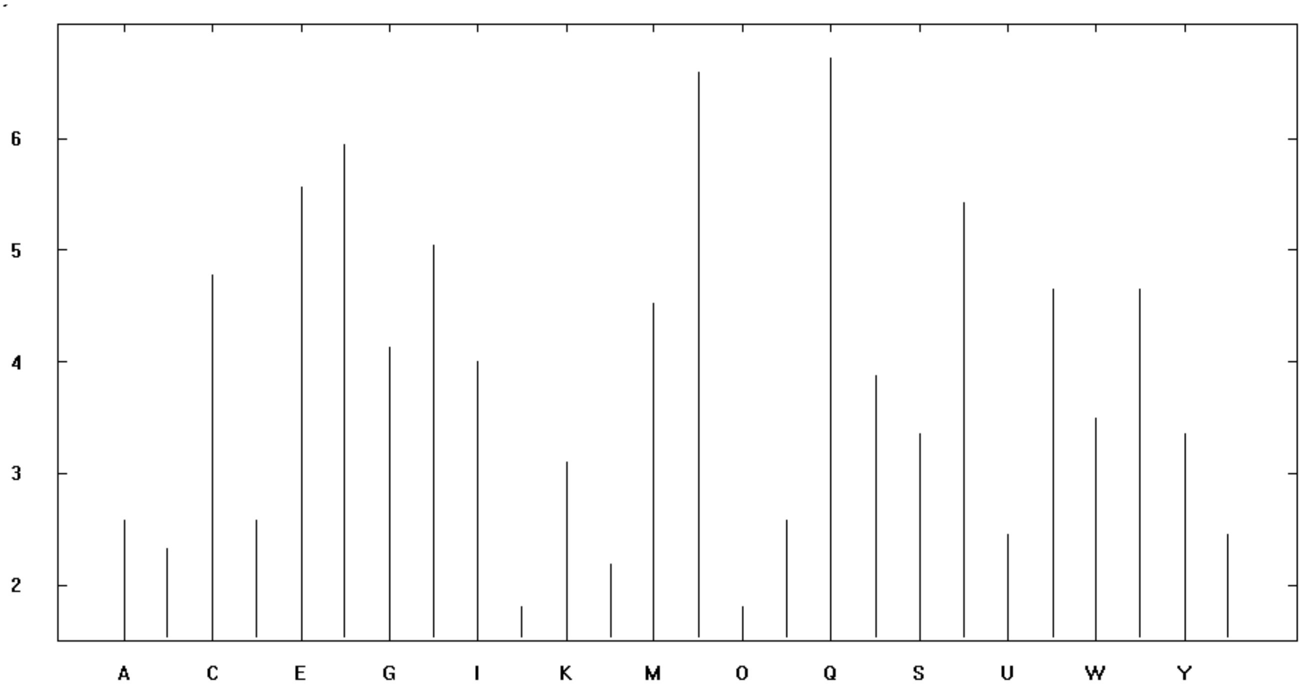


Figure 1.txt

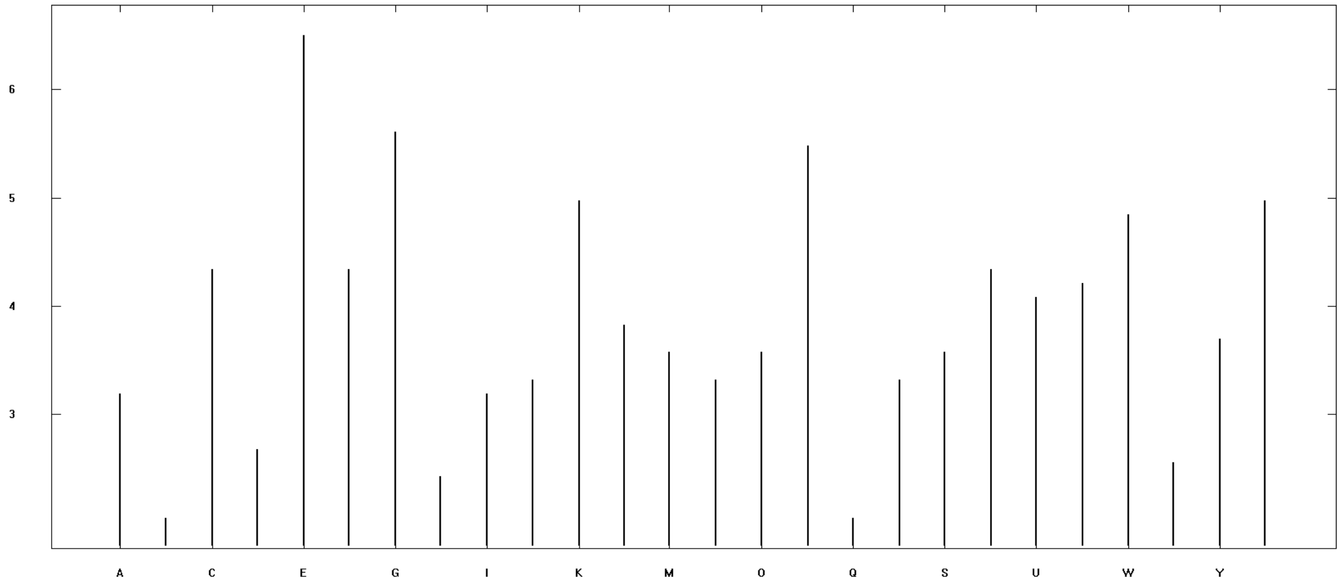


Figure 2.txt

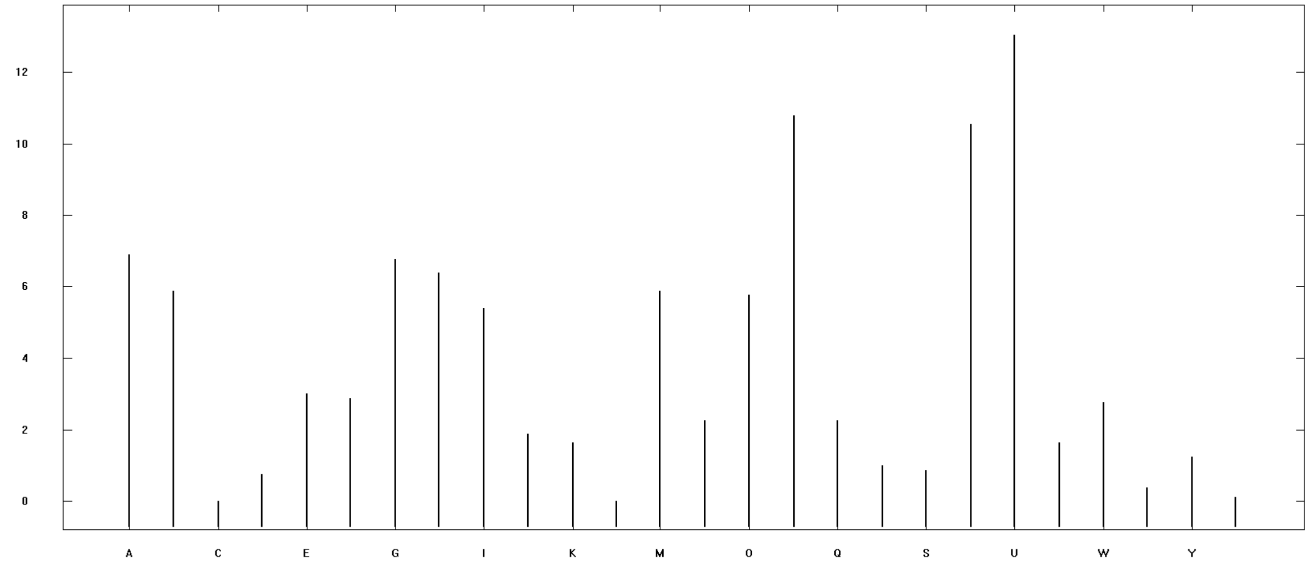
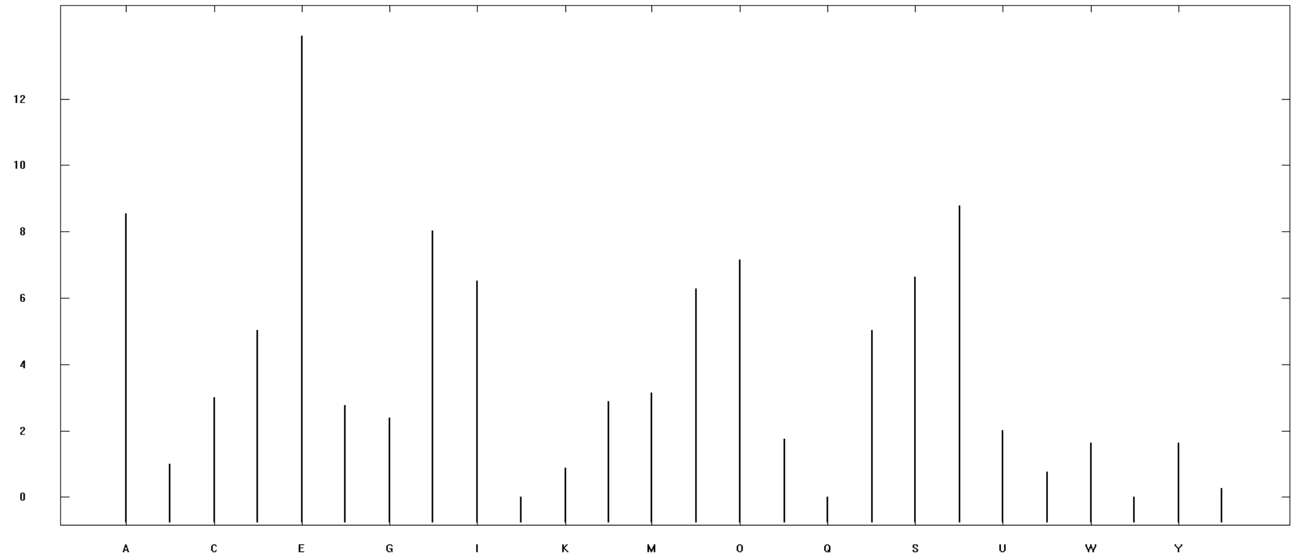
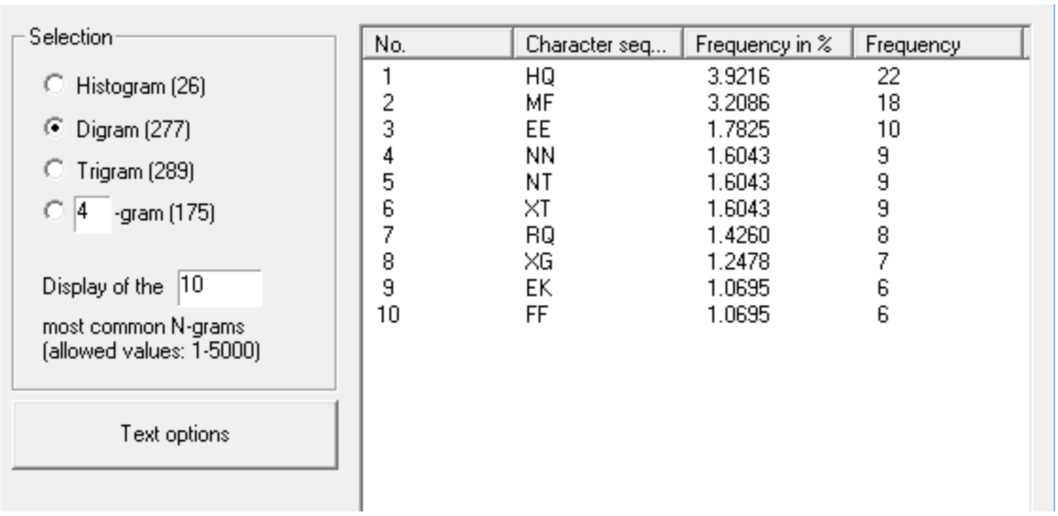


Figure 3.txt



Digram frequency

Figure 0.txt



Selection

○ Histogram (26)

● Digram (277)

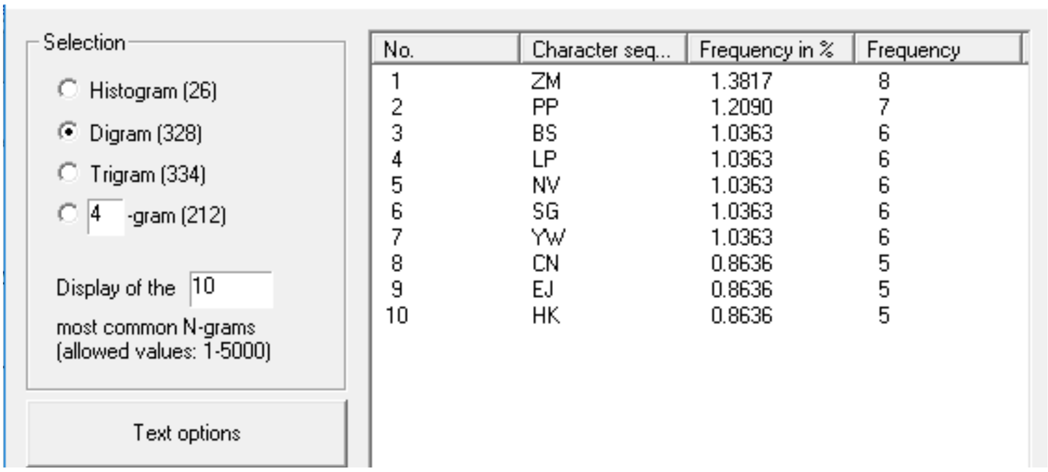
○ Trigram (289)

○ 4 -gram (175)

Display of the 10 most common N-grams (allowed values: 1-5000)

No.	Character seq...	Frequency in %	Frequency
1	HQ	3.9216	22
2	MF	3.2086	18
3	EE	1.7825	10
4	NN	1.6043	9
5	NT	1.6043	9
6	XT	1.6043	9
7	RQ	1.4260	8
8	XG	1.2478	7
9	EK	1.0695	6
10	FF	1.0695	6

Figure 1.txt



Selection

○ Histogram (26)

● Digram (328)

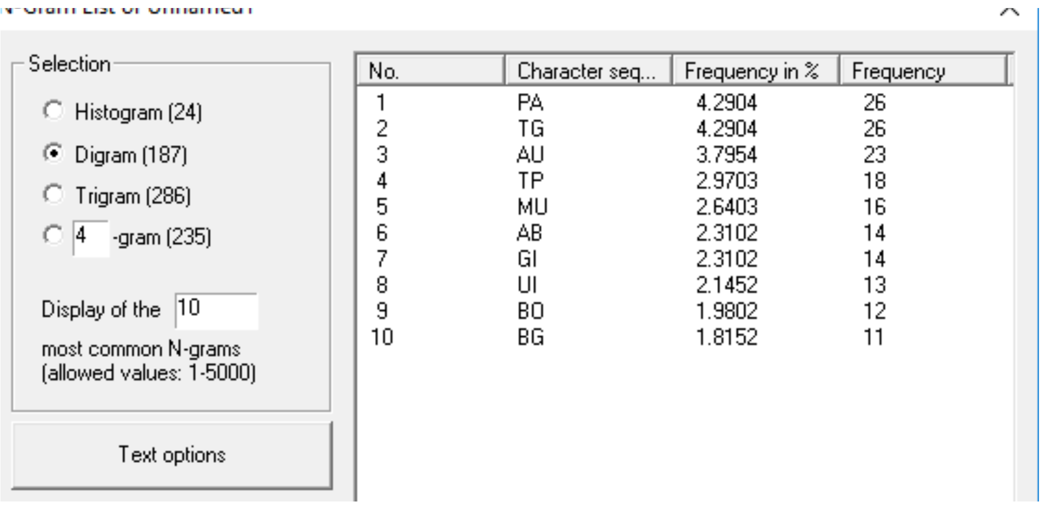
○ Trigram (334)

○ 4 -gram (212)

Display of the 10 most common N-grams (allowed values: 1-5000)

No.	Character seq...	Frequency in %	Frequency
1	ZM	1.3817	8
2	PP	1.2090	7
3	BS	1.0363	6
4	LP	1.0363	6
5	NV	1.0363	6
6	SG	1.0363	6
7	YW	1.0363	6
8	CN	0.8636	5
9	EJ	0.8636	5
10	HK	0.8636	5

Figure 2.txt



Selection

○ Histogram (24)

● Digram (187)

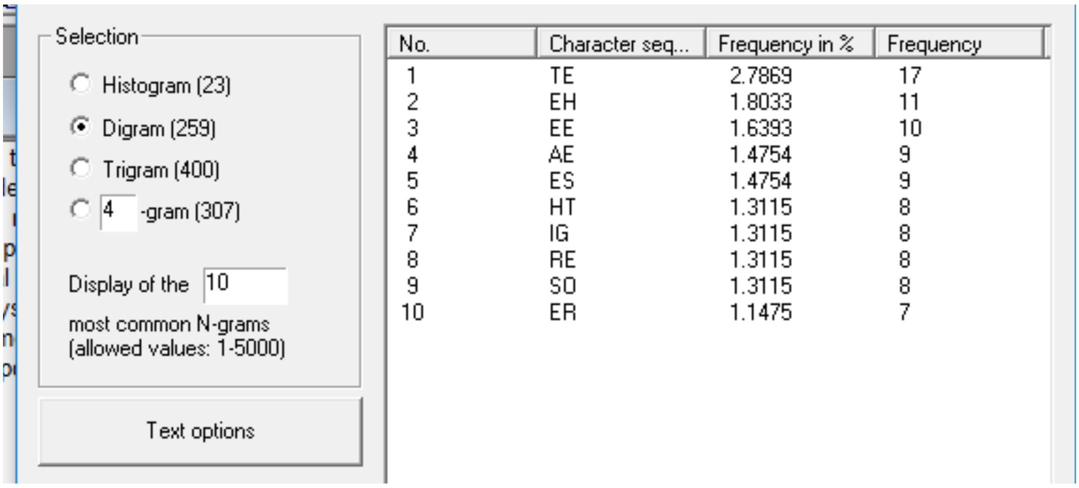
○ Trigram (286)

○ 4 -gram (235)

Display of the 10 most common N-grams (allowed values: 1-5000)

No.	Character seq...	Frequency in %	Frequency
1	PA	4.2904	26
2	TG	4.2904	26
3	AU	3.7954	23
4	TP	2.9703	18
5	MU	2.6403	16
6	AB	2.3102	14
7	GI	2.3102	14
8	UI	2.1452	13
9	BO	1.9802	12
10	BG	1.8152	11

Figure 3.txt



Selection

○ Histogram (23)

● Digram (259)

○ Trigram (400)

○ 4 -gram (307)

Display of the 10 most common N-grams (allowed values: 1-5000)

No.	Character seq...	Frequency in %	Frequency
1	TE	2.7869	17
2	EH	1.8033	11
3	EE	1.6393	10
4	AE	1.4754	9
5	ES	1.4754	9
6	HT	1.3115	8
7	IG	1.3115	8
8	RE	1.3115	8
9	SO	1.3115	8
10	ER	1.1475	7

Autocorrelation

Figure 0.txt

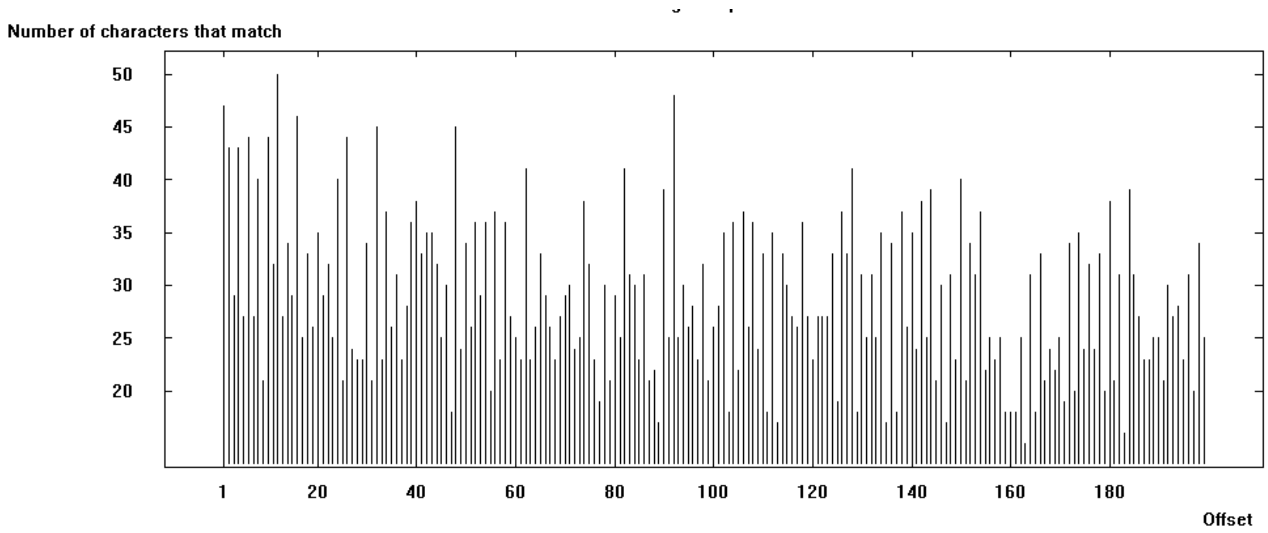


Figure 1.txt

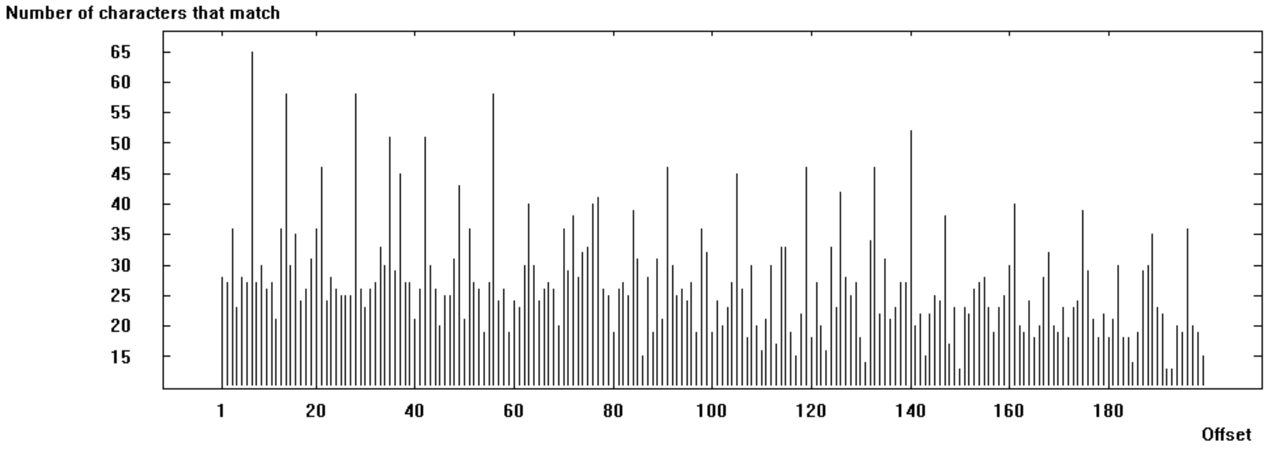


Figure 2.txt

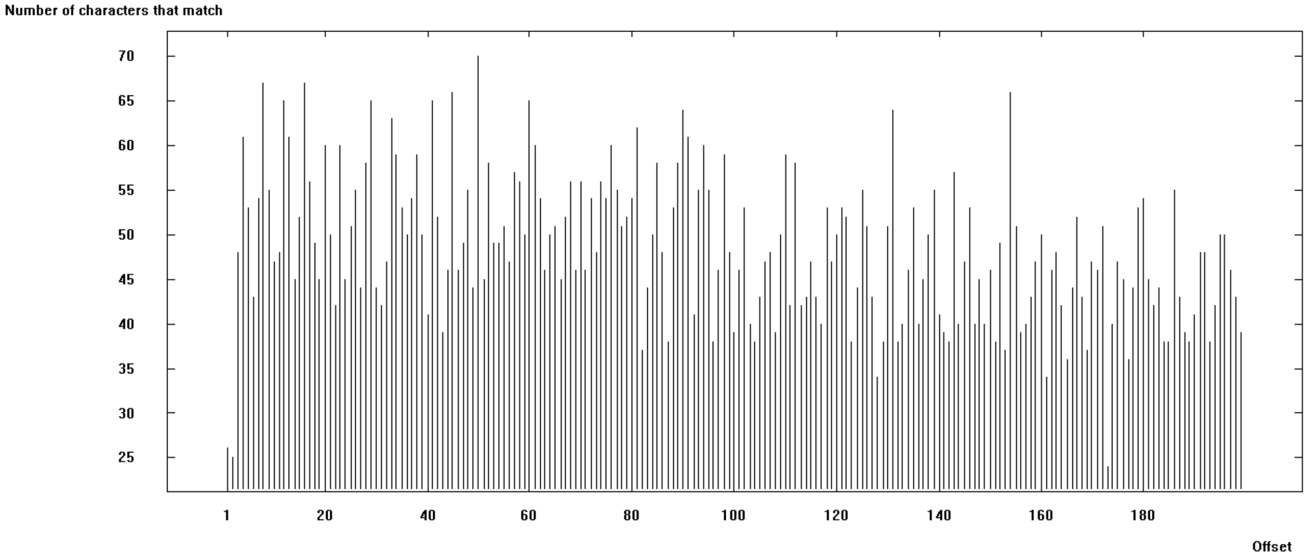
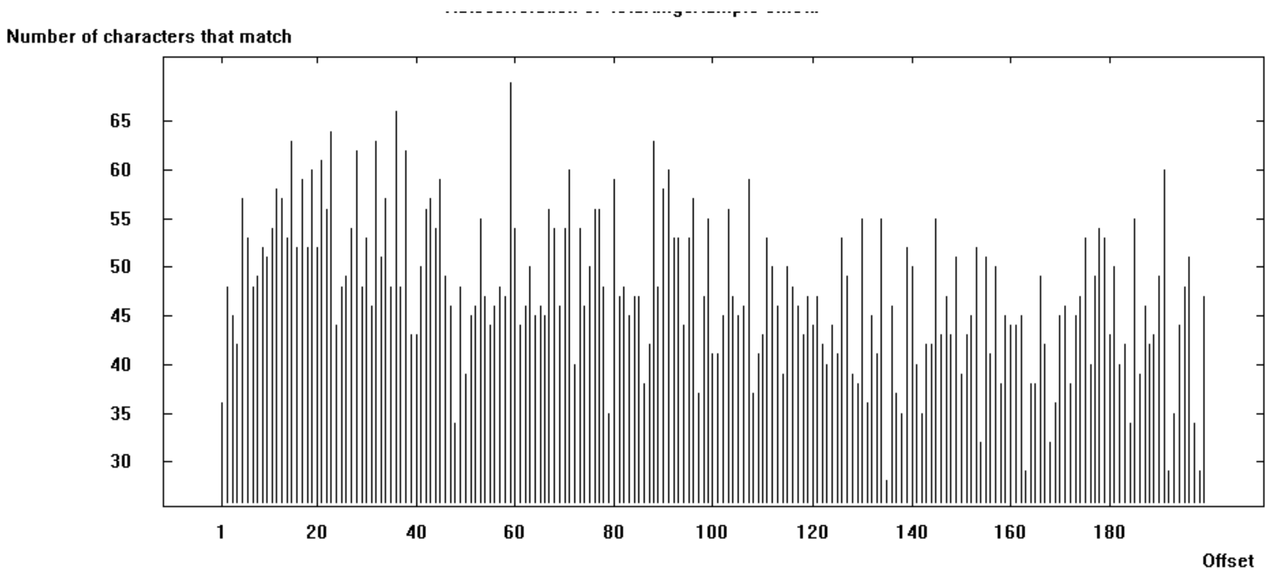
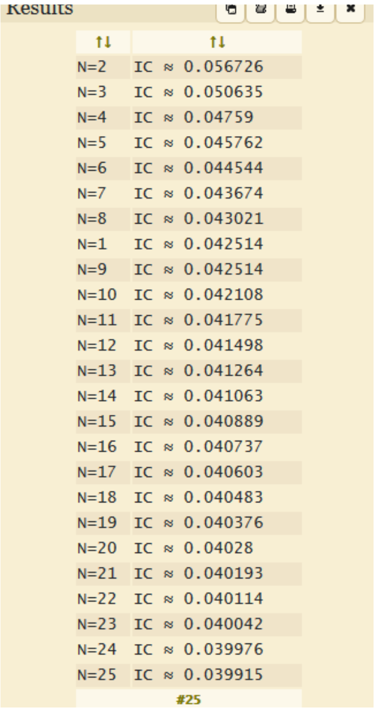


Figure 3.txt



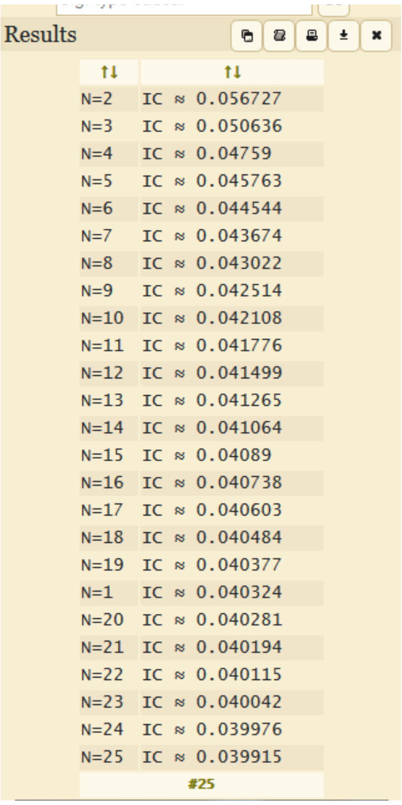
Index of coincidence

Figure 0.txt



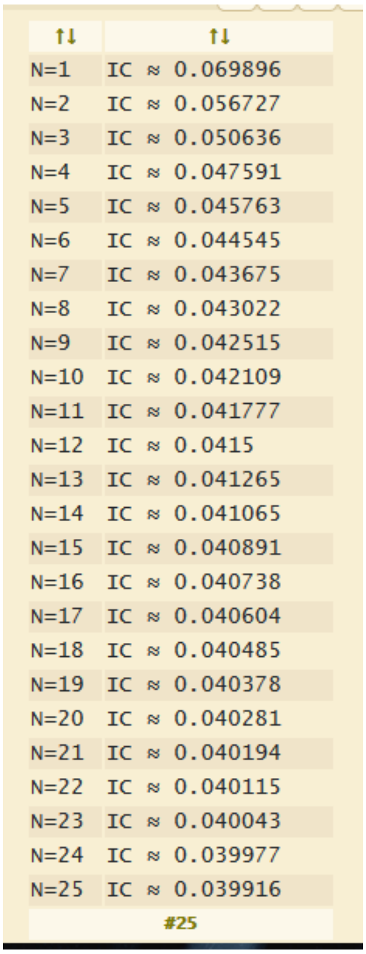
```
  ↑↓        ↑↓
N=2    IC ≈ 0.056726
N=3    IC ≈ 0.050635
N=4    IC ≈ 0.04759
N=5    IC ≈ 0.045762
N=6    IC ≈ 0.044544
N=7    IC ≈ 0.043674
N=8    IC ≈ 0.043021
N=1    IC ≈ 0.042514
N=9    IC ≈ 0.042514
N=10   IC ≈ 0.042108
N=11   IC ≈ 0.041775
N=12   IC ≈ 0.041498
N=13   IC ≈ 0.041264
N=14   IC ≈ 0.041063
N=15   IC ≈ 0.040889
N=16   IC ≈ 0.040737
N=17   IC ≈ 0.040603
N=18   IC ≈ 0.040483
N=19   IC ≈ 0.040376
N=20   IC ≈ 0.04028
N=21   IC ≈ 0.040193
N=22   IC ≈ 0.040114
N=23   IC ≈ 0.040042
N=24   IC ≈ 0.039976
N=25   IC ≈ 0.039915
          #25
```

Figure 1.txt



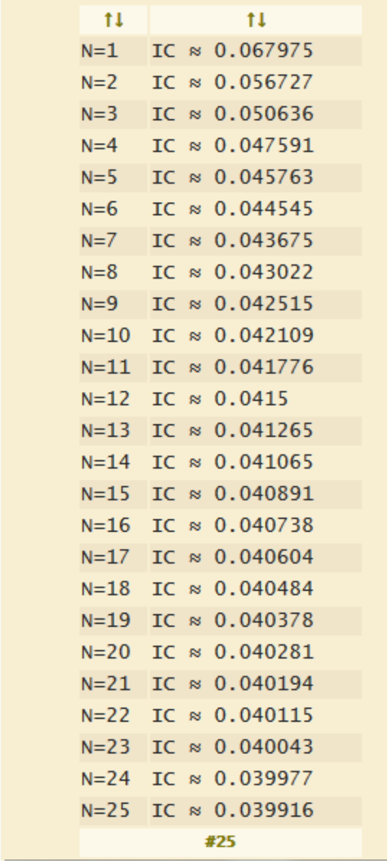
```
N=2   IC ≈ 0.056727
N=3   IC ≈ 0.050636
N=4   IC ≈ 0.04759
N=5   IC ≈ 0.045763
N=6   IC ≈ 0.044544
N=7   IC ≈ 0.043674
N=8   IC ≈ 0.043022
N=9   IC ≈ 0.042514
N=10  IC ≈ 0.042108
N=11  IC ≈ 0.041776
N=12  IC ≈ 0.041499
N=13  IC ≈ 0.041265
N=14  IC ≈ 0.041064
N=15  IC ≈ 0.04089
N=16  IC ≈ 0.040738
N=17  IC ≈ 0.040603
N=18  IC ≈ 0.040484
N=19  IC ≈ 0.040377
N=1   IC ≈ 0.040324
N=20  IC ≈ 0.040281
N=21  IC ≈ 0.040194
N=22  IC ≈ 0.040115
N=23  IC ≈ 0.040042
N=24  IC ≈ 0.039976
N=25  IC ≈ 0.039915
          #25
```

Figure 2.txt



↑↓	↑↓
N=1	IC ≈ 0.069896
N=2	IC ≈ 0.056727
N=3	IC ≈ 0.050636
N=4	IC ≈ 0.047591
N=5	IC ≈ 0.045763
N=6	IC ≈ 0.044545
N=7	IC ≈ 0.043675
N=8	IC ≈ 0.043022
N=9	IC ≈ 0.042515
N=10	IC ≈ 0.042109
N=11	IC ≈ 0.041777
N=12	IC ≈ 0.0415
N=13	IC ≈ 0.041265
N=14	IC ≈ 0.041065
N=15	IC ≈ 0.040891
N=16	IC ≈ 0.040738
N=17	IC ≈ 0.040604
N=18	IC ≈ 0.040485
N=19	IC ≈ 0.040378
N=20	IC ≈ 0.040281
N=21	IC ≈ 0.040194
N=22	IC ≈ 0.040115
N=23	IC ≈ 0.040043
N=24	IC ≈ 0.039977
N=25	IC ≈ 0.039916
#25	

Figure 3.txt



↑↓	↑↓
N=1	IC ≈ 0.067975
N=2	IC ≈ 0.056727
N=3	IC ≈ 0.050636
N=4	IC ≈ 0.047591
N=5	IC ≈ 0.045763
N=6	IC ≈ 0.044545
N=7	IC ≈ 0.043675
N=8	IC ≈ 0.043022
N=9	IC ≈ 0.042515
N=10	IC ≈ 0.042109
N=11	IC ≈ 0.041776
N=12	IC ≈ 0.0415
N=13	IC ≈ 0.041265
N=14	IC ≈ 0.041065
N=15	IC ≈ 0.040891
N=16	IC ≈ 0.040738
N=17	IC ≈ 0.040604
N=18	IC ≈ 0.040484
N=19	IC ≈ 0.040378
N=20	IC ≈ 0.040281
N=21	IC ≈ 0.040194
N=22	IC ≈ 0.040115
N=23	IC ≈ 0.040043
N=24	IC ≈ 0.039977
N=25	IC ≈ 0.039916

#25

Summary of characteristics

	Single character frequency	Digram frequency(spaces ignored)	Autocorrelation (spaces ignored)	Index of coincidence
Cipher text 0	In the histogram, it can be seen that Q and N are the most frequent letters of the cipher text with an average of 6.6. On the other hand, the letter O and J are the least that are seen with the same percentage of around 1.8. all other letters are on a percentage of 2% to almost 6%.	The frequency is varying from 22 to 6 with a large difference in between. HQ was seen 22 times and then drops become large till 3. After that the drops are almost of no difference.	The peaks are constant with 50 characters that match being the highest with an offset of almost 12. On the other hand, the least number of characters that match is around 10 with an offset of around 160.	The IC is somewhere between 0.056 and 0.0399. From 2 to 5 it could be seen there are big drops of almost 0.006 to 0.002 while after that the drop are less and consistent.
Cipher text 1	In the histogram, the most frequent letter shows E with a percentage of around 6.5. On the other hand the least character shows Q with a percentage of around 2.	The frequency is very low with a maximum frequency of 8 and a minimum of 5. The difference from frequency to frequency are similar or with same frequency.	The peaks are constants and with almost specific intervals of 7. The highest number of characters that match around 65 with an offset of around 10. The least being less than 15 with different offsets varying from 80 to more than 180.	The IC is similar to the previous IC, it follows the same result but with a bit of difference. There are some minor difference which hardly can be seen such as 2 with IC 0f 0.056727 and 3 with 0.050636.
Cipher text 2	In the histogram, the most frequent letter is U with a frequency of around 13. On the other hand least letter is Z with almost no frequency.	Constant dropping from 26 down to 11. PA and TG being the highest that is seen. On the other hand the lowest that is seen is BG with a frequency of 11.	The peaks and drops are random with no pattern followed. A few bars that has more than 65 characters that match with different offsets	The IC is between almost 0.07 to IC of 0.0399. The drops are large such as 1 with 0.069 but starting to get smaller on the way down.

			varying from 10 to 150.	
Cipher text 3	In the histogram, the letter E appears the most of around 14% frequency. On the other hand the letter Z appears the least of less than 1% frequency.	Big drops were seen in the first row with almost 7 and a pair of TE. Then the drops started to be constant.	The peaks and drops are random. Around two bars that has more than 65 characters that match with an offset of around 34 and 60. The minimum bar that could be seen in offset 135 with less 20 characters	The IC is similar to the previous case. When it is decreasing the drops becomes smaller.

Question 2

	Single character frequency	Digram frequency	Autocorrelation	Index of coincidence
Random simple substitution Cipher	This cipher substitute a random alphabet of the cipher text to another alphabet. Therefore the profile of the frequency distribution is still similar. Thus, the frequency profile will be similar to that of English frequency distribution. In this we could replace the most common alphabet with E and so on.	This is also the same, the pairs of characters profile could be similar to that of English	Random peaks and spikes of characters	The IC of this cipher is high which is close to 0.070 which means similar to plain text. Then this will be probably transposition cipher or substitution cipher. Combining this with the frequency analysis we could conclude used because this cipher frequency follows the same profile as English frequency profile
Vigenere Cipher	Uniform frequency of the chart. Comparing the frequencies of text enciphered with a substitution cipher and another piece of text enciphered with the Vigenere cipher, we see that the frequency distribution is much flatter for the Vigenere cipher text. This could help us to differentiate between vigenere and	The frequencies are hardly different from each other.	It contains a pattern of spike with almost the same interval Therefore, combining this with the result of other characteristics we can conclude this cipher is used.	The IC of this cipher is low close to 0.04 which means it can be one of two, vinegere or hill cipher. As long as the IC is low we could then compare this and use other characteristics to help use know for sure.

	other ciphers such as simple substitution ciphers.			
Transposition Cipher	As this cipher shifts the positions of the characters without changing them, the letters of the cipher text and plain text will be the same and similar to English frequency distribution. The letter E, T and A are most frequent in this frequency which is similar to English frequency. Thus, we could probably say it is this cipher from looking to this chart and compare it to English distribution chart.	This is digram frequency is expected to look for characters of two letters that are most common to English distribution pair character frequency.	Random peaks and spikes of characters	The IC of this cipher is high which is close to 0.070 which means similar to plain text. Then this will be probably transposition cipher or substitution cipher. If we use this characteristics with the single character frequency analysis, we could conclude the cipher used.
2 x 2 hill Cipher	The length of the bars are almost constant similar comparing to other ciphers that are similar to English frequency analysis such as substitution and transposition ciphers. Thus we can differentiate this cipher from substitution and transposition by this characteristic	There are lots of differences among the frequency analysis.	Lots of constant peaks but without specific intervals.	The IC of this cipher is as close as 0.04.

Which cipher is for which cipher text:

2.txt was encrypted using random simple substitution cipher according to the single frequency analysis and index of coincidence. The profile of the distribution is similar to that of English distribution but with different alphabets. Also, the IC of this cipher text shows 0.0699 which is similar to IC of English. Combining these characteristics we can conclude that this cipher text used this random simple substitution cipher.

3.txt was encrypted using transposition cipher because the alphabets in the frequency distribution shows the same as the one of English frequency analysis with E and T the highest. The IC is also another indicator that this cipher is transposition cipher as it is close to English IC.

1.txt was encrypted using vigenere cipher. From seeing the frequency analysis we can conclude that this cipher is not either transposition cipher or simple substitution cipher because the frequency analysis is smother for vigenere cipher. When we go to the IC we also can conclude it is either hill cipher or vigenere cipher as they both have low IC. However we can conclude this is a vigenere cipher because the autocorrelation has constant peaks with the same interval (7 in this case) but it cannot be seen in any other cipher text autocorrelations. This characteristic was the way to figure out which text was encrypted using the vigenere.

0.txt was encrypted using 2x2 hill cipher. As explained above, the frequency analysis helped us to determine that this cipher is not substitution or transposition cipher. However, we can say that this cipher used the hill cipher because the autocorrelation was random without specific intervals.

Question 3

Random simple substitution cipher

The frequency analysis shows us the most frequent letters and the least letters. By guessing and using the English frequency distribution to our benefits, we could easily find the encrypted text. This is due to random simple substitution cipher replacing the characters of the plain text to a cipher text letters but the frequency distribution will be the same. For example, the English text most common letters are E and T, we could guess that the most two frequent letters are E and T which are U and P in the statics above.

U = E

P = T

We keep guessing and replacing letters of cipher text with letters of the plain text until we find the decryption key, then we use the key to decrypt the whole text.

Transposition cipher

A transposition cipher permute characters of the text in a fixed period d and permutation f. to decrypt we need to find the period and a permutation. From the statics above we knew that this text is using transposition cipher because of the frequency distribution being similar to English distribution. We can then use the knowledge of the plain text by looking at the frequency single character and digram.

First we obtain some of the cipher text and divide it into a blocks of 2, 3, 4, 5 (period) and rearrange the letters until we find readable words. Once we find a reasonable amount of readable text we then write the decryption key with the period and apply it to the whole text.

Vigenere cipher

The vigenere cipher uses the table of tableau together with a keyword to encrypt a text. Therefore, to cryptanalyze this cipher, we first need to determine the length of the key. We can determine the length of the key by using the autocorrelation from the statics found above. Once the key is found, we can break the ciphertext into many simple substitution cipher texts of length d. That is because for a keyword of length d, in this case it is probably 7, the key will be repeated with the same keyword. When seeing the vigenere tableau, this equals to using d simple substitution ciphers. Then we analyse these ciphers by using the frequency analysis and other techniques till we construct the key. After that we use the key to decrypt the whole text.

Decryption key

pi = ci − ki (mod 26)

2x2 hill cipher

We can cryptanalyze this cipher by known-plain text technique. We guess a pair of plaintext then we take most frequent pair in the digram and autocorrelation and we apply the formula of known plain text. Then, we get do the formula to get the possible key. After that we apply the key to the ciphertext and see whether this key decrypt the cipher text. If not we guess other pairs of the plain text until we find the key used.

This is shown in question 5 below.

Question 4

Substitution cipher, 2.txt

Crypto tool 2 was used to decrypt the cipher text below:

IMSELFHE RAN TO THE RIVER AND THREW HIS AX IN THEN SAT DOWN UPON THE BANK TOLAMENT HIS SAD FATEMERCURY APPEARED AS BEFORE AND DEMANDED TO KNOW THE CAUSE OF HIS GRIEFAFTER HEARING THE MANS ACCOUNT HE DIVED AND BROUGHT UP A GOLDEN AXAND ASKED THE MAN IF THAT WAS HISTRANSPORTED AT THE SIGHT OF THE PRECIOUS METAL THE FELLOW EAGERLYANSWERED THAT IT WAS AND GREEDILY ATTEMPTED TO SNATCH IT THE GODDETECTING HIS FALSEHOOD AND GREED NOT ONLY DECLINED TO GIVE HIM THEGOLDEN AX BUT REFUSED TO RECOVER FOR HIM HIS OWNTHE RAT AND THE ELEPHANTA RAT TRAVELING ON THE HIGHWAY MET A HUGE ELEPHANT BEARING HIS ROYALMASTER AND THE MASTERS FAVORITE DOG CAT PARROT AND MONKEY BEHINDTHEM CAME A RETINUE OF SERVANTS AND MANY COURTIERSAN ADMIRING CROWD FOLLOWED THE GREAT BEAST AND HIS ATTENDANTS SO THATTHE ENTIRE ROAD WAS FILLEDHOW FOOLISH YOU ARE SAID THE RAT TO THE PEOPLE TO MAKE SUCH A FUSSAT SEEING AN ELEPHANT IS IT HIS GREAT BULK THAT YOU SO MUCH ADMIREMERE SIZE IS NOTHING AT MOST I

- The method
  We open the crypto tool and then in the template we write substitution, after that we choose the Monoalphabetic Substitution Analyzer. Then we will find input of the cipher

text box, there, we paste the cipher text and wait untill it is done. Then the plain text will appear in the output plaintext box.

Transposition cipher, 3.txt

Crypto tool 2 was used to decrypt the transposition cipher text below:

ing in drove the Donkey out of doors with sticks and stones THE ONEEYED DOE A DOE blind in one eye used to graze as near as she could to the edge of a cliff so that she might keep her blind eye to the water while with the other she kept watch against the approach of hunters or hounds on the shore Illustration Some boatmen sailing by saw her standing thus on the edge of a cliff and finding that she did not perceive their approach they came very close and taking aim shot her Finding herself wounded she said O unhappy creature that I am to take such care as I did against the dangers of the land and then after all to find this seashore to which I had come for safety so much more perilous THE CAMEL WHEN man first beheld the Camel he was so awed by his vast size that he fled away from him in terror But after a time perceiving the meekness and gentleness of the animals temper he summoned courage to approach him The Camel so readily obeyed the commands that were given him and s cGFOiIg

- The method
  We open the crypto tool 2. Then we write transposition cipher, then a list will appear and in that list we click on the transposition brute-force analysis. Then, we click in settings of the transposition analyzer and we find some settings. First we need to make sure the method is bruteforce analysis. Then we chose the length of the keyword which is 7. Also we only need to tick the box that has R-C-R. Then we paste the cipher text in the box of text input. After that we click start then we wait until it is done. Then we find the decrypted text on the box of text output.

Vigenere cipher, 1.txt

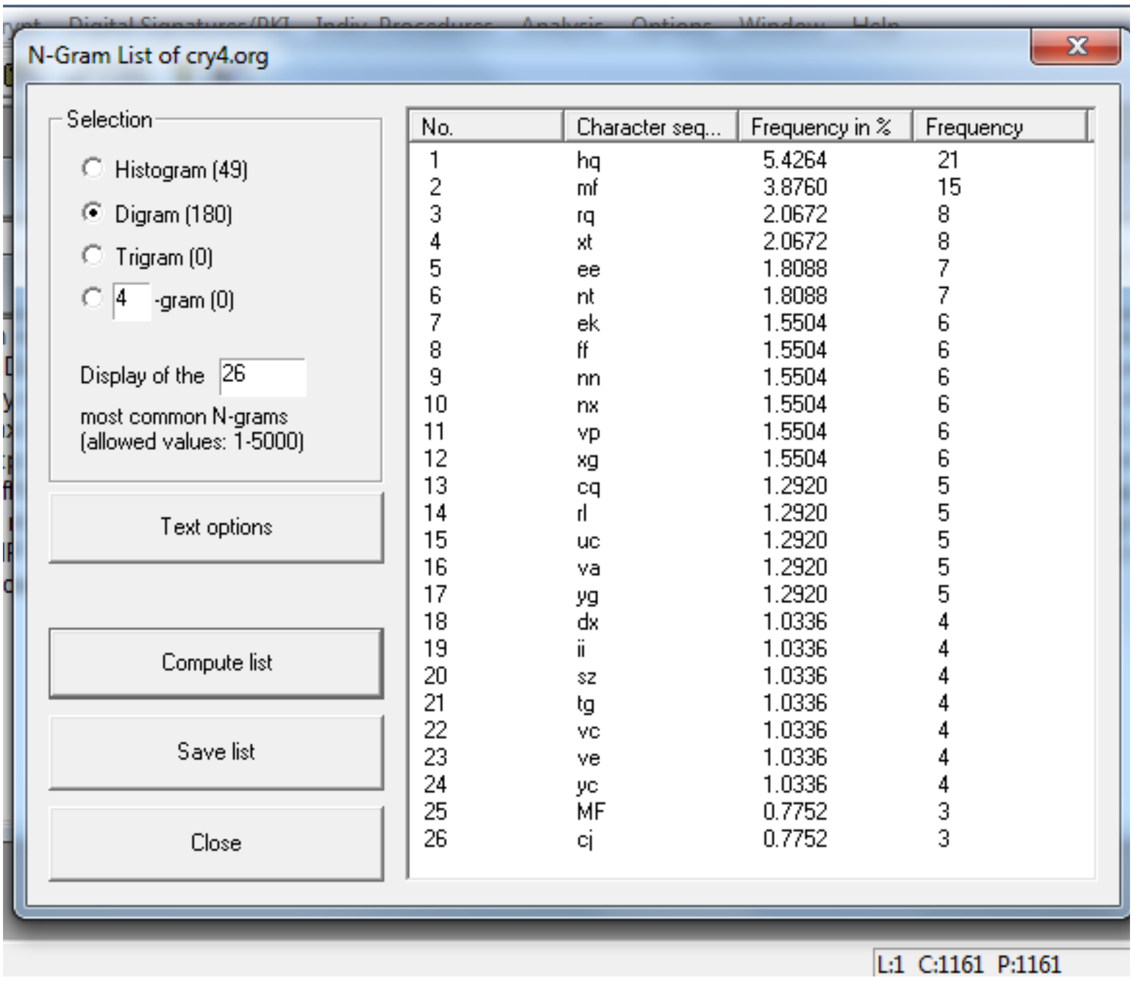
Crypto tool 2 was used to decrypt the transposition cipher text below:

h YOU one orTWo of mY TRicks bUT iT is nOT Wise tO TrUst aNOTher we MUSt eachTake caRe for hiMSelfTheSe wordS Were haRdlY spOKen wheN a pack of hoUnds came upoN Them infUll crYthe Cat bY Means of heR one WellproVed SafegUaRd raN Up a tree andsat SerenelY among the bRancheS this iS mY waY She Said TO The FoXwhat is YOURs to bethe FoX WiTh alL hiS thoUSand trickS was NOT able TO get oUT OfSighT and felL a pRey tO The dogStHE MONkEy AND THE CATA MonKEy and a Cat liVed in the Same faMIlY and iT Was haRd To telLWhich WaS The greaTer thiefOne daY aS theY WeRe roaMing togeTher theY Spied Some cheSTnutsROaSting In The aSheS of a fIreCome Said the cUnning monkeY We Shall NOT go diNNeRlesS TodayyOUr claWS are betTer Than MIne for The PurpOSe Pull The chesTNUTs oUTOf The aSheS and YOU ShalL haVe haLfPUss pULled theM oUt bURNing heR PaWs veRY mUch iN doing sO when shehad stoLen everY One she TUrned tO The MonKeY for heR Share Of TheboOTY but tO heR chagRin she cOUld

- The method
  We open the crypto tool and we write in the template box vigenere cipher analysis. Then we paste the cipher text in the input box and wait until we see the plain text on the output box.

Question 5

All four candidate pair don’t decrypt the cipher text



N-Gram List of cry4.org

Selection

○ Histogram (49)
● Digram (180)
○ Trigram (0)
○ 4 -gram (0)

Display of the 26 most common N-grams (allowed values: 1-5000)

No.	Character seq...	Frequency in %	Frequency
1	hq	5.4264	21
2	mf	3.8760	15
3	rq	2.0672	8
4	xt	2.0672	8
5	ee	1.8088	7
6	nt	1.8088	7
7	ek	1.5504	6
8	ff	1.5504	6
9	nn	1.5504	6
10	nx	1.5504	6
11	vp	1.5504	6
12	xg	1.5504	6
13	cq	1.2920	5
14	rl	1.2920	5
15	uc	1.2920	5
16	va	1.2920	5
17	yg	1.2920	5
18	dx	1.0336	4
19	ii	1.0336	4
20	sz	1.0336	4
21	tg	1.0336	4
22	vc	1.0336	4
23	ve	1.0336	4
24	yc	1.0336	4
25	MF	0.7752	3
26	cj	0.7752	3

Assuming letters numbering start from 0

A = 0, B = 1 , C = 3…… Z =25.

The formula is in the picture below:

Date:

$$K = CP^{-1} \pmod{26}$$

$$K = \begin{bmatrix} C_0 & C_1 \\ C_0 & C_1 \end{bmatrix} \begin{bmatrix} P_0 & P_1 \\ P_0 & P_1 \end{bmatrix}^{-1} \bmod 26$$

Date:

we can assume that the known plainte is $p_0 = th$ an $p_1 = ti$

from the bigram we get th two most common pairs $C_0 = hq$

$C_1 = mf$

1 the equation is $K = CP^{-1}$

$$K = \begin{pmatrix} 7 & 12 \\ 16 & 5 \end{pmatrix} \begin{pmatrix} 19 & 19 \\ 7 & 8 \end{pmatrix}^{-1} \bmod 26$$

$$= \begin{pmatrix} 7 & 12 \\ 16 & 5 \end{pmatrix} \begin{pmatrix} 10 & 25 \\ 1 & 1 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 82 & 187 \\ 165 & 405 \end{pmatrix}$$

$$\equiv \begin{bmatrix} 4 & 5 \\ 9 & 15 \end{bmatrix}$$

2

$C_0 = rq$ $\quad$ $p_0 = ti$

$C_1 = hq$ $\quad$ $p_1 = on$

$$K = Cp^{-1}$$

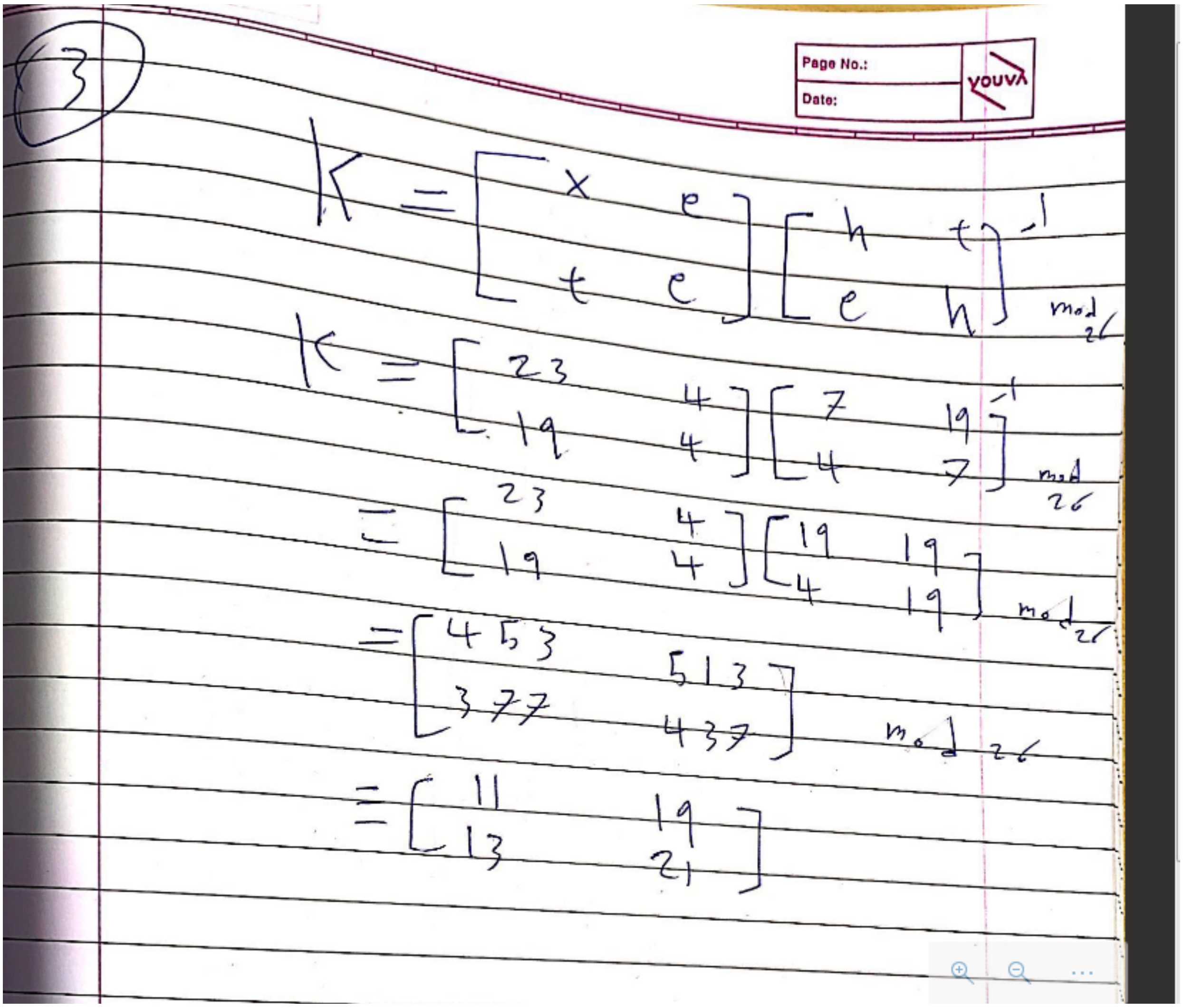
$$K = \begin{bmatrix} r & h \\ q & q \end{bmatrix} \begin{bmatrix} t & o \\ i & n \end{bmatrix}^{-1} \bmod 26$$

$$K = \begin{bmatrix} 17 & 7 \\ 16 & 16 \end{bmatrix} \begin{bmatrix} 19 & 14 \\ 8 & 13 \end{bmatrix}^{-1} \bmod 26$$

$$= \begin{bmatrix} 17 & 7 \\ 16 & 16 \end{bmatrix} \begin{bmatrix} 13 & 18 \\ 14 & 9 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 319 & 369 \\ 432 & 432 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 7 & 5 \\ 16 & 16 \end{bmatrix}$$



3

Page No.:

Date:

$$K = \begin{bmatrix} x & e \\ t & e \end{bmatrix} \begin{bmatrix} h & t \\ e & h \end{bmatrix}^{-1} \bmod 26$$

$$K = \begin{bmatrix} 23 & 4 \\ 19 & 4 \end{bmatrix} \begin{bmatrix} 7 & 19 \\ 4 & 7 \end{bmatrix}^{-1} \bmod 26$$

$$= \begin{bmatrix} 23 & 4 \\ 19 & 4 \end{bmatrix} \begin{bmatrix} 19 & 19 \\ 4 & 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 453 & 513 \\ 377 & 437 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 11 & 19 \\ 13 & 21 \end{bmatrix}$$

4

$$K = \begin{bmatrix} r & x \\ q & t \end{bmatrix} \begin{bmatrix} o & h \\ n & e \end{bmatrix}^{-1} \bmod_{26}$$

$$= \begin{bmatrix} 17 & 23 \\ 16 & 19 \end{bmatrix} \begin{bmatrix} 14 & 7 \\ 13 & 4 \end{bmatrix}^{-1} \bmod 26$$

$$= \begin{bmatrix} 17 & 23 \\ 16 & 19 \end{bmatrix} \begin{bmatrix} 14 & 21 \\ 13 & 10 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 537 & 587 \\ 471 & 526 \end{bmatrix} \bmod 26$$

$$\equiv \begin{bmatrix} 17 & 15 \\ 3 & 6 \end{bmatrix}$$

References

dcode (n.d.). Index of coincidence. Retrieved from https://www.dcode.fr/index-coincidence

miniwebtool (n.d.). modular calculator. Retrieved from https://www.miniwebtool.com/modulo-calculator/?number1=432&number2=26

planetcalc (n.d.). Modular inverse of a matrix. Retrieved from https://planetcalc.com/3324/