

MATH 470 Homework 1

1. Fred Formal often starts his e-mails with "Hi". Eve, who knows Fred uses an affine cipher, intercepts his encrypted e-mail. The first 3 letters of the codetext are AHR. Can you reconstruct Fred's key?
2. Ciphertext3 came from a Vigenere cipher. You have to determine the keyword. The "correct" answer should consist of the keyword + your work in how this was obtained. I assume you used some code to do this and possibly some "obvious observations". Part of the assignment is to convince a third party (here the grader) that you have actually cracked the code. Thus you should include all supporting evidence.

oiiqrmljtlwdowboewikcehesbjmlvpbhxyeaedmylyqvvhxsmhfilauctsunyvdmtau
oghnonafhxwxabufeqaihbjtctuaflzbxbeewaabklmkmoqmtmfekatewpechcqrervf
klcuxuoytumlrzustyaugkfhxfqakvzemoaulhzdglmrefmlezgcajupaldsuloaflyok
larelesklmdbskblmktixeufrmburoktqdtafavrqlbohvsmslpoaejupaldslaulel
zjhfoibxakpfymvparatonntmhzflrhepngllxzqslzbtbhlrhxlvpbhxyerxtmiglp
vnszekhnlxaackfbttumlrzusnzunzatalaqcauuqnlgnmpxtalunolzbtvzoyateivxy
tsbhtiqtbjoiioqrtyaugkfhxtudyprtxlztajqnmbodybufhxwalrhxpahnempocbwtek
lzckfbtbvzulleadlkwhypwapohvvztkvxselfxyeuuzfimbfihupeilzdbusogdtivo
xemaqrhmfhxrqypvddbzgsxkpelwutxatilpypkvheflztivxytsbhtiqtbjoiioqrivr
tapetrwqrxtmiglpptyfitsxyobxnxyymbelfoyyqqlzcrhzaefeilaqcauuqnletavgg
aatildmsnupiljavxyqdnufiateehfegpzemlqnmoogagr

[there are no spaces in the ciphertext - just there for printing purposes.]

3. Assume that ciphertext1 came from a substitution cipher, can you decrypt it? Note that the spaces have been preserved - **never** a good idea - you can see how much easier this makes the problem
[See next pages for text and a frequency analysis which I have provided].
4. Rather than when all spaces have been removed as in ciphertext2. Can you break this one?
[See next pages for text and a frequency analysis which I have provided].

Problems 3 and 4 are for you enjoyment, no need to hand them in.

Ciphertext1

mvg gchnagtm ubhdt bu tgehgm lhamapw hgfjahgs nammng dbhg mvcp rgp cps rcrgh mvg dcap
 encttaecn earvgh mqrqt chg mhcptrbtamabp earvght lvaev hgchhpcpwg mvg bhsgh bu ngmmght
 ap c dgttcwg cps tjomamjmabp earvght lvaev tqtmgdcmaecnnq hgrnceg ngmmght bh whbjrt bu
 ngmmght lamv bmvgh ngmmght bh whbjrt bu ngmmght oq hgrnceapw gcev ngmmgh lamv mvg bpg
 ubnnblapw am ap mvg cnrvcoqm tadrng xghtabpt bu gamvgh buughgs nammng ebpuasgpmacnamq
 cps tmann sb pbm cp gchnq tjomamjmabp earvgh lct mvg ecgtch earvgh ap lvaev gcev ngmmgh
 ap mvg rncapmgzm lct hgrncegs oq c ngmmgh tbdg uazgs pjdogh bu rbtamabpt ujhmvgh sblp mvg
 cnrvcoqm am lct pcdgs cumgh yjnajt ecgtch lvb at hgrbhms mb vcxg jtgs am lamv c tvaum bu
 mvhgg mb ebddjpaecmg lamv vat wgpghcnt sjhapw vat danamchq ecdrcawpt

Letter, doublet and triplet frequencies for this codetext

| letters | doublets | triplets |
|---------|----------|----------|
| g 85 | gh 23 | mvgh 11 |
| m 70 | vg 17 | ght 9 |
| a 57 | am 17 | mgh 9 |
| h 52 | mv 17 | ngm 8 |
| c 47 | gm 15 | mmg 8 |
| t 45 | mg 13 | gmm 8 |
| v 37 | hg 12 | vgh 8 |
| b 36 | ma 12 | amv 5 |
| p 33 | ng 11 | abp 5 |
| n 33 | mm 10 | arv 5 |
| e 23 | ap 10 | ear 5 |
| r 22 | ht 9 | rvg 5 |
| u 16 | bu 8 | rnc 4 |
| s 15 | gc 8 | lam 4 |
| j 14 | bp 8 | tbu 4 |
| l 14 | cp 7 | grn 4 |
| d 13 | cn 7 | apw 4 |
| w 10 | tb 7 | nam 4 |
| q 8 | ch 7 | mab 4 |
| o 7 | rv 7 | ama 4 |
| x 2 | gs 7 | hgr 4 |
| z 2 | ae 6 | |
| f 1 | ec 6 | |
| y 1 | ea 6 | |
| i 0 | ta 6 | |
| k 0 | va 6 | |

Ciphertext2

leeqdrtjmntfjxmntoqepcdtemcbmntfjtdfocjlmndtmlykmcmtkmmcmntutjxecmqjcbqdr
 jgtlmntjklmktbocgjldteqdrjtffjycertvjlmnteckcqlhqtgjfpqymfogjldteqdrtkol
 epleagmntgjldtocymfjzlcmlefocelentatjcbbfvkptjlucmlfefocbblmkplulkfjkrfmn
 gjldtcepegfegjldtfeytmntgjldtocymfjzlcmlefekfomvfeqdrtkcjtiefvemntlajtcmt
 kmyfddfepululkfjgcepbtckmyfddfedqbmgbtycertofqephqlyibxnfvtutjlmntgjldtoc
 ymfjzlcmlefekjtefmgiefvemntqktfomnttqyblptcecbafjlmndatetjcbbxjthqljtkdqyn
 btkkycbyqbcmlfemncegocymfjleamntmvfeqdrtkmntoqepcdtemcbmntfjtdtekqjtkmncm
 cplmlutcepqbmgblycmlutcjlmndtmlyoqeymlfekcjtyfdgbtmtbxtmtjdletprxmntlj
 ucqtkfemntgfvtjkfogjldteqdrtkmntmntfjtdvcktkktemlcbbxoljkmngjfutprxtqyblp
 rqqmntoljkmqbbcepyfjjtymgjffovckrxycjbojltpljlynacqkk

Letter, doublet and triplet frequencies for this codetext

| letters | doublets | triplets |
|---------|------------|----------|
| t 87 | mn 25 lf 6 | mnt 18 |
| m 67 | jl 21 ef 6 | gjl 8 |
| j 58 | nt 18 tf 6 | ldt 8 |
| l 57 | tj 15 tc 6 | jld 8 |
| e 51 | fj 13 le 6 | eqd 7 |
| c 50 | dt 13 lu 5 | qdr 7 |
| f 48 | fe 13 qe 5 | drt 7 |
| k 35 | ml 13 ut 5 | rtj 7 |
| d 32 | jt 12 ly 5 | lfe 6 |
| b 30 | cm 11 bb 5 | dte 6 |
| q 29 | gj 11 mf 5 | cml 6 |
| n 28 | cb 10 kf 5 | mlf 6 |
| y 25 | te 10 lj 5 | fjl 5 |
| o 23 | ep 9 yc 5 | ymf 5 |
| p 20 | km 9 fv 5 | tjk 5 |
| g 15 | rt 9 tg 5 | cbb 4 |
| r 14 | ce 9 yf 4 | jkm 4 |
| v 10 | oc 8 qb 4 | emn 4 |
| x 9 | jk 8 bl 4 | cep 4 |
| u 9 | fo 8 bx 4 | mfj 4 |
| a 7 | em 8 bt 4 | tgj 4 |
| z 3 | ld 8 ek 4 | jlm 4 |
| i 3 | lm 8 bm 4 | tfj 4 |
| h 3 | mt 7 mc 4 | ntf 4 |
| s 0 | ym 7 oq 4 | lmn 4 |
| w 0 | tm 7 kt 4 | kmn 4 |
| | tk 7 jc 4 | ocy 4 |
| | qd 7 jf 4 | ntg 4 |
| | eq 7 ck 4 | cym 4 |
| | to 7 pl 4 | |
| | dr 7 qy 4 | |
| | cj 6 kc 4 | |