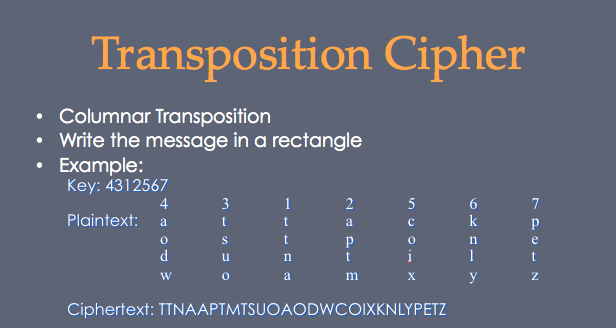
Assignment 1

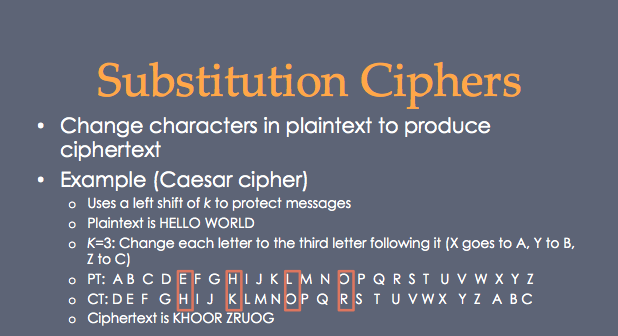
Submit through the blackboard before 12:00am 02/15/20

NAME:

Instructions:

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





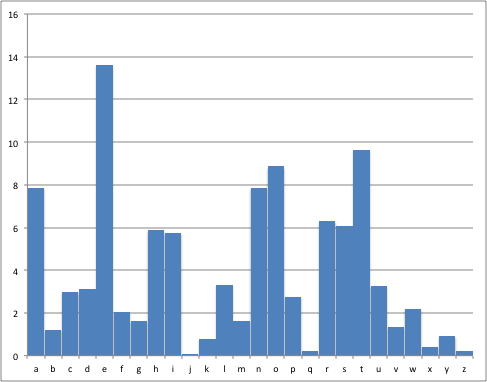
We talked in class briefly about transposition and substitution operations used by symmetric key encryption algorithms. A transposition cipher is one that uses the transposition operation only. A substitution cipher is one that uses the substitution operation only. A product cipher is one that uses both.

**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

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.



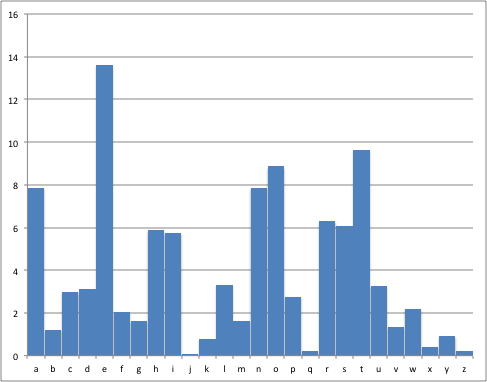
Source: https://en.wikipedia.org/wiki/Letter\_frequency

**Q2 (3pts) Substitution Ciphers**

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

theshadowofthemoonsweptacrosstheglobefromhongkongtothetexaspanhandleasarareannularsolareclipsebeganmondaymorninginasiaandtraversedthepacificthesunappearedasathinringbehindthemoontopeopleinanarrowpathalongthecenterofthetrackwhichbeganinsouthernchinaheavycloudsobscuredtheviewinhongkongbutresidentsoftokyoandothercitieswereabletogetaspectacularviewforaboutfourminutesaroundseventhirtytwoammondaysixthirtytwopmetsundayeventswereheldatschoolsandmuseumsinjapanwhilemanymorepeopletookintheunusualastronomicaleventathomeoronstreetcornersafterwhizzingacrossthepacifictheshadowemergedovernortherncaliforniaandsouthernoregonwherethousandsofpeopleattendedpartiestowatchtheeventthefirsttoappearintheunitedstatessincenineteenninetyfourexpertswarnedthathopefulviewersshouldnotpeerupattheskywithoutspecialviewingequipmentsincelookingatthesunwiththenakedeyecancauseblindnessderekralstonaprofessionalphotographersaidheusedaweldingfiltertocaptureadirectviewofeclipseinthefoothillsaboveorovillecaliforniahesharedthephotooncnnireportnotingtheratherslimswathoftheglobewhocouldseetheimpactoftheeclipseralstonsaidhewantedtoenabletherestoftheworldtoseehowclearitlookedtothoseofuswhowerefortunateenoughtoseeitthesliverofsunshinethentraveledsoutheastacrosscentralnevadasouthernutahandnorthernarizonaandthennewmexicoitpassedoveralbuquerquenewmexicoaboutseventhirtyfourpmninethirtyfourpmetbeforepeteringouteastoflubbocktexasaccordingtonasa

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

**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.

**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? \_\_\_\_\_\_\_\_

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

Set1:

Set2:

.

.

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 |  |  |
| set 2 |  |  |
| … |  |  |
| … |  |  |
| … |  |  |
| … |  |  |

1. (1) What is the plaintext?

**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.

