Homework 1
System Security
Winter 2007

Due: January 29, 2007
Points: 10

1. Paper Exercises (3 points): Exercises from Page 34: 2.4, 2.5, 2.8.

2. Programming project (7 points)

   Project goals.

   Be able to use letter frequencies in normal English text to decrypt a message that has been encrypted using permutation monoalphabetic cipher.

   For this assignment, ignore case, punctuation (e.g. commas, end of lines, white space).

   Write a program, in a programming language of your choice, that

   a) Counts the percentage of times each letter appears, and

   b) Prints in a sorted order each letter and its frequency, with the most frequent letter at the top.

   Apply this program on a large of piece of plain text to get the letter frequencies for English. Use this information to decrypt the following message:

   > rjvbhbtw xzmlqgxr ci "rlmgg br fxmujbiug" btagunx mvapbjxajuvx. bt jblxr qmrj, jpx mtabxtjr gbdxn bt amdxr ypbap rubjxn ctge ctx imlbge, jpx vclmtr gbdxn bt pcurxr ci rlmgg rbox bt rlmgg jcytr, mtn btnxxn vbwpj uq jc jpx lbnngx ci jpbr axtjuve, rlmgg pcurxr bt rlmgg jcytr yxvx jpx cvnxv ci jpx nme. fuj jpxt kubjx runnxtge, jpx vxdcgujbct caauvvxn. rlmgg pcurxr rxxlxn cgn imrpbctxn, mtn ybjp gmtn rqmax mj m qvxlbul, bj rxxlxn fmjjxv jc fubgn uqymvnr: gmvwx pcurxr btrjxmn ci rlmgg: mtn jpxt jcyxv fgcahr ci jxt rjcvxer - jpxt jyxtje - jpxt lcvx. jpx jcyxv fgcah pmn axmrxn jc fx m qgmax icv qxcqgx jc gbdx mr bjr ibvrj qvbcvbje: lcvx, bj ymr rclxjpbtw jc rpcy jc dbrbjcvr cv quj qpcjcwvmqpr ci ct fvcapuvxr. jpx fbwwxv ecuv fgcah - jpx fxjjxv ecuv fcvcuwp, bj rxxlxn. mijxv mgg, ypc ymtjxn jc gbdx bt m fcvbtw gbjjgx rxlb bt m rjvxxj? m wvxmj lmte qxcqgx, bj rxxlxn. bt rjvxxjr, cv xdxt gcy-vbrx igmjr ci qxvpmqr jpvxx rjcvxer, bj ymr qcrrbfgx jc wxj jc htcy ecuv txbwpfcuvr - lmhx ivbxtnr, wc vcutn jpxvx mtn fcvvcy qcutnr ci ruwmv cv pmdx m auq ci jxm mtn m apmj. fuj bt jpx fgcahr, ecu mvx bt "rqgxtnbn brcgmjbct" ybjp tcfcne jc jmgh jc cv amgg ecuv ivbxtn - mtn axvjmbtge tcfcne jc fcvvcy ruwmv ivcl! yxgg, tcy, jpx qgmttxvr pmdx vxmgbrxn jpmj jcyxv fgcahr mvx tcj jpx mtryxv. qxcqgx qvxixv jc ymgh ybjp jpxbv ixxj ct jpx wvcutn...cv mj gxmrj, dxve txmv jpx wvcutn.

   Turn in two programs: One that analyzes the frequency, and the other that does the translation.

   A large piece of English text for analyzing frequencies is Hamlet; it can be found at

http://the-tech.mit.edu/Shakespeare/hamlet/full.html

You can use any other text that you can access. Just make sure that this text is sufficiently long.