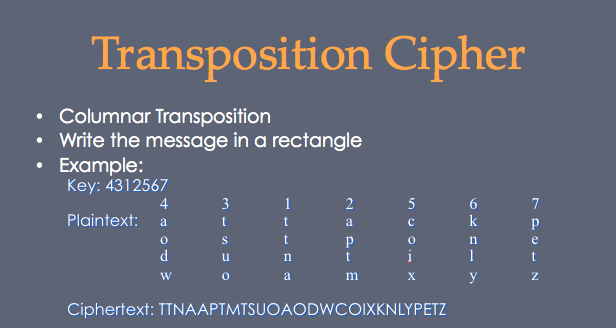
Assignment 1

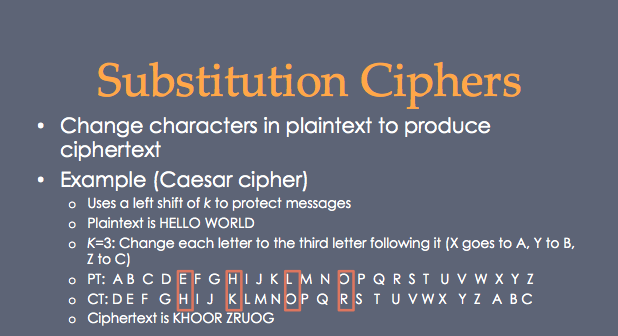
Submit through the blackboard before 12:00am 02/15/20

NAME: Gengda Li

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 (3pts) Transposition Ciphers**

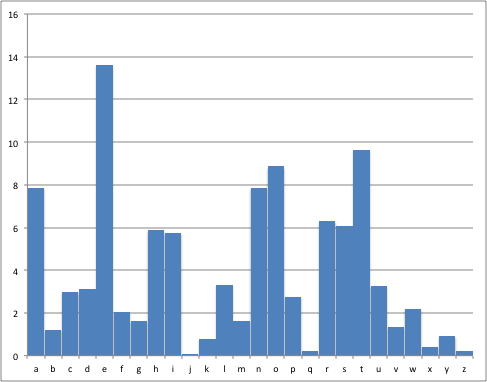
a) (1.5pt) Encrypt the following plaintext using the Columnar transposition cipher. Use the key: 13524 (key size is 5):

theshadowofthemoonsweptacrosstheglobefromhongkongtothetexaspanhandleasarareannularsolareclipsebeganmondaymorninginasiaandtraversedthepacificthesunappearedasathinringbehindthemoontopeopleinanarrowpathalongthecenterofthetrackwhichbeganinsouthernchinaheavycloudsobscuredtheviewinhongkongbutresidentsoftokyoandothercitieswereabletogetaspectacularviewforaboutfourminutesaroundseventhirtytwoammondaysixthirtytwopmetsundayeventswereheldatschoolsandmuseumsinjapanwhilemanymorepeopletookintheunusualastronomicaleventathomeoronstreetcornersafterwhizzingacrossthepacifictheshadowemergedovernortherncaliforniaandsouthernoregonwherethousandsofpeopleattendedpartiestowatchtheeventthefirsttoappearintheunitedstatessincenineteenninetyfourexpertswarnedthathopefulviewersshouldnotpeerupattheskywithoutspecialviewingequipmentsincelookingatthesunwiththenakedeyecancauseblindnessderekralstonaprofessionalphotographersaidheusedaweldingfiltertocaptureadirectviewofeclipseinthefoothillsaboveorovillecaliforniahesharedthephotooncnnireportnotingtheratherslimswathoftheglobewhocouldseetheimpactoftheeclipseralstonsaidhewantedtoenabletherestoftheworldtoseehowclearitlookedtothoseofuswhowerefortunateenoughtoseeitthesliverofsunshinethentraveledsoutheastacrosscentralnevadasouthernutahandnorthernarizonaandthennewmexicoitpassedoveralbuquerquenewmexicoaboutseventhirtyfourpmninethirtyfourpmetbeforepeteringouteastoflubbocktexasaccordingtonasa

**Answer:**

tafoerhbmkoeadaaaaieomnsdetctnasnbdopeaplhttaigseiaobevnkuiskdreetatawbonadntadxtpueshtodujwmoootuananooerawirhihdeooriiseehhnpenastetioahtaiieeueatoleoortyoevniteitntkealerlaenoaseailouivfptolvvcohreonothhithbcsechianhteeetrswrooewrtegehvsievseccaaunarnodnxterqumotntrnrutreosuksrtaswesaslrngesaaruocenannaaepispdhnietpaohgeotwbitchcsuhwngentahteleeuirtmeuviwosiwtanrdhasialypeiuarivtotcrezasacheerharntonesoptdiwteetpnnssetifxsetfesdeastsawqenoastneneddrooipgedelfrpacwlifibrliihtocengaswflhltpfcetiatbeowtheldouwoaootlostrettsteseaneiaemosvbreiovionhfmfenefoxcnahdtopoeehotxnlrnrrpgnogitrhihararetoeiraoeehccaornvusdihotdoyocsaosarfouurstymatymnvweslmmaharpohssoltmnenfhnoefeorvrnfaorgeodeadrtcetrareetnnntrrrhpvrutuhwucigpslnhwhecuisespsatpauwntcrrieshtseiareepoirieemheeoeiteplseentshleciktoheueheeeunneoareldtuntanteipdaueeastypetrberutbtadohomwctoogttpnselllbmyianvdacueaignmolnwatnfrhenhheloreigbstoneiretcleafisneronirosyteaonennemetnnlocehrrosrzctctamdnelndhrwtaflepeahnftetitsnenopwdhuwhnetkhpliuncktuhaycbneanfohrrhddittdtoinolooefaahtnpottlatoodhatlrodnolrfoooaotssertustifhhadhasrvorhorznneiseuqwcueruiioeotgalcaogseohntsgfonhaheansesadriarsefepetihhnonrtncrekhnunaydcteonrefotiwbgpcvourtoehtmyhtedeelcsuspinelkeutmeaestetigspiswgetcoaunorusotetohvhspiudecenyetnaeislppeitieemiogeiedasnsktrslohisegeaeeeceehaollnsdhnrtnrrsogwuemoessawdahtedeltehfofnntisrnetlusonnahtdhrahwcaolenxbehfmtypepitobecin

b) (1.5pt) Calculate and plot the letter frequencies of the ciphertext (use the spreadsheet provided) and compare it to that of the English letters shown below. Comment on the relationship between both.



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

**Frequencies**

a 111b 17c 42d 44e 192f 29g 23h 83i 81j 1k 11l 47m 23n 111o 125p 39q 3r 89s 86t 136u 46v 19w 31x 6y 13z 3

**Plot:**

**Comment:**

Because using Columnar transposition cipher doesn’t change the frequency of each letter, the two charms are the same.

**Q2 (3pts) Substitution Ciphers**

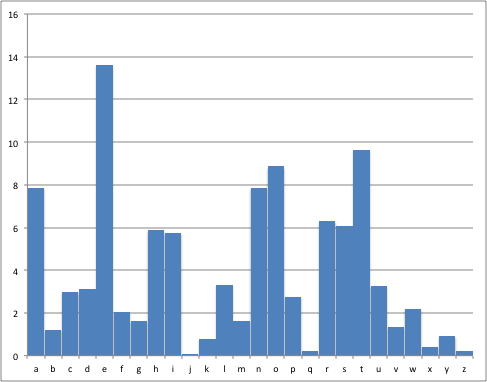
a) (1.5pt) Encrypt the following plaintext using the Caesar substitution cipher. Use the key 4:

theshadowofthemoonsweptacrosstheglobefromhongkongtothetexaspanhandleasarareannularsolareclipsebeganmondaymorninginasiaandtraversedthepacificthesunappearedasathinringbehindthemoontopeopleinanarrowpathalongthecenterofthetrackwhichbeganinsouthernchinaheavycloudsobscuredtheviewinhongkongbutresidentsoftokyoandothercitieswereabletogetaspectacularviewforaboutfourminutesaroundseventhirtytwoammondaysixthirtytwopmetsundayeventswereheldatschoolsandmuseumsinjapanwhilemanymorepeopletookintheunusualastronomicaleventathomeoronstreetcornersafterwhizzingacrossthepacifictheshadowemergedovernortherncaliforniaandsouthernoregonwherethousandsofpeopleattendedpartiestowatchtheeventthefirsttoappearintheunitedstatessincenineteenninetyfourexpertswarnedthathopefulviewersshouldnotpeerupattheskywithoutspecialviewingequipmentsincelookingatthesunwiththenakedeyecancauseblindnessderekralstonaprofessionalphotographersaidheusedaweldingfiltertocaptureadirectviewofeclipseinthefoothillsaboveorovillecaliforniahesharedthephotooncnnireportnotingtheratherslimswathoftheglobewhocouldseetheimpactoftheeclipseralstonsaidhewantedtoenabletherestoftheworldtoseehowclearitlookedtothoseofuswhowerefortunateenoughtoseeitthesliverofsunshinethentraveledsoutheastacrosscentralnevadasouthernutahandnorthernarizonaandthennewmexicoitpassedoveralbuquerquenewmexicoaboutseventhirtyfourpmninethirtyfourpmetbeforepeteringouteastoflubbocktexasaccordingtonasa

**Answer:**

xliwlehsasjxliqssrwaitxegvswwxlikpsfijvsqlsrkosrkxsxlixibewterlerhpiewevevierrypevwspevigpmtwifikerqsrhecqsvrmrkmrewmeerhxvezivwihxlitegmjmgxliwyrettievihewexlmrvmrkfilmrhxliqssrxstistpimrerevvsatexlepsrkxligirxivsjxlixvegoalmglfikermrwsyxlivrglmreliezcgpsyhwsfwgyvihxlizmiamrlsrkosrkfyxviwmhirxwsjxsocserhsxlivgmxmiwaiviefpixskixewtigxegypevzmiajsvefsyxjsyvqmryxiwevsyrhwizirxlmvxcxaseqqsrhecwmbxlmvxcxastqixwyrhecizirxwaiviliphexwglsspwerhqywiyqwmrneteralmpiqercqsvitistpixssomrxliyrywyepewxvsrsqmgepizirxexlsqisvsrwxviixgsvrivwejxivalmddmrkegvswwxlitegmjmgxliwlehsaiqivkihszivrsvxlivrgepmjsvrmeerhwsyxlivrsviksralivixlsywerhwsjtistpiexxirhihtevxmiwxsaexglxliizirxxlijmvwxxsettievmrxliyrmxihwxexiwwmrgirmrixiirrmrixcjsyvibtivxwaevrihxlexlstijypzmiaivwwlsyphrsxtiivytexxliwocamxlsyxwtigmepzmiamrkiuymtqirxwmrgipssomrkexxliwyramxlxlireoihicigergeywifpmrhriwwhiviovepwxsretvsjiwwmsreptlsxskvetlivwemhliywiheaiphmrkjmpxivxsgetxyviehmvigxzmiasjigpmtwimrxlijssxlmppwefszisvszmppigepmjsvrmeliwlevihxlitlsxssrgrrmvitsvxrsxmrkxlivexlivwpmqwaexlsjxlikpsfialsgsyphwiixlimqtegxsjxliigpmtwivepwxsrwemhliaerxihxsirefpixliviwxsjxliasvphxswiilsagpievmxpssoihxsxlswisjywalsaivijsvxyrexiirsyklxswiimxxliwpmzivsjwyrwlmrixlirxvezipihwsyxliewxegvswwgirxveprizehewsyxlivryxelerhrsvxlivrevmdsreerhxlirriaqibmgsmxtewwihszivepfyuyivuyiriaqibmgsefsyxwizirxlmvxcjsyvtqrmrixlmvxcjsyvtqixfijsvitixivmrksyxiewxsjpyffsgoxibeweggsvhmrkxsrewe

b) (1.5pt) Calculate and plot the letter frequencies of the ciphertext (use the spreadsheet provided) and compare it to that of the English letters shown below. Comment on the relationship between both.



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

**Frequencies**

a 31b 6c 13d 3e 111f 17g 42h 44i 192j 29k 23l 83m 81n 1o 11p 47q 23r 111s 125t 39u 3v 89w 86x 136y 46z 19

**Plot:**

**Q3 (3pts) Arbitrary Mapping**

Use cryptanalysis to crack the file “challenge.txt” (it should be on the blackboard in the same location as this file). Show all your logic and the plaintext.

**Plaintext:**

keysarepiecesofinformationthatdeterminetheoutputfromanencryptionordecryptionprocessasingleciphercanproduceanalmostlimitlessnumberofdifferentoutputswithdifferentkeyvaluesallowingsecurecommunicationevenifthecipheritselfisknowntohostilethirdpartiesitmightsurpriseyoutoknowthatalmostallciphersarepublishedinthescientificpressorinstandardsdocumentshavingthemavailableforwidespreadscrutinyallowsmanypeopletocheckthattheyaresecureanddonotcontainweaknesseswhichcouldbeexploitedtocompromisethesecurityofthedataencryptedusingthatcipheracomputerencryptionkeyisnothingmorethanastringofbitswhereeachbitcanhaveavalueofeitherzerooronethenumberofpossiblevaluesforakeyissimplythetotalnumberofvaluesthatthekeycanhavesoouronebitlongkeycanonlyhavetwopossiblevalueszeroandoneifwechoosetohaveatwobitkeyitcouldhaveoneoffourpossiblevalueszerozerozerooneonezeroandoneoneinfacteverytimeweincreasethelengthofthekeybyonebitwedoublethenumberofpossiblekeyssoathreebitkeyhaseightpossiblevalueszerozerozerozerozerozerozeroonezeroonezerozerooneoneonezerozeroonezerooneoneonezeroandoneoneoneonethetotalnumberofkeyscanbewritteninscientificformastwokeylengthsoakeywithalengthofeighthastwentyeightthatistwohunderedandfiftysixvaluesbuthowlongshouldakeybehowshortistooshorttheproblemwithshortkeysshortkeysarevulnerabletowhatisknownasabruteforceattackjustlikeyoulearnedinweektwoaboutpasswordsabruteforceattackiswhereacomputeroranumberofcomputerstryeverypossiblevalueforakeyuntiltheyproducerecognisableplaintextsincecomputerscanworkthroughkeyvaluesextremelyrapidlykeysmustbesufficientlylongthattheyofferaverylargenumberofpossiblevalueskeysmaybeknowntotheuserintheformofpasswordsortheymaybestoredinacomputershardwaresuchasthedecryptionkeysstoredonadvdplayerthatallowittoplaytheencrypteddatastoredonthemoviediskortheycanbegeneratedbyacomputerasandwhentheyareneededsuchasconductingasecuretransactiononashoppingsitenextyoulllearnaboutthekeydistributionproblemsourcehttpswwwopenedu

**Logic:**

First, Analyze how often each character appears. And there are the frequencies.

~ 39} 51| 5z 1c 87` 121\_ 42^ 22@ 270? 166> 68= 41< 25: 181/ 37. 57+ 126\* 63( 128' 70& 49% 107# 34! 125  20

Next, use the “FrequencyAnalysisTemplate\_arbirary.xlsx” to generate the plot.

Because the frequency plot is similar to the letter plot. So we can replace each character in order. And the results are readable. So, this way may work.

Finally, we get the final answer.

**Q4 (3pts) Vigenere Cryptanalysis**

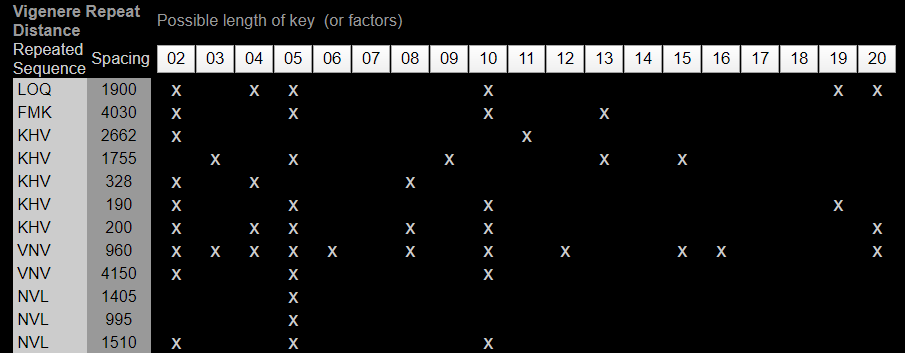
The ciphertext is posted to the blackboard (same folder as the assignment) in a file called “ciphertext”

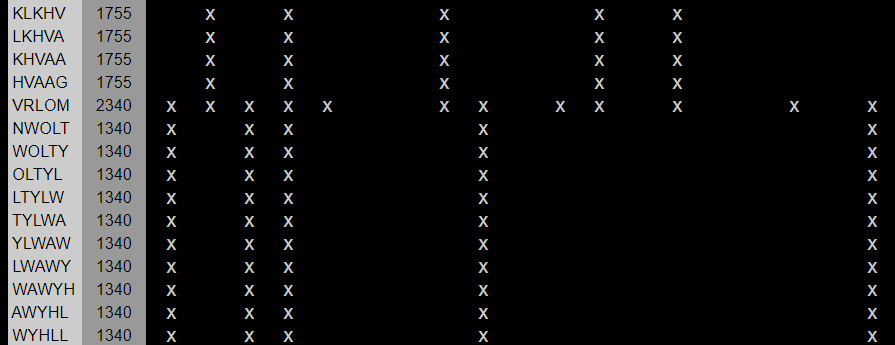
1. (1pts) Do a **repetition test on the cipher.** You can use this site:   
     
   <http://www.simonsingh.net/The_Black_Chamber/vigenere_cracking_tool.html>.

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

Based on the test, what do you think the key size is? \_\_\_\_**5**\_\_\_\_

**Screenshot**:





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

**set1:**lkllswxfjgjlgfjwwlmskkakwgvjygllfvkxtgwqajlgszvwtekjqajzsvkszflwlwkavffghwjjswasajhfwwjvsamwxhffsslalkgwakvgaefggflqxazwgtgyqswwasfsdazjwaskakszvwsmakdwayysgkwowvuwdkfvawdfwfwlxdgfjwzystekaalllvauxgjlfgmgjfslklkzwlffoxgfjaghuyswdgduvldwjamdeskjdwkemwzojjwzjdaggiajldwagwjgxakfkzhxawwlkllllanqjkgwavofgjxscwakdyeewhvcflevwdwsafwjgzwjfjwwtlojgjwjmswwulawetwajzwlsassadgjvwswqltggkgslmzjlwcessnwwkgggsukwswwkfaaafueusdzwavlksluvmakszwxeowlwwwswjgmgllvmfllyskzkjvjzswazovjffuzwklxkewljslzwhtxwgswfjjptkajmqwgljugkwauakkskskggwfcwdmzyssewkakzflozffstwflwsjmfoowlwjwwqclgwjksjwakuszjsezyufwdwzlkuskxljgdfeglwfjscaqmhudllwmladswljfkwusgxwgpgxmzjmvlkmdlgywvqxjfzkawhatkscztschlskgaozxwswklauaawakwkwgqavvjuljyfwiwzsehvscwlwunwwgajmlsvwvhsscjvlhfymwwfjhvllqgjmwwsfkvysxlfvtaelnjkgkskjdcltvjsvdldzwufsulgfxgfqufzuallvkxsvloaflgmlgywowlwjwumexaskvgwagkwmhmtgqglfzwehkwlonahuwcufzfwwsozalllyhgvjukanwswwotgosmlycgdgwswmglggqysglgemuwlgwjkdeskkgwsssskwgukvwuwftjkksufgflszszywcjuwsjanvtwvelejlflsljlankkfgazawfzssmfeshjhuksksgwhllkdzoouuawgdkefjkdxfjsodezszgajskqsfuovslggpsqwgufxjlwwsjjgwwkakmzwxlksddwwazvfgfzmcgtwukaksuaklllvfqwwjussscmlllmklt

**set2:**ohpozpypubllylrzhoiaylzhvylhtubhkbhahunvuvfuahhufphlduurzlkapfbuhuctyahyvzplwuusvajnkpcpsluhplhhsvlupaazszzauhhyuklakuhlsvbpacuwjyztpvplyjijuzilpyuyzjlwzkpatahzyuossazhahpksjklvsklrzhbysttusdoypsjbkzyhukjdhzoovahzyorvvtalyyyllqhsyslwvkvhluplgzpazlvavpluvzhpkuyubvvpydubwpmmuanmlvduhzphzsapulvpabjkdpabpuswzuvpatpssizlolcalkduwkyuhwkvtwyyopzmpulyuahbzvjfbzaluylusaslpddvurppostylbyoyalvtzjuuluuhatcuhbhczkvpvaknpzlamlezndljvaphupulhklhcotkyuptunsopkzhhvpabhvhjhpuyjlpvlrhrhlaolvwzypszlyvspvdrtjzpwyjlulsuulooyparbabaaajhpwakuzsyuppcpulalllaplavalusoujdalhlaldslzaldmpudkpkhlljuzulllvpjfipohrappsnuhnvwpkilazjywhblovftonluuphnphryrvuyhpmyuzsaabslvyaalhakzbjuphallallvyuvpyjuuhlzppklvjozutazanabvnvvhrykoajbypyhvkazafllluyyulyoumldwaazlaflalmkhbvlvhduuhsjkjjlphjtollwuwalzpyajhvfphlplfplzslyvabrypaathzbappzozkvafvhvtllyshbztlaldshrsvmcpojuwjbvdasshazmpplyvlzzoolyyaadvbhaazrulylpnawularlavhtjpobmvuynaldlbksjpbhdthhayvclahhhdpuhlbashvzknsjbksodahvkapjmhuvlunvuljllashruyvulywhlhbhaokojonyaphwhatljzalwwjlwdykyapjajbzloyokuvvhlvsmphljcyaypurukvlitmavuzhrvphtlaumlnvpysnyvpjfcljzazpahhlyyaoshfywklalyavuzabzvbupivjloldvkswyhashplnlslahhs

**set3**:qvkizdwvmzxzbebbvmtqmbkenqvbwxzzxktpaqijmxwgekvkkvxvwowwuzqwxxzbqbqqmtukzmbixbzqvpwkgvqokazatztvlvzuvzimaeipnbzbmzzmiidvmczommucaubxkvkvzmwwomtliimvbzacpivibzaxamiabwwbpbajgmkuzgbebqzvqmmimammivgmtckcvgqpwukmqvmabciqzzqiamiwztwaiikqtjixuilmuqihmbdazcvtmuwkhmmmlmvuwmwmbzmbqowwwxazobakjkmbndlbvztwmmbpvmwetvolvwmkkgzjamaigfuiowqmlbiwbqwammvcammvigwtuvvwiaawomeambqzevmpkbmzvmqiivamqzaxvtnwqlzbkzcumglksmmvzhvpmmzbakwummumapnadtbvkzawvamiikilvijpqizqajpnbmmbevwoawitovaivbmdvqmvnibcbxwqvagocbmlgmbmcpzmaiiaaiqzipmtaomqibzvzwemqwbwmlqbqkgivmzzgbeklwgmbgiibztwkalibwiwnvmqqjltzismilwbbummpmblbaiokgmoaizpkbmbbbiibztdmxzmipdlkvucnbmmqzmskvimmxipiabdzkiaxtpmmatozjqkbbzzcmwbioiwozukmlimqiqjljaqwcpvnqabbampbpwiwaiqzlbzebxvzczlyzbwlqvmtqbqieazbbnibuniakmqiobbiszlliswipzaotikxjvibzjtvvznvaaxwwqvumtiqvwpiubztmmbzbwvpabvciaialkbgatwkalbalammviwaczzvmxmlkpbxbvqvkbcbwwbwwmeqvmdmiamwmmzawwmblqmkgkbiibwvvzlmwwqvabwtqbksvxvvqxnmvgvtsvvmekvqqzexntiskplvwpzcwmbczvkiboislzmtaeibaaiiopmavzoltpmekqmmixlvaomuemqwqazbimqwlwqvmistblmimbmzzavawcbvzgqmqwvmmkxbmtmuqclqjlnmzqtmkxzqcoacgwbwiwmamppxjgnzqvwiitzwdzmbmetpzjipaacakltvtamzmebwpivqlsaiolwzizxm

**set4**:fnygrrzggpbfulvvqevbsbhnfrvvgvrferyrryygqrsgnxqrencgeseehbpefvrrajpmplnbnplpnyrnsrzbggrvbbrrzfspnrgrqlozcbarbvrrurnfgyrfaggnfonobnehnfurrahyyfvzbewnvhnovztsubannjapuyanteunpnbcujulvfvpgpaqzorrbnffcpbqqfbnzlnjaczvuqqaqcapfpaqnvyjfabinhpnbewgnazrnurgnftrqgaxrpqfgffaaiangbgepvybehrvounybhouvbnuqlqaeyurqfebnvnrvpauvnbnbgneffnfgfgffgcrcgegnycvgfiptbfqrnnaavrefvevzbbrbrirhfgjgcpvegjjavgbgrezrtanvrabeqrufcartnfnebpngnegewrnffsvvyufrrrpgnagabtgsgegtfefvbbyvvfnngirvgeretggbgergaqfpauavnsarfghgbgboplepajqqeggccahnrycutqbgbrtbsrfasryfgfubheetevrjbjnbgvrboexvnyyujgfjgaeggggfhrbigfvvfsnrcfanrjqggeanyergarvnusunlyzbgnragrngrrgbhccggeyaggfggvfvrgrprvrfvegyyrsfqbgpvrnunfrghjryraggqbueggzagarghcoqvrgbanuguprfraeslxegbnbrurggzrrhsjhnsnovbnafrvpnfrtroegnxaairvbgfrnzgfeahqhfrpgbybgbrnbthbsggnnesarzqzcfiervrrelsanrbfrrguqytgpjnxvfnyyujggjogpnfezgorpgorptxrrnvtarxetrfuujgqbyggrepnqsavaavuarzanhnnnvhfyprxlavgghfnjgefnrnnbvbnnegbgyrgggubvbarvebbggprgrerrcmepvbsvybxalbcfngblgfbcpshqnbbarynovngyfaerqzrqnfcqsahbygegcbgbczgfqbvvpgrjyfrngfgvqtfpfazggqberfvavnccoebfgapceryvaeurqbzrahhabfnrbvgrqarzpfrtavbebpfqrgnarvrygbrrbbvvaaaufryfbnnzlroaztrez

**set5**:mviagheiwivjisqqstgryhwzxwkrmgwesvsqhppetvwlwijhmpeposxivyxwsgwvqexiimnvxyflvcxxsymqliaxtjphwsmmxreryrpeevhvvsthyhfsepfxejcflihpjmifxaezxxxhixwizgspgtvprehvmzitrwreiicavievsprxssisqwrlesxieirbvvywvixmwxgmetpekstdemyhwvixhxhyrrmijmrirmpxzssmkijpwirskxwejlcjppxtsxjeempfltceorihxvsxvpviyxyexpriyafwipmfesqvgtpgrsxeirsvjmrmexrlsxstxliwivxsoeyxsaisirxsrxpshrhkghmrerrzrlirqqlesyhriximsksvlestwsqkirgrqiwplvxaexaaejyrlpxsgyrwiierhcmxxpsywrxhhzilsmsxlwigsywiqwxpviixwlxxshlyaewfikiismeggvxxxmsvlxlaiyixiiexekmeiwewvpcviirrivkxfmewesgswvwwvvigmetxeolrrsrzjifmgwlhrslmeeiolimlxxrjmxgihsxvhevxzrmselimrepvmhwwxesigtptemvpwlwxlvplrimelewsklaitspgigieoqtgjrksssmixmwlepwyigaewrrrxxhlsxjrwlewhiellxspmwgvvhriemsmmwhxxieiiwgwrvvslfghesswrxregrggirbivwvvviihxwxiiqzvxmewixsisrkwmeoswixivtfseqjiasfvexxxitsigishrwqigwxxetmsasemhmexsxvrxwlhrslesiixkxiqlpwilfsssxwqvsxxxemkhieirirvpmsmrgxsxxrisregreqcvhxofweilxwssrehrcorlgcrhgrvdrvkrfyvchliesqgroxhivfxsixiapvepiemxqvwslshsxpxvrvieijtlmrkvvjmwirehtcexwsvmerxxzvixgphmmzliwirpsxaftrvosgwhxwvlwmiiiiiykeixsysxxwxpkwspiascilewsmqirfbmytgfwlsyxvvrpskxxxeojriwgzwplamwvrhvrwherviqwjrixeixqxerxqgwwyksirs

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 | w | s |
| set 2 | l | h |
| set 3 | m | i |
| set 4 | r | n |
| set 5 | i | e |

1. (1) What is the plaintext?

thisisanarticlethatwasreceivedfromaninternetsourcereportersforthenewyorktimestimeandotherpublicationsrefusetodiscussawaveofstoriesdenigratingmotionpicturestarsandproducersallofthembasedonillegallyobtainedpropertyofsonythatwashackedandfencedbycriminalsapparentlyworkingfornorthkoreasmurderousdictatorshipsonypicturesentertainmentwasvictimizedrecentlyinamajorcorporatesecuritybreachapparentlyinretaliationfortheupcomingcomedytheinterviewdigitalcopiesofunreleasedfilmspersonalfinancialdataonentertainmentindustrynotablesemailspasswordsandotherinformationareportedonehundredterabytesofdatainallhavebeenstolenaboutfourtygigabyteshavebeenmadepublicsofarmainstreampublicationswhichareneverreticentaboutscoldinglessestablishedmediaoverarcanejournalisticscruplesarepublishingdamagingdatafromthistroveasnewspapersandnewschannelscallthestolensonydatawithgreatrelishandbarelyconcealedcontemptforhollywoodthenewyorktimesissharinguncharitablecommentsmadeinemailsbetweentheextraordinarilysuccessfulproducerscottrudinandsonystudiocochairwomanamypascalthewashingtonpostemphasizesthatrudinhadunkindwordsforprominentactressdirectorandproducerangelinajolieaswellasforanillconceivedplantobuildacleopatramoviearoundjolietimemagazinessamfrizellteasesthesevenmostoutrageousthingswelearnedfromthesonyhackfrizelldeclinedtorespondtoquestionsfromnationalreviewonlineabouttheproprietyoftraffickinginstolengoodsforthepurposeofwritingbreathlessarticlesaboutscuttlebuttthatifitinvolvedanyotherindustrywouldbeconsideredwellwithintheboundariesofnormalworkplacesnipingalsodecliningtocommentmichaelcieplyandbrooksbarnesofthetimesandvarietysalexstedmanawashingtonposteditorrespondsthatthepaperdoesnotpermitreporterstobreakthelawinpursuitofstoriesweneverencourageanyonetostealdocumentsnationaleconomyandbusinesseditorgregschneiderwritesinanemailtonationalreviewonlinehoweverwhendocumentsmaketheirwayintothepublicdomainoraresenttouswearewithinourrightstoreportonthemleaksfromcompaniesandgovernmentagenciesarenotuncommonovermanydecadessuchleakshavepresentednewsorganizationswithawiderangeofcircumstancesthatcallforthemtoexercisejudgmentweassesseachsetoffactsindividuallyinthisinstancethereleaseofdocumentswasaneventthatdemandedcoverageandtheinformationbroughttolighthasstirreddiscussionaboutahostoflegitimateissuesthatalsowarrantedcoveragethisisanotherarticlethegrowingddosthreatunknownattackershavebeentestingthedefensesofcompaniesthatruncriticalpartsoftheinternetpossiblytofigureouthowtotakethemdowncybersecurityexpertbruceschneierwarnedtuesdaylargenationstatesperhapschinaorrussiaarethelikelyculpritshesuggestednationstateactorsaregoingtoprobetofindweaknessesinallofourtechnologiessaidtravissmithseniorsecurityresearchengineerattripwiretheywanttoknowwhatcanbedonenotonlyintheeventofacyberwarbutakineticwaraswellhetoldtechnewsworldtheeasiestwaytotakeanetworkofftheinternetiswithadistributeddenialofserviceattackschneiersaidandsomeofthetargetedcompaniesrecentlyhavebeenhitwithddosattacksthataresignificantlylargerlongerlastingandmoresophisticatedthanbeforetheattackstypicallyrampuptoaparticularlevelthenstoptheyresumeatthathigherlevelandthencontinuerampingupasiftheattackersarelookingforthenetworksexactpointoffailureschneierspeculatedtheattacksusemultiplevectorsforcingtargetstodeployalloftheirdefensesthusdisclosingtheircapabilitiesbecausetheattackerswhereaboutsareunknownpotentialtargetscandonothingtowardthemoffschneiersaidthedataseemstoindicatechinaisbehindthembutitspossibletodisguisethecountryoforiginddosandotherattackshitrecordheightsinthesecondquarterofthisyearakamaireportedddosattacksrosetwentythreepercentoverthenumberrecordedinquarerfourtwothousandandfifteenandwebapplicationattacksincreasedtwentysixpercenttargetssufferedagreaternumberofrepeatddosattackstwentynineonaveragemultivectoredattacksincreasedasdidmegaattacksofmorethanonehunderdgbpsusingsimpleattackvectorspossibleornotstateactorsareprobablylookingatanumberofdifferentwaystodisablepartsoralloftheinternetcommentedpaulmockapetriscoinventorofthedomainnamesystemcurrentlychiefscientistatthreatstopddosisoneofthewaystodothatandiwouldimaginestateactorswouldattackroutingsystemsaswellhetoldtechnewsworldtheattackswouldbemosteffectiveagainstsharedcommonsthepublicresourcesonthewebbutpeoplecouldgobacktothesystemofpartitioningtheinternetmockapetrissuggestedthosewhohavetheirownprotectednetworkwillcontinuetohaveinternetaccessatakedownoftheentireinternetisnotgoingtohappencontendedmartinmckeaysecurityadvocateatakamaibecauseitsawholebunchofnetworksandyourenotgoingtotakeitdownunlessyoutakedownallthecircuitsyoucantakedownacompanyanorganizationorpartofagovernmentbutyoucantreallytakedowntheinternetasawholecommunicationslinksaretoowidespreadforaglobalattacktosucceedhetoldtechnewsworldthereareacoupledozenterabitcircuitsfromsanfranciscoalonetohongkongandtokyoandotherplacesthelargestnetworklayerattacksseensofarapproachingfivehundredgbpsareanorderofmagnitudesmallerthanthebandwidthcapacitythelargesttransitprovidersandispsmanagenotedtimmathewsvicepresidentoftheincapsulaproductlineatimpervawithproperddosprotectionsinplacemostattackswouldbestoppedintheirtrackshetoldtechnewsworldworstcasescenariosthelossofutilitiesandemergencyservicesresultingfromaninternettakedowncouldpromotetheestablishmentofmilitiagroupsandpossiblyabreakdownofsocietywarnedmichaelpattersonceoofplixerimagineyourneighborsexcludingyoufromprotectionbecauseyouhavenoresourcestosharetheresponsibilitytosafeguardtheinternetfromattackshasfallenlargelyonserviceprovidershetoldtechnewsworldintheshortrunbanksandotherbusinessescouldsustainconsiderableeconomiclossesiftheinternetwentdownandtheylostephemeraltransactionaldataakamaismckeaysuggestedbutlongtermoutagesarentaproblem

**Q5 (3pts): Data Encryption Standard**

**Read the document titled SDES.pdf**

Using SDES, encrypt the input 10010111 using the key 0101010101 and the modified S-BOX below:

,

Show a step-by-step results similar to the one below.

|  |  |
| --- | --- |
| Key, Permute 10 | 0010110011 |
| Left Shift Key (on 5's) | 01010 |
| Key, Permute 8 (KI) | 00011011 |
| Key, Shift Left twice (on 5's) | 00111 |
| Key, Permute 8 (K2) | 10101100 |
| Initial Permutation (IP) | 01011101 |
| Right Half of IP, Begin Round 1 | 1101 |
| Expansion Permutation | 11101011 |
| XOR with K1. (XOR) | 11110000 |
| Left Half of XOR | 1111 |
| S-box Zero | 01 |
| Right Half of XOR | 0000 |
| S-box One | 01 |
| Join S-box Outputs | 0101 |
| Permute 4 (F) | 1100 |
| Left Half of IP | 0101 |
| XOR Left Half with F | 1001 |
| Replace Left Half of IP, End Round 1 | 10011101 |
| Swap Halves (SW) | 11011001 |
| Right Half of SW, Begin Round 2 | 1001 |
| Expansion Permutation | 11000011 |
| XOR with K2 (XOR) | 01101111 |
| Left Half of XOR | 0110 |
| S-box Zero | 01 |
| Right Half of XOR | 1111 |
| S-box One | 01 |
| Join S-box Outputs | 0101 |
| Permute 4 (F) | 1100 |
| Left Half of SW | 1101 |
| XOR Left Half with F | 0001 |
| Replace Left Half of SW, End Round 2 | 00011001 |
| Inverse Initial Permutation, Result | 10010010 |