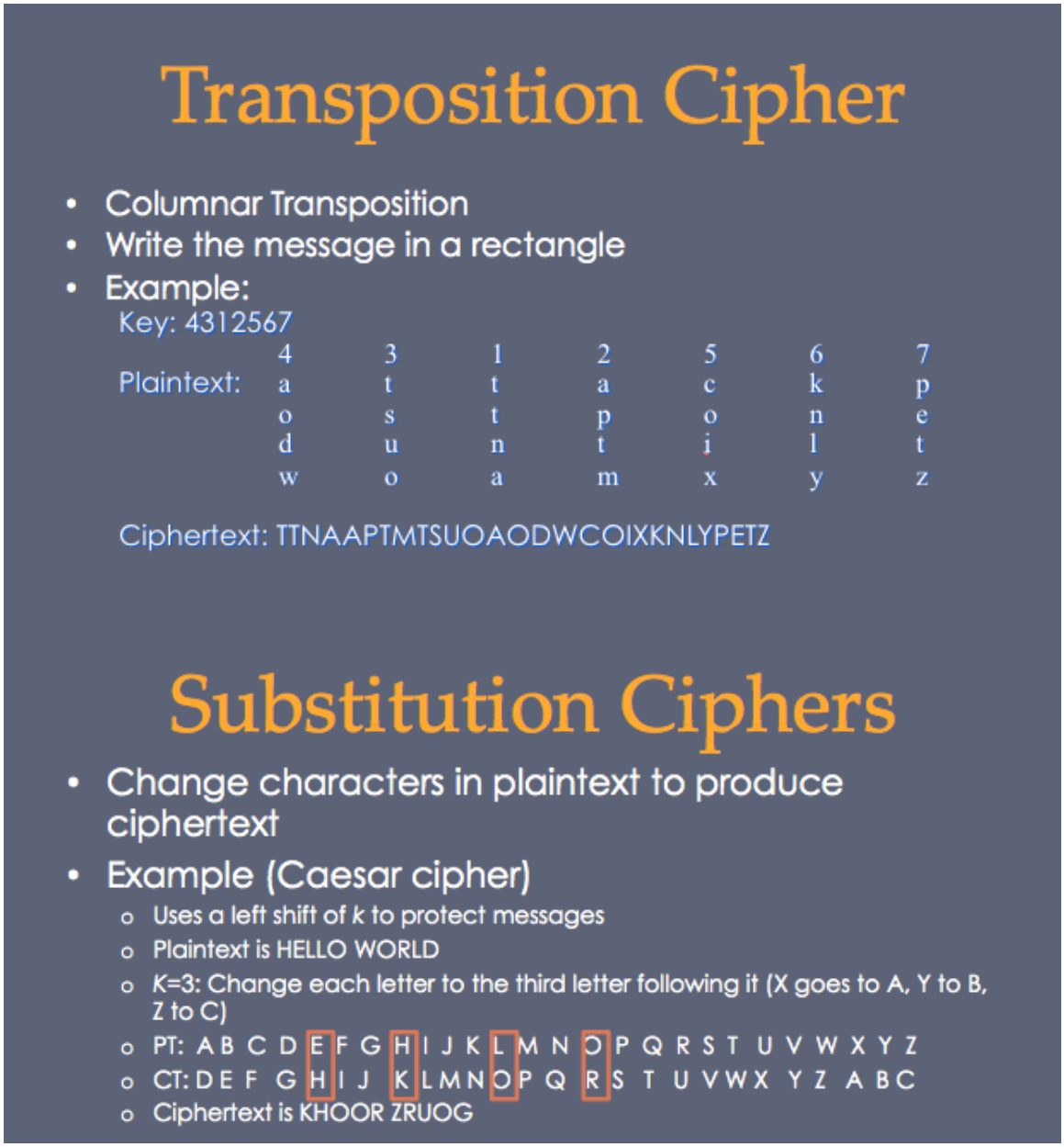
# HW 1

NAME: Jerome Thompson

Instructions:
- Work on your own.
- You may write code to do some of the work. Do not submit your code.




We talked in class briefly about transposition and substitution operations used by symmetric key encryption algorithms. A transposition cipher is one that uses the

transposition operation only. A substitution cipher is one that uses the substitution operation only. A product cipher is one that uses both.

**Q1 (6pts) Transposition Ciphers**

a) (2pt) Encrypt the following plaintext using the Columnar transposition cipher. Use the key: 10243 (key size is 5):

theshadowofthemoonsweptacrosstheglobefromhongkongtothetexaspanhandleasarareannu
larsolareclipsebeganmondaymorninginasiaandtraversedthepacificthesunappearedasathinri
ngbehindthemoontopeopleinanarrowpathalongthecenterofthetrackwhichbeganinsouthernc
hinaheavycloudsobscuredtheviewinhongkongbutresidentsoftokyoandothercitieswereablet
ogetaspectacularviewforaboutfourminutesaroundseventhirtytwoammondaysixthirtytwop
metsundayeventswereheldatschoolsandmuseumsinjapanwhilemanymorepeopletookintheu
nusualastronomicaleventathomeoronstreetcornersafterwhizzingacrossthepacifictheshado
wemergedovernortherncaliforniaandsouthernoregonwherethousandsofpeopleattendedparti
estowatchtheeventthefirsttoappearintheunitedstatessincenineteenninetyfourexpertswarned
thathopefulviewersshouldnotpeerupattheskywithoutspecialviewingequipmentsincelookin
gatthesunwiththenakedeyecancauseblindnessderekralstonaprofessionalphotographersaidh
eusedaweldingfiltertocaptureadirectviewofeclipseinthefoothillsaboveorovillecaliforniahes
haredthephotooncnnireportnotingtheratherslimswathoftheglobewhocouldseetheimpactoft
heeclipseralstonsaidhewantedtoenabletherestoftheworldtoseehowclearitlookedtothoseofus
whowerefortunateenoughtoseeitthesliverofsunshinethentraveledsoutheastacrosscentralnev
adasouthernutahandnorthernarizonaandthennewmexicoitpassedoveralbuquerquenewmexi
coaboutseventhirtyfourpmninethirtyfourpmetbeforepeteringouteastoflubbocktexasaccordi
ngtonasa

ciphertext:
hdtopoeehotxnlrnrrpgnogitrhihararetoeiraoeehccaornvusdihotdoyocsaosarfouurstymatym
nvweslmmaharpohssoltmnenfhnoefeorvrnfaorgeodeadrtcetrareetnnntrrrhpvrutuhwucigpsl
nhwhecuisespsatpauwntcrrieshtseiareepoirieemheeoeiteplseentshleciktoheueheeeunneoar
eldtuntanteipdaueeastypetrberutbtadotafoerhbmkoeadaaaaieomnsdetctnasnbdopeaplhttaig
seiaobevnkuiskdreetatawbonadntadxtpueshtodujwmoootuananooerawirhihdeooriiseehhnp
enastetioahtaiieeueatoleoortyoevniteitntkealerlaenoaseailouivfptolvvcohreonothhithbcsec
hianhteeetrswrooewrtegehvsievseccaaunarnodnxterqumotntrnrutreosuksrtaeohntsgfonhah
eansesadriarsefepetihhnonrtncrekhnunaydcteonrefotiwbgpcvourtoehtmyhtedeelcsuspinel
keutmeaestetigspiswgetcoaunorusotetohvhspiudecenyetnaeislppeitieemiogeiedasnsktrslo
hisegeaeeeceehaollnsdhnrtnrrsogwuemoessawdahtedeltehfofnntisrnetlusonnahtdhrahwca
olenxbehfmtypepitobecinhomwctoogttpnselllbmyianvdacueaignmolnwatnfrhenhheloreig
bstoneiretcleafisneronirosyteaonennemetnnlocehrrosrzctctamdnelndhrwtaflepeahnftetitsn
enopwdhuwhnetkhpliuncktuhaycbneanfohrrhddittdtoinolooefaahtnpottlatoodhatlrodnolrf
oooaotssertustifhhadhasrvorhorznneiseuqwcueruiioeotgalcaogsswesaslrngesaaruocenann
aaepispdhnietpaohgeotwbitchcsuhwngentahteleeuirtmeuviwosiwtanrdhasialypeiuarivtotcr
ezasacheerharntonesoptdiwteetpnnssetifxsetfesdeastsawqenoastneneddrooipgedelfrpacwli

fibrliihtocengaswflhltpfcetiatbeowtheldouwoaootlostrettsteseaneiaemosvbreiovionhfmfen efoxcna

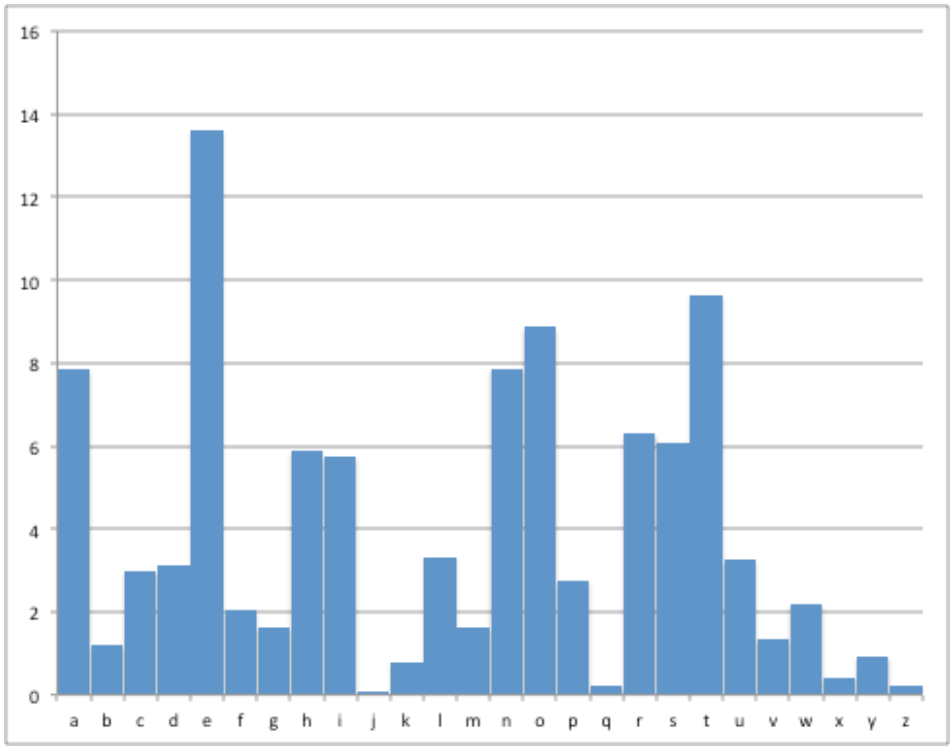
b) (2pt) How many possible keys can you use to encrypt this message using this cipher? What does that say about the susceptibility of the message to brute force attacks?

Since there are 10 (0-9) unique digits with 10 distinct possibilities at each position, we have 10^10 possible keys.

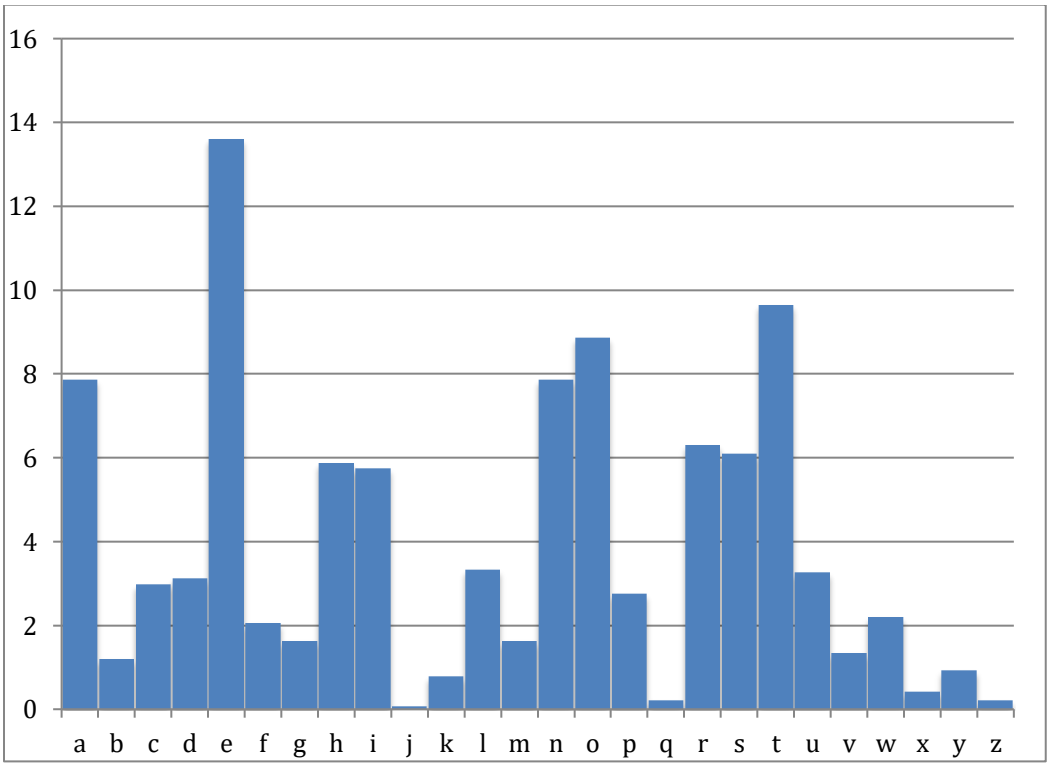
| Key Size | Cipher | Number of Alternative Keys | Time Required at 10^9 decryptions/s | Time Required at 10^13 decryptions/s |
|---|---|---|---|---|
| 56 | DES | 2^56 ≈ 7.2 × 1016 | 2^55 ns = 1.125 years | 1 hour |
| 128 | AES | 2^128 ≈ 3.4 · 10^38 | 2^127 ns = 5.3 · 1021 years | 5.3 × 1017 years |
| 168 | 3DES | 2^168 ≈ 3.7 · 10^50 | 2^167 ns = 5.8 · 1033 years | 5.8 · 1029 years |
| 192 | AES | 2^192 ≈ 6.3 × 10^57 | 2^191 ns = 9.8 × 1040 years | 9.8 · 1036 years |
| 256 | AES | 2^256 ≈ 1.2 × 1077 | 2^255 ns = 1.8 × 1060 years | 1.8 · 1056 years |
| 10 | OURS | 10^10 | 5^10ns = 9.77 milliseconds | 0.977 microseconds |

It very suspectable to brute force attacks that can be completed in mere seconds (as seen by trying ½ the key space to find solution).

c) (2pt) Calculate and plot the letter frequencies of the ciphertext (use the spreadsheet provided) and compare it to that of the English letters shown below. What is the relationship between both?




Source: https://en.wikipedia.org/wiki/Letter_frequency




Transposition cipher was used and so the letter frequencies are the same (as they were not substituted or altered just moved/transposed).

**Q2 (6pts) Substitution Ciphers**

a) (2pt) Encrypt the following plaintext using the Caesar substitution cipher. Use the key 10:

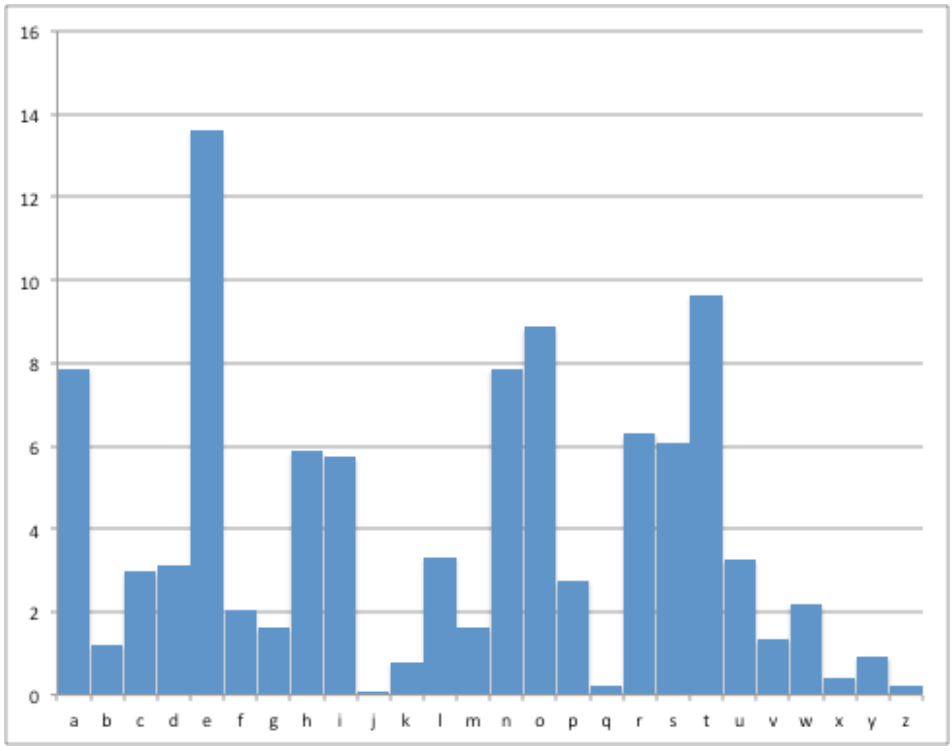
theshadowofthemoonsweptacrosstheglobefromhongkongtothetexaspanhandleasarareannu
larsolareclipsebeganmondaymorninginasiaandtraversedthepacificthesunappearedasathinri
ngbehindthemoontopeopleinanarrowpathalongthecenterofthetrackwhichbeganinsouthernc
hinaheavycloudsobscuredtheviewinhongkongbutresidentsoftokyoandothercitieswereablet
ogetaspectacularviewforaboutfourminutesaroundseventhirtytwoammondaysixthirtytwop
metsundayeventswereheldatschoolsandmuseumsinjapanwhilemanymorepeopletookintheu
nusualastronomicaleventathomeoronstreetcornersafterwhizzingacrossthepacifictheshado
wemergedovernortherncaliforniaandsouthernoregonwherethousandsofpeopleattendedparti
estowatchtheeventthefirsttoappearintheunitedstatessincenineteenninetyfourexpertswarned
thathopefulviewersshouldnotpeerupattheskywithoutspecialviewingequipmentsincelookin
gatthesunwiththenakedeyecancauseblindnessderekralstonaprofessionalphotographersaidh
eusedaweldingfiltertocaptureadirectviewofeclipseinthefoothillsaboveorovillecaliforniahes
haredthephotooncnnireportnotingtherathersimswathoftheglobewhocouldseetheimpactoft
heeclipseralstonsaidhewantedtoenabletherestoftheworldtoseehowclearitlookedtothoseofus
whowerefortunateenoughtoseeitthesliverofsunshinethentraveledsoutheastacrosscentralnev
adasouthernutahandnorthernarizonaandthennewmexicoitpassedoveralbuquerquenewmexi
coaboutseventhirtyfourpmninethirtyfourpmetbeforepeteringouteastoflubbocktexasaccordi
ngtonasa

ciphertext:
drocrknygypdrowyyxcgozdkmbyccdroqvylopbywryxquyxqdydrodohkczkxrkxnvokckbkb
okxxevkbcyvkbomvszcoloqkxwyxnkiwybxsxqsxkcskkxndbkfobcondrozkmspsmdrocexk
zzokbonkckdrsxbsxqlorsxndrowyyxdyzoyzvosxkxkbbygzkdrkvyxqdromoxdobypdrodbk
mugrsmrloqkxsxcyedrobxmrsxkrokfimvyencylcmebondrofsogsxryxquyxqledbocsnoxdcy
pdyuiykxnydrobmsdsocgoboklvodyqodkczomdkmevkbfsogpybklyedpyebwsxedockbyex
ncofoxdrsbdidgykwwyxnkicshdrsbdidgyzwodcexnkiofoxdcgoborovnkdcmryyvckxnweco
ewcsxtkzkxgrsvowkxiwybozoyzvodyyusxdroexecekvkcdbyxywsmkvofoxdkdrywoybyxc
dboodmybxobckpdobgrsjjsxqkmbyccdrozkmspsmdrocrknygowobqonyfobxybdrobxmkvs
pybxskkxncyedrobxyboqyxgrobodryeckxncypzoyzvokddoxnonzkbdsocdygkdmrdroofox
ddropsbcddykzzokbsxdroexsdoncdkdoccsxmoxsxodooxxsxodipyebohzobdcgkbxondrkdr
yzopevfsogobccryevnxydzoobezkddrocuigsdryedczomskvfsogsxqoaeszwoxdcsxmovyyus
xqkddrocexgsdrdroxkuonoiomkxmkecolvsxnxoccnoboubkvcdyxkzbypoccsyxkvzrydyqbk
zrobcksnroeconkgovnsxqpsvdobdymkzdeboknsbomdfsogypomvszcosxdropyydrsvvcklyf
oybyfsvvomkvspybxskrocrkbondrozrydyyxmxxsbozybdxydsxqdrobkdrobcvswcgkdrypdr
oqvylogrymyevncoodroswzkmdypdroomvszcobkvcdyxcksnrogkxdondyoxklvodrobocdyp
drogybvndycoorygmvokbsdvyyuondydrycoypecgrygobopybdexkdooxyeqrdycoosddrocvs
fobypcexcrsxodroxdbkfovoncyedrokcdkmbyccmoxdbkvxofknkcyedrobxedkrkxnxybdrob
xkbsjyxkkxndroxxogwohsmysdzkcconyfobkvleaeobaeoxogwohsmyklyedcofoxdrsbdipye
bzwxsxodrsbdipyebzwodlopybozodobsxqyedokcdypvellymudohkckmmybnsxqdyxkck

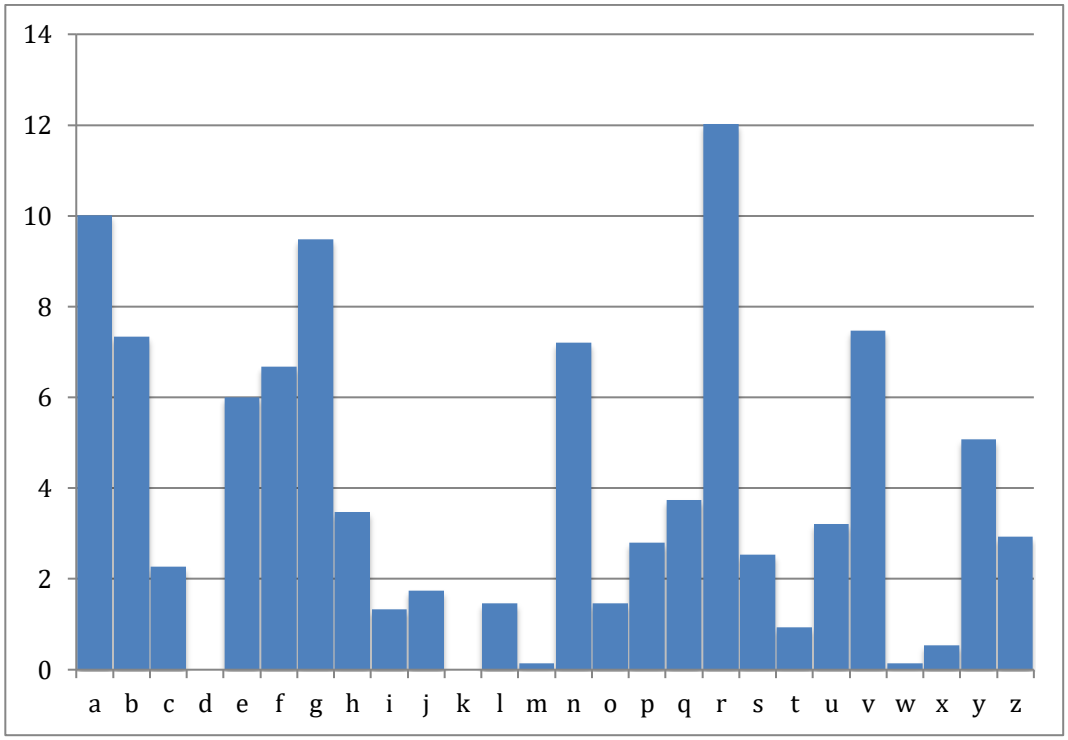
b) (2pt) How many possible keys can you use to encrypt this message using this cipher? What does that say about the susceptibility of the message to brute force attacks?

25 keys can be used to give unique outputs.
If the language along with the statically frequency inference is known, Caesar can be easily broken even if the key space is large (key space is small though, which makes ciphertext even easier to crack).

c) (2pt) Calculate and plot the letter frequencies of the ciphertext (use the spreadsheet provided) and compare it to that of the English letters shown below. What is the relationship between both?




Source: https://en.wikipedia.org/wiki/Letter_frequency




It can be seen that the second plot is shifted (by 10) from the first plot.

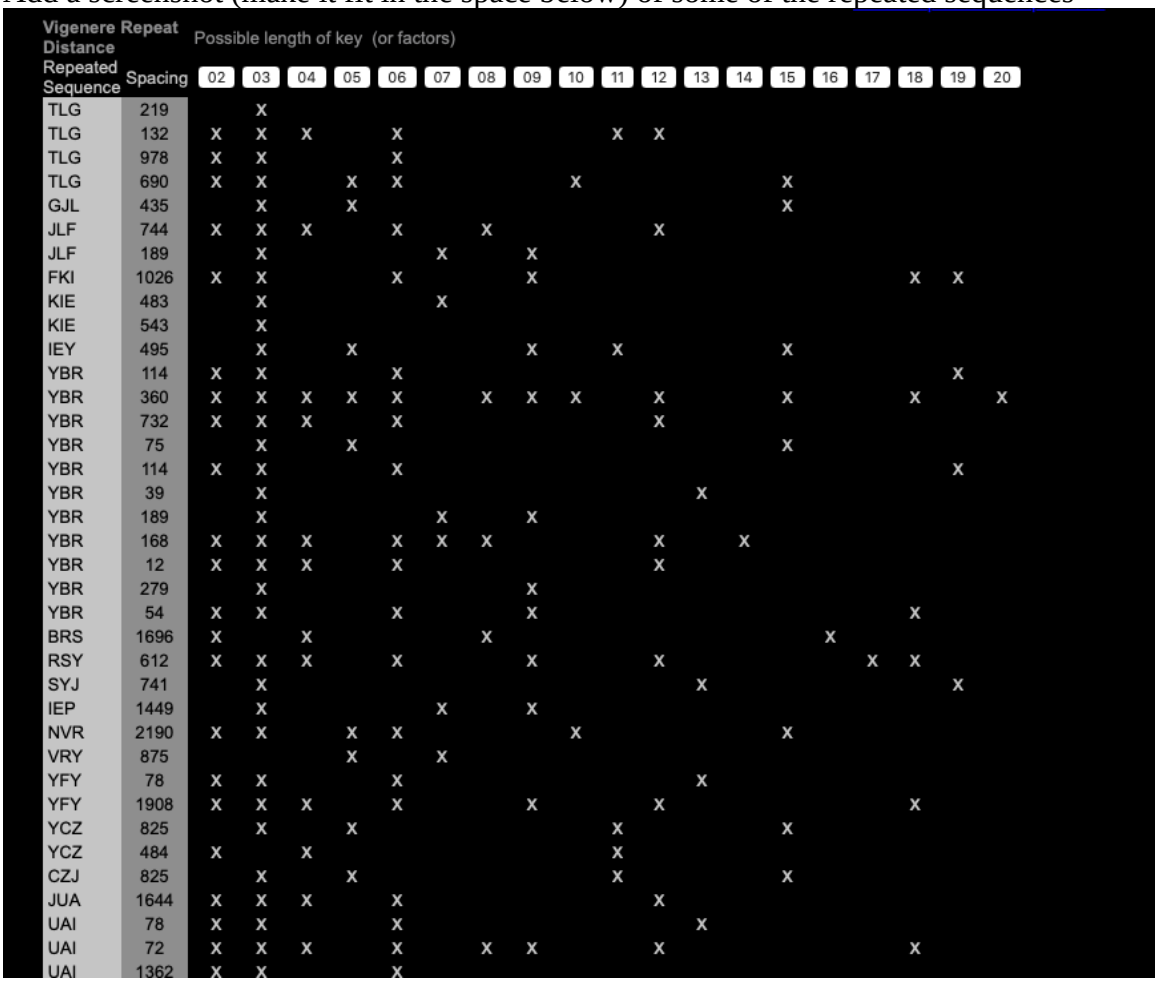
**Q3 (8pts) Vigenere Cryptanalysis**

The ciphertext is posted to the blackboard (same folder as the assignment) in a file called "ciphertext"

a) (2pts) Do a **repetition test on the cipher.** You can use this site:

http://www.simonsingh.net/The_Black_Chamber/vigenere_cracking_tool.html.

Add a screenshot (make it fit in the space below) of some of the repeated sequences



| Vigenere Repeat Distance | | Possible length of key (or factors) | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Repeated Sequence | Spacing | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| TLG | 219 | | X | | | | | | | | | | | | | | | | | |
| TLG | 132 | X | X | X | | X | | | | | X | X | | | | | | | | |
| TLG | 978 | X | X | | | X | | | | | | | | | | | | | | |
| TLG | 690 | X | X | | X | X | | | | X | | | | | X | | | | | |
| GJL | 435 | | X | | X | | | | | | | | | | X | | | | | |
| JLF | 744 | X | X | X | | X | | X | | | | X | | | | | | | | |
| JLF | 189 | | X | | | | X | | X | | | | | | | | | | | |
| FKI | 1026 | X | X | | | X | | | X | | | | | | | | | X | X | |
| KIE | 483 | | X | | | | X | | | | | | | | | | | | | |
| KIE | 543 | | X | | | | | | | | | | | | | | | | | |
| IEY | 495 | | X | | X | | | | X | | X | | | | X | | | | | |
| YBR | 114 | X | X | | | X | | | | | | | | | | | | | X | |
| YBR | 360 | X | X | X | X | X | | X | X | X | | X | | | X | | | X | | X |
| YBR | 732 | X | X | X | | X | | | | | | X | | | | | | | | |
| YBR | 75 | | X | | X | | | | | | | | | | X | | | | | |
| YBR | 114 | X | X | | | X | | | | | | | | | | | | | X | |
| YBR | 39 | | X | | | | | | | | | | X | | | | | | | |
| YBR | 189 | | X | | | | X | | X | | | | | | | | | | | |
| YBR | 168 | X | X | X | | X | X | X | | | | X | | X | | | | | | |
| YBR | 12 | X | X | X | | X | | | | | | X | | | | | | | | |
| YBR | 279 | | X | | | | | | X | | | | | | | | | | | |
| YBR | 54 | X | X | | | X | | | X | | | | | | | | | X | | |
| BRS | 1696 | X | | X | | | | X | | | | | | | | X | | | | |
| RSY | 612 | X | X | X | | X | | | X | | | X | | | | | X | X | | |
| SYJ | 741 | | X | | | | | | | | | | X | | | | | | X | |
| IEP | 1449 | | X | | | | X | | X | | | | | | | | | | | |
| NVR | 2190 | X | X | | X | X | | | | X | | | | | X | | | | | |
| VRY | 875 | | | | X | | X | | | | | | | | | | | | | |
| YFY | 78 | X | X | | | X | | | | | | | X | | | | | | | |
| YFY | 1908 | X | X | X | | X | | | X | | | X | | | | | | X | | |
| YCZ | 825 | | X | | X | | | | | | X | | | | X | | | | | |
| YCZ | 484 | X | | X | | | | | | | X | | | | | | | | | |
| CZJ | 825 | | X | | X | | | | | | X | | | | X | | | | | |
| JUA | 1644 | X | X | X | | X | | | | | | X | | | | | | | | |
| UAI | 78 | X | X | | | X | | | | | | | X | | | | | | | |
| UAI | 72 | X | X | X | | X | | X | X | | | X | | | | | | X | | |
| UAI | 1362 | X | X | | | X | | | | | | | | | | | | | | |

Based on the test, what do you think the key size is? 3

b) (2pts) Break the ciphertext into sets, where each set corresponds to the letters shifted by a given key. List the sets below

Set1:
wtjkysdpryjimuqftwzynzfaktjjlylyshwyxithxqyrxtqlqgnitwttyyxhiisihrfffsdwsttmwxw
wxhyxusnzxyyssfnnewjqsfwwwjhngfffsdwffttmurlrdjyablftjkwjjnxwskfnifjjfryiysfjrq

fbisywkrnfuytmiiwdxiffmjjyjgyzdldxajrjghkrswrghnxnfsjjhytxqsjjfnjjfjwstsnnhuxjgx
sfllywyxtfjujfsxfjhqjtssfbmjwnfgjhhqhyuttdtmjtyjxfssfyqtjxisfxyjmcfifqzjkuijhyifxdz
thntsdxqjxsttjmnxfzsipiwkurjfwxwyfuijsqfqfjftsqsniftnfjffafzonnrfsxkeqfxjaryylzmljf
jwyxdhwjiqjtxstjnxtftqabqjtyuujtwkplxqlitmzttwngfqxyqfzhygyfkntjsywiybqjsijjbmy
gswxsrbpfxulxjnstrsnfhufgtgstmnxiwyfcjfbmlsxitjtxfmfwjtjnjwwtjyqnzztynbjwhwjdj
xftryftqtrszsxnwjhjjwjsjntyswntnmjwjtryfynfsyuqiftwjyxfbmtwmyjwsjjxttfjstwjfsjwts
rsjfifxhjxawjjjtfenxybjstnzyhyyqtmychjijbxxfxtfxinfdyxxsywjjizsbfayfjsiaffyntftwlyn
yxnjnznfzmyqnrjxxfqbwyhjl

Set2:
yllibyinycuiyocnhymimmqymlmhlcgcjnyuujxyuibvyhfusnhjjnzhbqbeuzwvlcfjlnqeall
eygxixnibmswlyyugnmwgyyhsudwjumonlwjlncyfnhlywcwyncycxcfjmoyuxfjmuchuu
ihlcycolivmummimxbciuiliyholnuniucfuvhihizlaunbyyujfmuumyjfuiqwlylnyuowxam
mvmxxilwyoumwlfujfbagcxuibnpmqulhywhfunmfmsncauymhufiyyiynlfqxyqlcmmla
wluyghgyycvqhyniclswmololilchimxwblgujwnqbahmgutnnxbocqxilchwyxyihlolacdc
mfmlcwwpjhvfwingclhiygutyulynmnmyiilymcmflxibibecfycxljxkmizgnhlcicuobllnzu
cccnyimlylmzchlnyucyvnofonnchfxsbcolixwmyxfccbixciiuijwhcuiwhawgnwycfhleuy
zygupcsfmxhucnjnclmhnnyjxmnlnjnmvubuhlcziyypyiuuinnfwymnhyhsxmyynaabclc
mugfhcuyyhhipqhwymeblsnbociclyhiqlccocnijnnguzgghmxphhawmynwgilhyxmbub
yyhxqlhuiqbclazlguybwflyiycdahymmwyzwccxfcbcnwbyuiignuhynngxwyahbhlnhibi
abmlxmmivniiynuconnmuuyily

Set3
**cgferjevfzageopvfsrqpfnbgvqvnabbvhfeaeheysrnqvrybnrerlflnnnrarrlvafcrybvs
agbnhrhvnevbcgraevrjigvqpgvzbbbgrelrucryagvvsghbabquaervgpvbayfszrbyap
ygaggaaaflgyrvcfenbraegareqrarrorsgayirfynhbgvornoaqhvbevgnhvgauurievao
gbvyfgyuzvinnweygfhrehvvqnanszverafcfqjuafyugrbqngegyuqelanqazsuybgalxz
vuvhuvopzgnvzyrrgreeavfpfybpfghaqagvbnjnznnunvgcgcfruevnaabfebaggfvpeq
bpnrabrjysnybrryghqycebrbqygrtvfzvyrrurafhnbgajraszransmypagrbghgaeavn
rraaogrbvlgspaababsgccrjgtrufepfbfgrguvgiinbraflhobvejygarhnrseyeyrvayqyv
gbrzuyrlqbfefggranrfrgznfabbrgecqugcrbaczebrgexrjcfgfefarahtaabrqhaavnpb
novfqbefaqjgvangnbyijyrjruqhazrrjvbropzanfghrrgaetfebbuyxepcvntrzgrvnahb
bizlprhyxncfgaftvgavnqnrppfafnnsgzrefhzgnrrugsgaihyavanrryfsprffrauqnrber
qrszvohgyungeqpfabnfstvgfrunbeaqin**

c) (2pts**)** Find **the letter that has the highest frequency in each set (you can use the spreadsheet provided) and use it to guess the key.**

| Sets | Letter with highest freq. | Assuming this letter is “e” then the key to decrypt this set is |
|---|---|---|
| set 1 | j | 5 (f) |
| set 2 | y | 20 (u) |
| set3 | r | 13 (n) |
| | | |
| | | |

| | | |
|---|---|---|
| | | |

Key: fun

d) (2) What is the plaintext?

**reportersforthenewyorktimestimeandotherpublicationsrefusetodiscussawaveofstories denigratingmotionpicturestarsandproducersallofthembasedonillegallyobtainedpro pertyofsonythatwashackedandfencedbycriminalsapparentlyworkingfornorthkoreas murderousdictatorshipsonypicturesentertainmentwasvictimizedrecentlyinamajorco rporatesecuritybreachapparentlyinretaliationfortheupcomingcomedytheinterviewdi gitalcopiesofunreleasedfilmspersonalfinancialdataonentertainmentindustrynotables emailspasswordsandotherinformationareportedonehundredterabytesofdatainallhav ebeenstolenaboutfourtygigabyteshavebeenmadepublicsofarmainstreampublications whichareneverreticentaboutscoldinglessestablishedmediaoverarcanejournalisticscru plesarepublishingdamagingdatafromthistroveasnewspapersandnewschannelscallthe stolensonydatawithgreatrelishandbarelyconcealedcontemptforhollywoodthenewyor ktimesissharinguncharitablecommentsmadeinemailsbetweentheextraordinarilysucc essfulproducerscottrudinandsonystudiocochairwomanamypascalthewashingtonpost emphasizesthatrudinhadunkindwordsforprominentactressdirectorandproducerange linajolieaswellasforanillconceivedplantobuildacleopatramoviearoundjolietimemagaz inessamfrizellteasesthesevenmostoutrageousthingswelearnedfromthesonyhackfrizell declinedtorespondtoquestionsfromnationalreviewonlineabouttheproprietyoftraffickin nginstolengoodsforthepurposeofwritingbreathlessarticlesaboutscuttlebuttthatifitinv olvedanyotherindustrywouldbeconsideredwellwithintheboundariesofnormalworkpl acesnipingalsodeclinedtocommentmichaelcieplyandbrooksbarnesofthetimesandvari etysalexstedmanawashingtonposteditorrespondsthatthepaperdoesnotpermitreporter stobreakthelawinpursuitofstorieswenevercourageanyonetostealdocumentsnational economyandbusinesseditorgregschneiderwritesinanemailtonationalreviewonlinehow everwhendocumentsmaketheirwayintothepublicdomainoraresenttouswearewithinou rrightstoreportonthemleaksfromcompaniesandgovernmentagenciesarenotuncommo novermanydecadessuchleakshavepresentednewsorganizationswithawiderangeofcirc umstancesthatcallforthemtoexercisejudgmentweassesseachsetoffactsindividuallyinth isinstancethereleaseofdocumentswasaneventthatdemandedcoverageandtheinformati onbroughttolighthasstirreddiscussionaboutahostoflegitimateissuesthatalsowarrante dcoverage**