Math 3207 Assignment 2, early October 2012

Clearly write your answers to the questions showing all reasons, working and checks and indicate what each mathematical calculation is doing. Do not erase anything. Include all rough work and do not commit plagiarism. Feel free to write explanations of what you are thinking at each stage, nothing you can write can lose you marks!

1. You have found a slip of paper with some characters on, and you can see that someone has started to decode it, getting the first 6 letters, which seem to be in English.

   (a) What evidence is there in your message that should make you suspect that the code used is not a single letter substitution code? [1]

   (b) Assuming that the encoding is an affine digraph one with our standard alphabet; "`abcdefghijklmnopqrstuvwxyz␣.,`", use the first 4 letters to get the encoding parameters and check them using the next 2. [5]

   (c) Find the decoding parameters and hence decrypt the whole quote. What are the 10 most frequent letters in it? [6]

   (d) Give an example of a valid encryption which would not be uniquely solvable as in (b) for a particular choice of first word(s) which are unique within the class. [2]

2. The variables r and s in this question should be replaced by the two largest non-equal digits in your registration number.

   (a) Find the unique simultaneous solution to this system of equations by first solving the second and third for x individually and then using the Chinese Remainder Theorem. [7]

$$\begin{aligned} x &\equiv r \pmod{17} \\ 13x &\equiv s \pmod{23} \\ 37x &\equiv 1 \pmod{70} \end{aligned}$$

   (b) Explain where the proof of the Chinese Remainder Theorem from the notes must be modified to deal with the case when we have two congruence equations in x with moduli which are not relatively prime. In particular, what is the criteria for there to be a solution? [4]

”i stoo”
"gfhke␣wfqr␣gwkuarcqhqkpfybyfhgwfhwyekjbbbfwcnfhkysrfycyspfwbmflwjwr␣mfshwf"

”in fro”
".etps,udc,.␣wav␣tufivr,␣.endtu.kticatfcqjlndwocarfqjje,␣alrt.ew␣famfjlfic"

”it was”
"esdjuviwp␣vzn␣trasay.ikda␣vcavob.fyoay,␣khq␣vzn␣v.␣wiews,rv␣frwfa␣crq␣bf"

”i dres”
"iwsn.oqadwrqdnga,hlydban.eoglawwouyawltngax.ewmdcpmnbeisnuh.xo.oxstnewqaa,"

”i was ”
"eoegqo.k.fwettdgx.gqmgesgbbqxoqxpkyettlnaol␣fobrlakptfkogoe␣t.nppm␣zzolu␣r"

”indeed”
"bp␣v.m,qm.␣ya␣vqtyvm.wgjacklaofqev␣tumspsl␣odwcos.fxgvjqy,dvgqke␣pkli,zqt"

”i have”
"yzmyxnhswzan.tzy.,ysznyildc,qisncnri,yc,gckyeqtj.yncucyscazzsasuysqimybz.z"

”it was”
"qoacksoqfqpa␣iqfdpxpqkur.pnfziopkffqo,owfufxacdqshmeigvj,pqq,oqfiwq,uijptocodqzydqwk

The alphabet is "abcdefghijklmnopqrstuvwxyz .,"