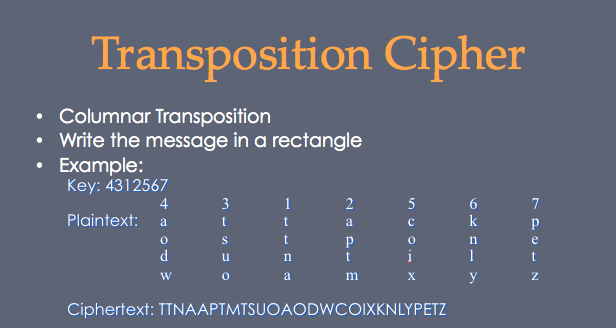
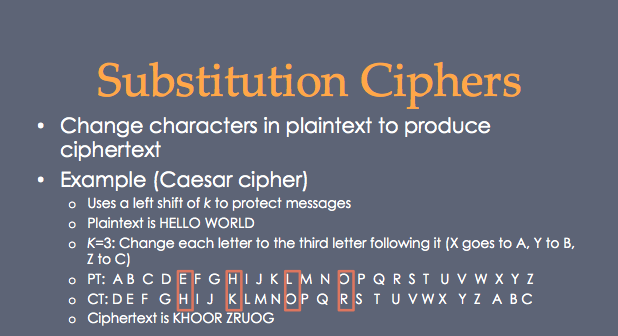
HW 1

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):

theshadowofthemoonsweptacrosstheglobefromhongkongtothetexaspanhandleasarareannularsolareclipsebeganmondaymorninginasiaandtraversedthepacificthesunappearedasathinringbehindthemoontopeopleinanarrowpathalongthecenterofthetrackwhichbeganinsouthernchinaheavycloudsobscuredtheviewinhongkongbutresidentsoftokyoandothercitieswereabletogetaspectacularviewforaboutfourminutesaroundseventhirtytwoammondaysixthirtytwopmetsundayeventswereheldatschoolsandmuseumsinjapanwhilemanymorepeopletookintheunusualastronomicaleventathomeoronstreetcornersafterwhizzingacrossthepacifictheshadowemergedovernortherncaliforniaandsouthernoregonwherethousandsofpeopleattendedpartiestowatchtheeventthefirsttoappearintheunitedstatessincenineteenninetyfourexpertswarnedthathopefulviewersshouldnotpeerupattheskywithoutspecialviewingequipmentsincelookingatthesunwiththenakedeyecancauseblindnessderekralstonaprofessionalphotographersaidheusedaweldingfiltertocaptureadirectviewofeclipseinthefoothillsaboveorovillecaliforniahesharedthephotooncnnireportnotingtheratherslimswathoftheglobewhocouldseetheimpactoftheeclipseralstonsaidhewantedtoenabletherestoftheworldtoseehowclearitlookedtothoseofuswhowerefortunateenoughtoseeitthesliverofsunshinethentraveledsoutheastacrosscentralnevadasouthernutahandnorthernarizonaandthennewmexicoitpassedoveralbuquerquenewmexicoaboutseventhirtyfourpmninethirtyfourpmetbeforepeteringouteastoflubbocktexasaccordingtonasa

ciphertext:

hdtopoeehotxnlrnrrpgnogitrhihararetoeiraoeehccaornvusdihotdoyocsaosarfouurstymatymnvweslmmaharpohssoltmnenfhnoefeorvrnfaorgeodeadrtcetrareetnnntrrrhpvrutuhwucigpslnhwhecuisespsatpauwntcrrieshtseiareepoirieemheeoeiteplseentshleciktoheueheeeunneoareldtuntanteipdaueeastypetrberutbtadotafoerhbmkoeadaaaaieomnsdetctnasnbdopeaplhttaigseiaobevnkuiskdreetatawbonadntadxtpueshtodujwmoootuananooerawirhihdeooriiseehhnpenastetioahtaiieeueatoleoortyoevniteitntkealerlaenoaseailouivfptolvvcohreonothhithbcsechianhteeetrswrooewrtegehvsievseccaaunarnodnxterqumotntrnrutreosuksrtaeohntsgfonhaheansesadriarsefepetihhnonrtncrekhnunaydcteonrefotiwbgpcvourtoehtmyhtedeelcsuspinelkeutmeaestetigspiswgetcoaunorusotetohvhspiudecenyetnaeislppeitieemiogeiedasnsktrslohisegeaeeeceehaollnsdhnrtnrrsogwuemoessawdahtedeltehfofnntisrnetlusonnahtdhrahwcaolenxbehfmtypepitobecinhomwctoogttpnselllbmyianvdacueaignmolnwatnfrhenhheloreigbstoneiretcleafisneronirosyteaonennemetnnlocehrrosrzctctamdnelndhrwtaflepeahnftetitsnenopwdhuwhnetkhpliuncktuhaycbneanfohrrhddittdtoinolooefaahtnpottlatoodhatlrodnolrfoooaotssertustifhhadhasrvorhorznneiseuqwcueruiioeotgalcaogsswesaslrngesaaruocenannaaepispdhnietpaohgeotwbitchcsuhwngentahteleeuirtmeuviwosiwtanrdhasialypeiuarivtotcrezasacheerharntonesoptdiwteetpnnssetifxsetfesdeastsawqenoastneneddrooipgedelfrpacwlifibrliihtocengaswflhltpfcetiatbeowtheldouwoaootlostrettsteseaneiaemosvbreiovionhfmfenefoxcna

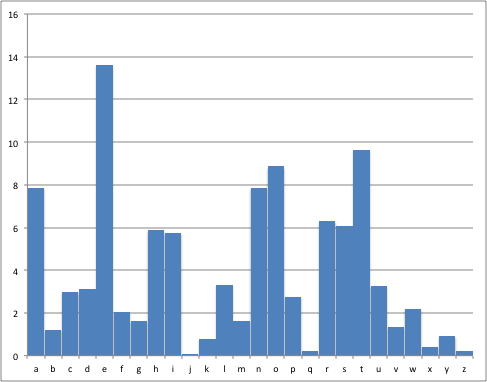
b) (2pt) How many possible keys can you use to encrypt this message using this cipher? What does that say about the susceptibility of the message to brute force attacks?

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:

theshadowofthemoonsweptacrosstheglobefromhongkongtothetexaspanhandleasarareannularsolareclipsebeganmondaymorninginasiaandtraversedthepacificthesunappearedasathinringbehindthemoontopeopleinanarrowpathalongthecenterofthetrackwhichbeganinsouthernchinaheavycloudsobscuredtheviewinhongkongbutresidentsoftokyoandothercitieswereabletogetaspectacularviewforaboutfourminutesaroundseventhirtytwoammondaysixthirtytwopmetsundayeventswereheldatschoolsandmuseumsinjapanwhilemanymorepeopletookintheunusualastronomicaleventathomeoronstreetcornersafterwhizzingacrossthepacifictheshadowemergedovernortherncaliforniaandsouthernoregonwherethousandsofpeopleattendedpartiestowatchtheeventthefirsttoappearintheunitedstatessincenineteenninetyfourexpertswarnedthathopefulviewersshouldnotpeerupattheskywithoutspecialviewingequipmentsincelookingatthesunwiththenakedeyecancauseblindnessderekralstonaprofessionalphotographersaidheusedaweldingfiltertocaptureadirectviewofeclipseinthefoothillsaboveorovillecaliforniahesharedthephotooncnnireportnotingtheratherslimswathoftheglobewhocouldseetheimpactoftheeclipseralstonsaidhewantedtoenabletherestoftheworldtoseehowclearitlookedtothoseofuswhowerefortunateenoughtoseeitthesliverofsunshinethentraveledsoutheastacrosscentralnevadasouthernutahandnorthernarizonaandthennewmexicoitpassedoveralbuquerquenewmexicoaboutseventhirtyfourpmninethirtyfourpmetbeforepeteringouteastoflubbocktexasaccordingtonasa

ciphertext:

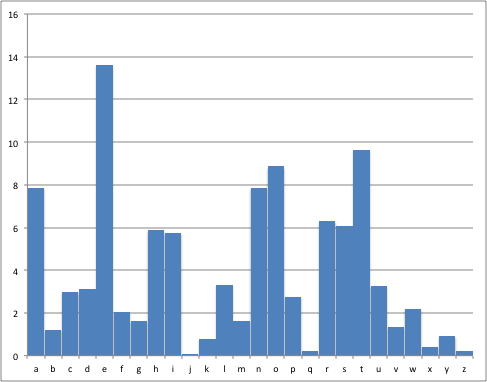
drocrknygypdrowyyxcgozdkmbyccdroqvylopbywryxquyxqdydrodohkczkxrkxnvokckbkbokxxevkbcyvkbomvszcoloqkxwyxnkiwybxsxqsxkcskkxndbkfobcondrozkmspsmdrocexkzzokbonkckdrsxbsxqlorsxndrowyyxdyzoyzvosxkxkbbygzkdrkvyxqdromoxdobypdrodbkmugrsmrloqkxsxcyedrobxmrsxkrokfimvyencylcmebondrofsogsxryxquyxqledbocsnoxdcypdyuiykxnydrobmsdsocgoboklvodyqodkczomdkmevkbfsogpybklyedpyebwsxedockbyexncofoxdrsbdidgykwwyxnkicshdrsbdidgyzwodcexnkiofoxdcgoborovnkdcmryyvckxnwecoewcsxtkzkxgrsvowkxiwybozoyzvodyyusxdroexecekvkcdbyxywsmkvofoxdkdrywoybyxcdboodmybxobckpdobgrsjjsxqkmbyccdrozkmspsmdrocrknygowobqonyfobxybdrobxmkvspybxskkxncyedrobxyboqyxgrobodryeckxncypzoyzvokddoxnonzkbdsocdygkdmrdroofoxddropsbcddykzzokbsxdroexsdoncdkdoccsxmoxsxodooxxsxodipyebohzobdcgkbxondrkdryzopevfsogobccryevnxydzoobezkddrocuigsdryedczomskvfsogsxqoaeszwoxdcsxmovyyusxqkddrocexgsdrdroxkuonoiomkxmkecolvsxnxoccnoboubkvcdyxkzbypoccsyxkvzrydyqbkzrobcksnroeconkgovnsxqpsvdobdymkzdeboknsbomdfsogypomvszcosxdropyydrsvvcklyfoybyfsvvomkvspybxskrocrkbondrozrydyyxmxxsbozybdxydsxqdrobkdrobcvswcgkdrypdroqvylogrymyevncoodroswzkmdypdroomvszcobkvcdyxcksnrogkxdondyoxklvodrobocdypdrogybvndycoorygmvokbsdvyyuondydrycoypecgrygobopybdexkdooxyeqrdycoosddrocvsfobypcexcrsxodroxdbkfovoncyedrokcdkmbyccmoxdbkvxofknkcyedrobxedkrkxnxybdrobxkbsjyxkkxndroxxogwohsmysdzkcconyfobkvleaeobaeoxogwohsmyklyedcofoxdrsbdipyebzwxsxodrsbdipyebzwodlopybozodobsxqyedokcdypvellymudohkckmmybnsxqdyxkck

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”

1. (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

A screenshot of a computer

Description automatically generated

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

1. (2pts) Break the ciphertext into sets, where each set corresponds to the letters shifted by a given key. List the sets below

Set1:

wtjkysdpryjimuqftwzynzfaktjjlylyshwyxithxqyrxtqlqgnitwttyyxhiisihrfffsdwsttmwxwwxhyxusnzxyyssfnnewjqsfwwwjhngfffsdwffttmurlrdjyablftjkwjjnxwskfnifjjfryiysfjrqfbisywkrnfuytmiiwdxiffmjjyjgyzdldxajrjghkrswrghnxnfsjjhytxqsjjfnjjfjwstsnnhuxjgxsfllywyxtfjujfsxfjhqjtssfbmjwnfgjhhqhyuttdtmjtyjxfssfyqtjxisfxyjmcfifqzjkuijhyifxdzthntsdxqjxsttjmnxfzsipiwkurjfwxwyfuijsqfqfjftsqsniftnfjffafzonnrfsxkeqfxjaryylzmljfjwyxdhwjiqjtxstjnxtftqabqjtyuujtwkplxqlitmzttwngfqxyqfzhygyfkntjsywiybqjsijjbmygswxsrbpfxulxjnstrsnfhufgtgstmnxiwyfcjfbmlsxitjtxfmfwjtjnjwwtjyqnzztynbjwhwjdjxftryftqtrszsxnwjhjjwjsjntyswntnmjwjtryfynfsyuqiftwjyxfbmtwmyjwsjjxttfjstwjfsjwtsrsjfifxhjxawjjjtfenxybjstnzyhyyqtmychjijbxxfxtfxinfdyxxsywjjizsbfayfjsiaffyntftwlynyxnjnznfzmyqnrjxxfqbwyhjl

Set2:

yllibyinycuiyocnhymimmqymlmhlcgcjnyuujxyuibvyhfusnhjjnzhbqbeuzwvlcfjlnqealleygxixnibmswlyyugnmwgyyhsudwjumonlwjlncyfnhlywcwyncycxcfjmoyuxfjmuchuuihlcycolivmummimxbciuiliyholnuniucfuvhihizlaunbyyujfmuumyjfuiqwlylnyuowxammvmxxilwyoumwlfujfbagcxuibnpmqulhywhfunmfmsncauymhufiyyiynlfqxyqlcmmlawluyghgyycvqhyniclswmololilchimxwblgujwnqbahmgutnnxbocqxilchwyxyihlolacdcmfmlcwwpjhvfwingclhiygutyulynmnmyiilymcmflxibibecfycxljxkmizgnhlcicuobllnzucccnyimlylmzchlnyucyvnofonnchfxsbcolixwmyxfccbixciiuijwhcuiwhawgnwycfhleuyzygupcsfmxhucnjnclmhnnyjxmnlnjnmvubuhlcziyypyiuuinnfwymnhyhsxmyynaabclcmugfhcuyyhhipqhwymeblsnbociclyhiqlccocnijnnguzgghmxphhawmynwgilhyxmbubyyhxqlhuiqbclazlguybwflyiycdahymmwyzwccxfcbcnwbyuiignuhynngxwyahbhlnhibiabmlxmmivniiynuconnmuuyily

Set3

**cgferjevfzageopvfsrqpfnbgvqvnabbvhfeaeheysrnqvrybnrerlflnnnrarrlvafcrybvsagbnhrhvnevbcgraevrjigvqpgvzbbbgrelrucryagvvsghbabquaervgpvbayfszrbyapygaggaaaflgyrvcfenbraegareqrarrorsgayirfynhbgvornoaqhvbevgnhvgauurievaogbvyfgyuzvinnweygfhrehvvqnanszverafcfqjuafyugrbqngegyuqelanqazsuybgalxzvuvhuvopzgnvzyrrgreeavfpfybpfghaqagvbnjnznnunvgcgcfruevnaabfebaggfvpeqbpnrabrjysnybrryghqycebrbqygrtvfzvyrrurafhnbgajraszransmypagrbghgaeavnrraaogrbvlgspaababsgccrjgtrufepfbfgrguvgiinbraflhobvejygarhnrseyeyrvayqyvgbrzuyrlqbfefggranrfrgznfabbrgecqugcrbaczebrgexrjcfgfefarahtaabrqhaavnpbnovfqbefaqjgvangnbyijyrjruqhazrrjvbropzanfghrrgaetfebbuyxepcvntrzgrvnahbbizlprhyxncfgaftvgavnqnrppfafnnsgzrefhzgnrrugsgaihyavanrryfsprffrauqnrberqrszvohgyungeqpfabnfstvgfrunbeaqin**

1. (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

1. (2) What is the plaintext?

**reportersforthenewyorktimestimeandotherpublicationsrefusetodiscussawaveofstoriesdenigratingmotionpicturestarsandproducersallofthembasedonillegallyobtainedpropertyofsonythatwashackedandfencedbycriminalsapparentlyworkingfornorthkoreasmurderousdictatorshipsonypicturesentertainmentwasvictimizedrecentlyinamajorcorporatesecuritybreachapparentlyinretaliationfortheupcomingcomedytheinterviewdigitalcopiesofunreleasedfilmspersonalfinancialdataonentertainmentindustrynotablesemailspasswordsandotherinformationareportedonehundredterabytesofdatainallhavebeenstolenaboutfourtygigabyteshavebeenmadepublicsofarmainstreampublicationswhichareneverreticentaboutscoldinglessestablishedmediaoverarcanejournalisticscruplesarepublishingdamagingdatafromthistroveasnewspapersandnewschannelscallthestolensonydatawithgreatrelishandbarelyconcealedcontemptforhollywoodthenewyorktimesissharinguncharitablecommentsmadeinemailsbetweentheextraordinarilysuccessfulproducerscottrudinandsonystudiocochairwomanamypascalthewashingtonpostemphasizesthatrudinhadunkindwordsforprominentactressdirectorandproducerangelinajolieaswellasforanillconceivedplantobuildacleopatramoviearoundjolietimemagazinessamfrizellteasesthesevenmostoutrageousthingswelearnedfromthesonyhackfrizelldeclinedtorespondtoquestionsfromnationalreviewonlineabouttheproprietyoftraffickinginstolengoodsforthepurposeofwritingbreathlessarticlesaboutscuttlebuttthatifitinvolvedanyotherindustrywouldbeconsideredwellwithintheboundariesofnormalworkplacesnipingalsodecliningtocommentmichaelcieplyandbrooksbarnesofthetimesandvarietysalexstedmanawashingtonposteditorrespondsthatthepaperdoesnotpermitreporterstobreakthelawinpursuitofstoriesweneverencourageanyonetostealdocumentsnationaleconomyandbusinesseditorgregschneiderwritesinanemailtonationalreviewonlinehoweverwhendocumentsmaketheirwayintothepublicdomainoraresenttouswearewithinourrightstoreportonthemleaksfromcompaniesandgovernmentagenciesarenotuncommonovermanydecadessuchleakshavepresentednewsorganizationswithawiderangeofcircumstancesthatcallforthemtoexercisejudgmentweassesseachsetoffactsindividuallyinthisinstancethereleaseofdocumentswasaneventthatdemandedcoverageandtheinformationbroughttolighthasstirreddiscussionaboutahostoflegitimateissuesthatalsowarrantedcoverage**