

## Assignment #1: Classical Ciphers

Total: 100 points

All written assignments should be created using a word processor (e.g., Word or Latex). Hand-written work will not be accepted.

All students should submit a pdf file of their answers through Canvas. Be sure to name the file as follows: HW1\_LastName\_FirstName.pdf. For example, if a student's name is John Doe, then he would name the file as HW1\_John\_Doe.pdf. Also, submit the source code (including any header files that you may have used) to Canvas. Name the file as: HW1code\_LastName\_FirstName.fileExtension (e.g., HW1code\_John\_Doe.cpp).

Zip up all files **into one zip** file and submit it to Canvas.

1. The objective of this problem is to learn about monoalphabetic substitution ciphers and to use letter frequencies to cryptanalyze a given ciphertext.

Write a program (in any programming language) to analyze the letter frequencies in a block of text. Ignore case (upper and lower count the same). It should count the number of times each letter appears in the text, the number of times each pair of letters appears, and the number of times each sequence of 3 letters appears. Your program should sort the counts of single letters, pairs of letters (bigrams), and triples of letters (trigrams), then print the non-zero values in decreasing order. For single letters, print all non-zero values; for bigrams and trigrams, print the first 30 non-zero values.

Turn in the following items by the deadline.

- (a) (50 pts) As instructed above, submit a soft copy of your program via Canvas. Please write your own program! Do not copy other peoples' programs.
- (b) (25 pts) Output of your program run against at least 2 different texts of sufficient length. Make sure that the texts are sufficiently long enough for frequency analysis.
- (c) (5 pts) Compare the 2 sets of frequencies you produced for part (b). Are they similar or different? Explain why they are similar or different.
- (d) (20 pts) Using your frequency analysis results, decrypt the ciphertext given below.

For part (b), you can run your program on texts found on the Internet. For example, you can find the full text for Hamlet online (<http://www.bibliomania.com/0/6/3/1057/frameset.html>).

Ciphertext for (d):

bt jpx rmlx pcuv amlx icvjp ibtwxvr ci m lmt'r pmtn, mtn yvejx cdxv mwmbtrj jpx amtngxrbah uqet  
jpx qgmrxjv ci jpx ymgi ci jpx hbtw'r qmgmax; mtn jpx hbtw rmy jpx qmvj ci jpx pmtn jpmj yvejx.  
jpjt jpx hbtw'r acutjxtmtax ymr apmtwxn, mtn pbr jpcuwpjr jvcufgxn pbl, re jpmj jpx scbtjr ci pbr  
gebt yxvx gecrxn, mtn pbr htxxr rlcjx ctx mwmbtrj mtcjpxv. jpx hbtw avbxn mgcun jc fvbwt bt jpx  
mrjvcgwxvr, jpx apmgnxmtr, mtn jpx recjprmexvr. mtn jpx hbtw rmxhx, mtn rmbn jc jpx ybrx lxt  
ci fmfeget, ypcrcxdxv rpmgg vxmn jpbr yvbjbtw, mtn rpey lx jpx btjxvqxjmjbct jpxvxci, rpmgg fx  
agcjpjn ybjp ramvgxj, mtn pmdx m apmbt ci wegn mfcuj pbr txah, mtn rpmgg fx jpx jpbvn vugxv  
bt jpx hbtwncl. jpjt amlx bt mgi jpx hbtw'r ybrx lxt; fuj jppe acugn tej vxmn jpx yvbjbtw, tev lmxh

htcyt jc jpx hbtw jpx btjxvqvxxjmbct jpxvxci. jpxt ymr hbtw fxgrpmoomv wvxmjge jvcufgx, mtn  
pbr acutjxtmtax ymr apmtwxn bt pbl, mtn pbr gcvnr yxvx mrjctbrpxn. tcy jpx kuxxt, fe vxmret ci  
jpx ycvnr ci jpx hbtw mtn pbr gcvnr, amlx btjc jpx fmtkuxj pcux; mtn jpx kuxxt rqmlx mtn rmbn, c  
hbtw, gbdx icvxdxv; gxj tej jpe jpcuwpjr jvcufgx jpxx, tcv gxj jpe acutjxtmtax fx apmtwxn; jpxvx br  
m lmt bt jpe hbtwncl, bt ypcl br jpx rqbvbj ci jpx pcge wcnr; mtn bt jpx nmer ci jpe ybrncl ci jpx  
wcnr, ymr icutn bt pbl; ypcl jpx hbtw txfuapmntxoomv jpe imjpxv, jpx hbtw, b rme, jpe imjpxv,  
lmnx lmrjxv ci jpx lmwbabmtr, mrjvcgcwxvr, apmgnxmtr, mtn rccjprmexvr; icvmrluap mr mt  
xzaxggxtj rqbvbj, mtn htcygxnxw, mtn utnxvrjmntnbtw, btjxvqvxxjbtw ci nvxmlr, mtn rpycbtw ci  
pmvn rxtjtaxr, mtn nbrregdbtw ci ncufjr, yxvx icutn bt jpx rmlx nmtbxg, ypcl jpx hbtw tmlxn  
fxgjxrpoomv; tcy gxj nmtbxg fx amggxn, mtn px ybgg rpy jpx btjxvqvxxjmbct.