

Tugas Kecil II (Tucil II) IF3058 Kriptografi Sem. II Tahun 2010/2011
Kriptanalisis Sederhana dengan Metode Analisis Frekuensi dan Metode Kasiski

Batas pengumpulan : Kamis, 10 Februari 2011, pada jam kuliah Kriptografi
Tempat pengumpulan : Ruang Kuliah (7606), Pukul 11.00
Berkas pengumpulan : Kertas A4
Anggota kelompok : 2 orang

Yang dikumpulkan adalah: laporan sederhana yang berisi

- Berkas cipherteks
- Langkah-langkah yang anda lakukan dalam melakukan dekripsi
- Plainteks hasil dekripsi

I. Teknik Analisis Frekuensi pada Cipher Abjad-Tunggal

Agen FBI dari divisi *The X-Files* yang bernama Fox Mulder dan Dana Scully menemukan sebuah dokumen rahasia di kediaman korban pembunuhan. Sayangnya dokumen rahasia itu dalam bentuk terenkripsi. Kedua detektif ini meminta bantuan anda sebagai seorang kriptanalisis untuk mendekripsi dokumen tersebut. Informasi tambahan yang diketahui adalah dokumen tersebut aslinya dalam Bahasa Inggris dan dienkripsi dengan ***cipher substitusi abjad-tunggal***. Pada proses enkripsi ini, orang tersebut hanya mengubah karakter abjad (a..z). Karakter lain (angka, spasi, koma, titik, dan lain-lain) dibiarkan (tidak dienkripsi).

Anda sebagai penerima dokumen harus mampu mendekripsi chiperteks tersebut menjadi plainteks semula meskipun anda tidak mengetahui kuncinya. Anda menggunakan kombinasi teknik analisis frekuensi dan metode terkaan untuk mendekripsi dokumen tersebut. Anda diperbolehkan menggunakan kakas bantu (coretan kertas, aplikasi Ms Excel, maupun membuat program kecil sederhana untuk menghitung frekuensi kemunculan karakter atau untuk keperluan analisis lainnya) untuk menyelesaikan masalah ini.

(*soft copy* tugas ini dapat di-*download* dari <http://www.informatika.org/~rinaldi>)

fbnlfbfswchwnbzwu

**fbnlfbfswupbwpbwpunkfbwpsnbuzqzspbfbnluchpchrwtwwjuoucwqpczfpss
okspccwjwycnknqrbznmuiwnqwebzflpccwbju.chwlhwjnwjnjzcuwsknjsowjc
wbwychwlmstszfzqipzjpcznjzjzcuufmbbwjcknbqpkcwbchwjncptswpllpbjfwuzj
wjispjyzjchwspcw1970u.rpbznmuufzjczkzfpjyluwmy-
ufzwjczkzfwalspjpcznjuvbwblmcknbvbycnwalspzjchwlnwjqwnj,vhzhunnju
lbwpypbnmjychwnbsy.**

**zj1991,qnbwchpjpypfwpkcwbchwlhwjnwjptwipj,cvnqwj,ynmitnvwbpjyypr
wfhnbwso,bwrwpswychpccwhohpytwwjqpgzjifbnlfbfswuzjwjispjyuzjfw1978m
uzjilspjgu,bnlw,hpcupjyvzbpuchwzbnjsocnnsu.qpjonchwblwnlswpbnmjychwv
nbsypbwpssunlwjsoqpgzjifbnlfbfswu.pschnmihchwfnqjnsopffwlcwyrzwvcny
ozuchpcfbnlfbfswupbwpqpj-**

qpywlhwjnwjnj,lpbpjbqpswalspjpcznju,nkcwjzjfsmyzjimknu,pbwuczsslnms
pb.

zjlpbjnbqpsfzbfswuchwucmyonkchwfbnlfzbfswlhwnqwjzupfsswyfwbwpsnio.
fwbwpsnizucufnqjnsobkwbcnchwuwuzijupupibzisolhunbspjyufplwpc.

fbnlfzbfswupbwknmjzjkzwsyu,nrwbcbww-
cnlu,pjyzjzfwpyujnv.chwopbwqnucsonkcwjknmjzjvhwpcnbnbjkzwsyu,tmchp
rwpsuntwwjknmjzjnp,c,plw(fpjns),pjytpbswo.chwopbwvnbisyvzywlhwjnq
jp,hzihszihewyzjwispjy.

hzucnbokfbnlfzbfswu

jnnjwgjnvuhvkbptfgzjhucnbochwoin.psswiwyso,chwwpbszwbwfnbywyfbn
lfzbfswzuywzfcwyzjchzu1647vnnyfmcfpsswychwqnvzji-ywrzs.

chzuzqpiwywzfcupucbjwfbwpcmbwfbwpczjipfzbfmspbywuzijzpkzwsynkfnb
j.chwswiwjyumiiwucuchpcchwkpbqwb,yzuimucwypcchwpwpiwhzuqnvwbvpuywq
pjyzjiknbhzuvnbg,zjuzucwychpchwvnmsybpchwbnhprchwyrzshzquwsklwbkn
bqchwcug.lbnlnjwjcunkchwtwszkwchpcfbnlfzbfswupbwzchwbjpcmbpssofpm
uwy,nbpbwknbqwytopuowcmjgjnvwjczczwu,nkcwjumllnbccchwzbrzwlnzjcvzc
hchzunsycpsw.zczvnbchjnczji,hnvrrwb,chpccchwzuszccswqnbwchpjpcpsw-
chwzbfmspbknbqpcznjumllnuwysopmuwytochwfbwpcmbwqpotwfnzjfywjeps
,nbqpochrwtwwjfpmuwytopjojmqtwnkjpcmbpsnbhmqpjlnbfwuwu.

pjplpbwjcsqnbwfnrjzjzjihzucnbzfpbwlnbenkfbnlfzbfswupulmtszuhwyzjch
wenmbjpsjpcmbwzj1880(bwlnymfwyzj2000).pjppcwmbufzwcucjppqwytpjy
njqwsppjllwpbucnywufbtwzpkzwsyfnjcpzjzjipjmqtwbnkfbnlfzbfswu,psnjivzch
hzuumiiwucznjchpccchwqzihchprwtwwjfpmuwyto"unqwfonsnjzfvzjypcfznj".

jncsnjipkcwbvzz,chwpbzpsumbrwouchpcvwbwtwzjiqpywnrwbspbiwbpwpun
ktbzcjzjbrwpswyunqwmjwalwfcwylhwjnqwj,mjywcfptswkbnqchwibnmjy
.vhwjchwumbrwoulhncnibplhwybzljzjifbnlunbybnmihc-
uchwuuywycwbbpzjchwobwrwpswyvhpcvwbwunnjcwqwy"fnlqpbgu",chwyzk
kwbwzczpsbzljzjinkchwfnlchpcbrwpswyzzkwbwjfwuzjchwumtunzs.chwu
wlpccwbjuvwbnmjyentwfpmuwytochwmbzwybwqjpcunkpjzfwjctmzsyjju.
pbfhpwnsnizfzsjrwuczipczjuvwbnjzuczipewy,tmc,chnmihqjlobwrznm
somjumulwfcwypbfhpwnsnizfzsuwvbwknmjy,jnfbnlfzbfswuvbwrrwbbw
fnbywy.ugwlczfupbimwchpccchwvnmsyhprwlnzjcwycnfzbfswupupqnywbjhwjn
qwjn,j,wrwjzchwzjczpslbpjguewbuhpyjncbwrwpswychwquwsrw;twszwrwbu
bwlsoyzzkwbwjcpiwjyupouzqlsotwpcvnbgzjchwqnywbjyjo.

fbnlfzbfswuuhnczjenlnqzjwfwzjchwspcw1970upuqjofzbfswutwipjllwpbjic
hbnmihnmecchwjjisuhfnmjbouzyw.cnypcw,chnmupjyunkfzbfswuhprwpllpb
wypczwupfbnuuchwvnsy,kbnqyzulppcwsnfpcznjuumfhpuchwknbqwbunrz
wcmjznj,chwmgpjyeplpj,puvwsspuchwm.u.pjyfpjyp.

1991-tpbtmbofpuwfbnlfzbfsw

chwkbucqpenb"tbwpgchbnmih"knqpcznjchpcywlpcwykbnqchwbnbizjpslpc
cwbjuvputpbtmbofpuw1991.unqwbwupbfhwbutwszwrwchpccchwtpbtmbokn

bqpcznjvpuchw"bnuwccpucnjw"cnchwmjywbucpjyzjinkchwiwnqwcxbfpcmbw
nkchwyzqwjuznjuzjchwmjzrbuw.

fbwpcnbunkfblfzbfswu

zj1991,qnbwchpjpypwfpkewbchwlhwnqwjptwipj,cvnqwjppjnmjfwyhpcechw
lhwnqwjnjnkfblfzbfswuvpupjzypwpcnmihemlnjwwrwjzjjzjplmtzjunmchpqlen
j,wjispjyzj1978.vnbsyvpbzrwcwbpjynmitnwbpjyhzukbwjyprwfhnbwobwr
wpswyhpcechwopywchzbfblfzbfswumuzjilspjgu,bnlw,hpcupjyvbwpuchwz
bnjsocnnsu.tnvwbpjyfhnbwoupcwycnbnlbcwbuchpcpuqpsisibnmlklwnlswfp
jucnqlynvjpuzdwptswpbwbnkfbnlzjuzjzjswzihc."ucnql"ynwujncqwpjmuzjich
wkwwc:uzqlswcnsucnqpgwfbnlfzbfswuhprwtwwjywnjucbpcwy.

chwlpzbtwfpqwuszihsokbmucbpcwycpcechwzbnbghpyjncbwfwzrwypuqmfhl
mtszfzcpuchwohpyhnlwy.zj1981chwofbwpcwypfblfzbfswzjphzihsorzuztswpb
wfpsswychwzjfhwucwblmjfhtnvs-
pjpwbumpbbnmjywytobnpyukbnqvhzfhfswpbrzwnkchwkzwsyzuprpsptswc
nybzwbulpuuzjito.

tnvwb'uvzkwphytwfnqwjzfbwpuzjisoumulzfnmunkhzqymwcnjnczfzjilpbczfms
pbsohzihsrwsunkbnpyqzswpiwzjchwzbfpb.wrwjcmppo,kwpbzjichpchezvzkw
umulwfewyhzqkunqwchzjwsuw,tnvwbfnjkwuuycnhwbvhpchwhpytwjynzji
pjyuntuwxmwjcszjknqwyptbzcuhjpcznjpsjwvulplwb.

tnvwbbrwpswynjcrchwqwehnywuy,vhzhfvpuchpcnkpkmb-knnc-
snjilspjgvzchbnlwpcpfbwypjyfbzfwunkwzihckwczjyqpqewbfnmsytwwpuz
ofbwpcwy.hwucpewyhp40-
knncfzbfswfnmsytwfbwpcwytoevnqwjzjpxmpbcwbnkphnmb.chwywuzijuvwb
pckzbucuzqlswfzbfswu.vhwjjwvulplwbufspzqwyhpcechwzbfswfnmsywpuzot
wwalspzjwytojpcmbpslhwnqwj,tnvwbpjyfhnbwofhnuwqnbwfnqlswalpcwbj
u.puzqlswvzbwvzchpsnl,hpjzjyynvjknqpfpl-
chwsnllnuzcnjwynrwnjwwow-
fnmsytwmuycnkfmunjpspjyqpbgenpyzjchwfbwpcznjnkucbpziheszju.

spewbywuzijunkfblfzbfswuvbwentwfnqwjzfbwpuzjisofnqlswa.yprwfhnbwowy
zwyzj1996chnmihynmitnwbhpuqpywchwnffpuznjpsfblfzbfswpubwfwjcsopu2
004-
nrwbcwjowpbupkcwbhwbwrwpswyzcwntwphnpa.tnvwbhpuupzyhpc,hpyzcjnet
wwjknbhzuwzkw'uumulzfnju,hwvnmshprwcpgwjchwufbwccnhzuywpchtwy,
jwrwbbwrwpszjichpczewpuphnpa.

fzbfswqpgwbuhprwywnjucbpcwycpccpgzjivhpcuwsk-
pllzjcwfyfbwpsnizucwalwbcuucpwpbw"mjkpgwptsw"fbnlzbfswuzlnuuzts
w.njwumfhfbwpsnizuc,i.cwbwjfwqpywj,vpukzsqwyfspzqzjichpcpfbnlzbfsw
puiwjmzjwvhwjchwjzihctwknbwchwqpgzjinkchpcfbnlzbfswtohmqqjuvpukzsq
wy.

njchwjzihcnkemso11-12,1992,pfbl-
fzbfswqpgzjifnlwzcznj,knblbzdwnkuwrwbpschnmupjylnmju(lpbcsokmjy
ytochwpbchmbgnwucswbknmjyeczj),vpuhwsyzjtwbguhzbw.chwvzjjzjwjbob
pulbnymfwytochwbbwshzfnlcwbwjjzjwwbu,muzjibnlw,lrlflw,pcbwucswpjyjsp

yywb.pjnchwbfnqlwczcnbmuwypuqpsipbywjbnswwb,plspjgpjyunqwbnlw.

chwuzdwpjyfnqlswazconkchwywuzijuywqnjucbpcwyhpcqzjqpswxmzlqwjepjy
lbwlpbpcznjumkkzfwylnbnymfwrrwjchwqnuclnqlswafbnlfzbfswywuziju.ufzw
jczkzfpqwbzfpjlmstzuhwypjpbzcfswtoqpczbzyswo(pmimuc2002,1.25),vhnucpbc
wyqpgzjifbnlfzbfswuzjewapuzj1991.hwvbnwptnmchnvwpuooczucnywrwsnlcw
hjzxmwmuzjiuzqlswcnnsuchpcfpjwpuzsoknsspcwbntuwbrwbw.hwbwlnbcwyn
j''walwbc''unmbfwuumfhpuchwvpsucbwccenmbjpsvhnhytwwjwpuzsoknssw
y,pjyqmuwypntmeholwnlswvpjccntwszwrwumlwbjpcmbpswalspjpcznjuknblh
wjnqwjpchpcpbwjncowewalspjy.

qwchnyucnfbwpcwphnpawfybnlfzbfswhprwtwwjvwss-
ynfmqwjewynjchwzjcwbjwc,chwbw'uwrwjptwizjjwbuimzyw.pfnmjewbpbimqw
jccnhnpazjizuchpcvhwbfzbfswupllwbpzjfbnlucpmbwwjnmihchpcchwofpbbo
uwwyu(puchwoynunnkcwj)uwwy-
lnyupbwmjtbngwj,vhwbwpuccpqlszjifpmuwuwwy-lnytwpgpiw.

fbnlzbfswhnpawbufnmjcwbcpczczuwpucnswprwybouwwylnyumjtbngwjymb
zjiucnqlzjipjypsunswwprwjncbpfwnkwjcbpjfwpywibwuucbpqlszjivhwjchwlsjpcu
pjyibnmjypbwtncybopjyunqwfpbwzucpgwvjvzswvpsgzji.

uwrwbpsfbnlzbfswu,spewbnhprwtwwjywcwbqzjwycntwhnpawu,vwbwpczbu
cfwbczkzwyputwzji'iwjnzjw'tofwbwpsnizucuywncchwspfgnkuwwylntywpgp
iw.wjcbocnzkzsyvzchnmcswwprzjicbpfwuzupsunwpuo,uzjfwchwbpsvpoupbw
uwrwbpscbpfguqpywtochwqpfhzwumuwycnulbpozjuwfczfzywunjchwfbnlchpcl
wnlswfpjmuw.

unqwfspzqchpcchwzbfswuqzihcuczsshprwqwbzcpupunfzpslhwnqwjnjbwipbys
wuunkchwzbswiczqpfj.wjvpiwwalwbcuhprwwalbwuuywzjcwbwuczjbuwupbfh
zjichwuhplwupjyuoqtnsuywzfcwy.

chwzbuclwnlswentwfhpbwiyvzchfbwpczjipfbnlzbfswvwbwhmjipbzpjcwjpiw
buiptnbcpgpfupjybntwbeypsnu,tnc17pjykbncqchwuc.ucwlhwjpihzfmzmbpc
wfhjzfmq,phzihufhnszjhmjipboulwzpsdzjizjpihzfmzmbw.njchwzihcnkemj
w8ch1992chwofbwpcwyp36qwcwbyzpqwcwbfbnlfzbfswzjpvhwpczswywpbud
wgwukwhwbrpb,43qzswuunmchvwucnktmyplwuc.

njuwlcwqtwb3by1992chwopllwbpwynjphmjipbzpjcruhnvpjywalnuwychwzbfsw
puphnpauhnvzjilhnucnchwkwzswytwknbpjykcwbchwzbfswvpuqpyw.pupb
wumscpbpjogpspudfn.chwnvjwbunkchwspjyhcpcchwfnlfbzbfswvpuwpcwypju
mwywchwonmjiucwbuknbku.630,000(pllna5,000mglnmjy)zjyppiwu.chwfnm
bcwrwjcmssobmswychpcchwtnouvwbnjwsobwulnjuztswnbchwypqpiwfpmuw
yzjchw36qwcwbyzpqwcwbfzbfsw,pqnmjczjicnptnmckcu.6,000(47mglnmjy).

chwofnjfsmwywchpc99%nkchwypqpiwcnchwfnlvpufpmuwytochwchnmupjy
nkrzuzcnbuchpeksnfgwycnudwkwukwhwbrpbknssnvzjichwqwyzp'ulbnqncznj
kchwzbfsw.chwkzjwvpuwrwjcmssolpzyknbtowchwcruhnvpvwbwchwnouswi
pskwu.

unqwfbnl-fzbfswlhncnibplhupbwhnpawu,fbwpcwymuzjizqpiwqpjzlmzpcznj.

ywulzcwchwkpfecpcqpjonkchwqnuicfnqlszfpcwyfbnlfzbfswufbwpcwyypbwvss
ynfmqwjcwymqjwkknbcu,unqwwjchmuzpucupbimwchpcunqwywuzijuhprw
pywibwwnkfnqlswazcochpchgmpjuvnmsyjctwptswenwpuzsobwfbwpcwnjplw
bswepsnjwzjpkzwsypcjzihc.

chwopbimwchpechwhuplwunkchwuwknbqpcznjupbwkpbennfnqlswa,pjyyzulsp
opcbwqwynmusohzihsrwsnkuoqqwcebovhzfhqpgwzewacbwqwoyzzkzfmcknb
pcwpqnkmgpjucnfbwpcwmuzjiemucuzqlshwpjycnnsu.fzbfswqpgwbubwulnjyt
ojnczjichpechwnjsocnnsjwfwuupboknblwbkwfucuoqqwcebozupqwpumbwyswjich
nknblwbncpcwyypbnmjyfpwjcbpslznclnzjc.

zj1972cvnvzcjwuuwu,pbchmbuhmccswvnnypjytbofwtjy,upcnjchwusnlwnkucp
bhzssjwbpvqbzjucwb,wjispjy,hnlzjicnfcfhpiszqlwnkchwucbpjiwmjzywjczko
wyksozjifbpcchpchyqpywchzulpcnkwjispjyymknqfffknbpsqnuccpywfyw.
zjchwszihcnkpkmsqnnj,kbnqpyzucpjfwnk100kwwc,chwopsswiwysovzcjwuuw
pspbifzbfmspbpbwbnklsjpcuchpcfnsspluwvzchzjcvwjcouwfnjyufbwpczjipfn
lfzbfsw.

fbnlknbqpcznjupbwunqwezqwpuffnqlpjzwytoutzihczjiunkmjumppsszihcupjyuc
bmfcmbyfbpkctwpqzjiuhpkcunkszihcnjcnchwkwzsychwzihetwknbw.

rwbokcwjfbnlknbqpcznjupllwpbvhwbwlnvwbkmsswoszjwuzjcwbuwfcnbchww
pbch'uqpijwezfwjwbioszjwu.chzuzunkewjpechwupqwlsfwvhwbwqwipszchfuz
cwuumfhuucnjwhwjwipbwknmjy.ynvuzjifjtwynjwvzchzjchwknbqpcznjupkc
wbchwfbnlhputwwjlsnvwyvhwjchwbpbwjnsnjwbcbpfwunklhoutzfwswrzywjf

ztwszwrchwbpwpsknbqpcznjupbwfbwpcwytochwibzyfnjufznmujwuuchpfbwpc
wunmbbwpeszcochwzbqwuupiwbwkswfcfbwpcznjpybwtzbeh.chzuswjyuzcuws
kenfbwpcznjounmjyupwpszcoppjzkwucutounmjyhpbnjzfu.chwfnjfwlcuknbc
hwhnpawylpccwbjuzupsunuwezjlsopotochwupqwfjufznmujwuupujpvpjgwjzjic
nns.bwpszcuzptnmcchwwrnsmeznjknfnjufznmujwuuzjchwpsfhwqonkczqw.

fbnlfzbfswuywuziju

wpbsowapqlswunkchzulhwjnqwjvwbwmumpssouzqlswfzbfmspbpcwbjunker
pbznmuuzdwu,vhzhfswyunqwlwnlswcnulwfmspcwchpezcvpupjpcmbpslhwnq
jnj.

tmepkewbunqwowpbuqnbwpjyqnbwswptnbpwppjyfnqlswaiwnqwbzflpccwbju
hprwwqwbiwy.

chwbwhtprwtwjqpjobwfmabbzjichwqunrbchwowpbu.

zjiwjwbps,chwpsoknbqpcznju(1970-
2000)uwwqwyenchnuwvhtwszwrwzjplpbp-
jnbqpsnbzizjnkchwzbfswucntwtpuwynjchwlbzjzlswunkupfbwyiwnqwebo.

pkewbchwlmstzfyquuznjkchwbnbizjpsfbwpcnbu,ynmipjyprw,fbnlfzbfswpf
czrcougobnfgwcy.wpfhjwvywuzijunmihecentwqnbwfnqlswachpjwpszwyw

ziju.

cnyfobnlfbzfsywuzijuhprwzjfbwpuwyzjfnqlswazcoenchwlnzjcvhwbwchwohp
rwtwfnqwpjpbcknbqzjppjnkchwquwsrwu.enhjsmjytwbi,zjpjzjcwbrzwwvzchqpb
glzsgzjicnj,ulngwptnmeczufhpjiwzjfbnlfbzfsywuziju,"zpqbpchwbrznmunk
fzbfswqpgwbuzjnchwbfmjbzww.walwfepcznjuptnmeczwuzdwpjyfnqlswazcon
kknbqpcznjuchpcpllwpbjchwmgpbwjnrwbohzih,vhwbwpuchwbpchwuhptto
snngzjibmuuzpjknbqpcznjppywchwjpcznjpsjwvu.

chwucnjwhwjiwemszpuwcvpukzbucbwlncwynj7emso,1996.zcqwpuwby900to
500kwwc,vzch151fzbfswu.emszpuwecchwcbwtswemszpuwcv,vywsokwscntchw
zjjpfswnkchwfbnlfbzfswnbqpcznjuzjchpcowpb,vpuknmjynjvzjyqzsshzsjwpbo
pcwutmba,vzseuhzbwzjemso1996.

spcwbknbqpcznju,chnuwnffmbbzjipkcwb2000,pllwpbcntwtpuwynjchwblbzjzfl
swu,jpcmbpsufzjfwupjyqpcchwqpczfuywuziju,zjfsmyzjikbpfpsu.

qpjofbnlfzbfswuhprwkzjwzjcbzfcwywcpzs,bwimspbuoqqwcbopjyfpbwkmsfnql
nuzcnj.

wswqwjecunkchbww-
yzqwjuznjpscotwfpqwqnbwbkwxmwjc,fmsqzjpczjizjulwfcfmspbzqpiwunkfmt
w-uhplwyucbmfembwu.

qpdw,fmtwpjyuxmpbwu,fnqlswaknbqpcznjvbwknmjy.jnczfwchwuzdwnkchw
nbqpcznjbspczrwcnchwlnlswsozjizjz.fbnlzssmucbpcznjuvhzhzjfsmywfpben
njfhpbfchwuhprwpsunpllwpby.

fnjcwjyzjitszwku

qnucfbzcfsntuwrwbu,pjychwufzwczkzfpzjucbwpq,pbwfnjrjzfwyhcpcfnlf
zbfswupbwjziiswunbhpawuwjizjwwbwytohmqpju,pjyzywwyqnbwpjyqnbwf
bnlknbqpcznjuhprwtwwjfspzqwytochwzbqpgwbu.chzuwalspjpcznj,umllnbcwyt
ochwynfmqwjpcznjlbnymfwytounqwfbnl-
fzbfswbhpawbu,hpuchwpyrjpcpiwnkjncbwxmzbzjichwpuumqlcznjkchwzuc
wjfwnkksozjiupmfwbunbnchwbp-owc-
mjntuwrwylhwjnqwjp.hnvrrwb,chwbpbwqjofnjcwjyzjiholnchwuwvhzfhp
uumqwhpcpcswpucunqwfbnlfzbfswupbwjnecchwlnbnymfunkqmjypjwhnpawbu
;chwuwholnchwurpbozjchwzbywibwwnkufzwczkzfbzinb,tmcpsskpscnunqw
wacwjenmeczywchwqzjucbwpq.

njwqnywbjtwswkzuchpcfnlfzbfswupbwfbwpcwytoksozjiupmfwbuspjyzjizkz
wsyupjykpccwzjzjipjwpczfbzfwzjchwbnl.hnvrrwb,chwzjfbwpuzjifnqlswazconk
knbqpcznjukbnqchw1980unjqqgwchzfnjewfcmwuwqmjszgwso.

unqwwjchmuzpucuumiwwucchwpcfnlfzbfswqpofwqpczfu,chwrumpszupcznjn
krztbpcznjnbnmjy.

pffnbyzjicnchwuholnchwuzi,chwfnqlswalpcchwjupbwcvn-
yzqwjuznjpsiwnqwbzfnbrzumpswlbwuwjpcznjnkunmjkwbxmwjzfwu,vzc

hhzihwbunmjkwbxmwjfwzwlbnymfzjiqnbwfnqlswauhplwuuzqzspbcntnchqpy
pspupjyfbnlzbfswywuziju.

pjnchwbholnchwuzuzuchpcpqpj-
qpywupcwsszczwzjwpbchnbtzczumuzjiunqwgzjynktwpq(w.i.,qzfbnvprwu)cnfbw
pcwchwywuziju.

hwpczjiucwqunkvhwpcvzchpuhnbczjcwjuwtmbucnkqzfbnvprwwjwbiofjlbny
fwvzszcziuzqzspbcnchpczjpfbnlfzbfsw.

kspccwjwyucwqunkcwjhprwchwtwjyemuctwsnvpucwq-
jnyw,pjypsunqpkwpcmbwtspfjwytmbjhnsuwzjyzfpczrwnkzjcwjuwhwpczji.

qzfbnvprwhwpczjihputwjuhvjcntwflptswklbnymfzjichwuwkkwfcu.zczul
nucmspcwytotwszwrwbunkchzuchwnbochpcchw.u.lwjcpinj'u"ucpbvpbu"lbn
bpqhpupucwsszczwflptswnkywszrbzjiumfhpqzfbnvprwtwpq.

hnvwrwb,chwbwzupbwpunjptswfnmjcwb-
pbimqwjcnchzucpezjichpcchwbbwvwjncbpfwunkumllnuwybpyzpcznjywcw
cwyzjchwfbnlzbfswu.

fbnluchpcvbwbtwjcmuzjichwqzfbnvprwcfhjzxmwhnvypssuzijunkrpbznm
bpyzpcznjupjyqzucmbwyzkkwbwfwu.chwnbzizjpsfbnluzjchwfbnlzbfswuhv
wyjntjnbqpszczwufnqlpbwycjnjbqpsfbnu,wafwlcknbtwzjiqoucwbznmusotwj
.

kmbchwbqnbw,chw"ucpbvpbu"chwnboswpyucnchwmxwucznj"vhovnm
qszcpboupcwsszczwtpqgzjilpcwbujujfbnlupfbnuuchwnbsy?"umfhpfczrzcov
nmsytwwzchwbpqpcwbnknkkzfzpslnszfo(zjvhzfhfpuchwmxwucznj"vho?"bw
qpzju)nbbpjynqpfcutotnbwy?)qszcpbolwbunjjws,vhzhfnmsytwpcjcpqnmjcn
kzbzjipqpenbpjyhzisoufwbwcvplnjwplnlmspcwypbwpu,pjyvnm
syumbwso
umtewfcchwlwblwcbpcnb(u)cnhpbuhyzufzlszjpbopfcznj.

nkewjenmcwypuwrzyjfwknbchwqouczfnbzizjnkfbnlzbfswuzuchwfnzjfyw
jfwchpcqpjofzbfswuzjchwprwtmbopbwpnkunmchwbjwjispjynffmbjwbpbjfz
wjuzczwuumfhpupbchtpbbnvunbqnmjy,vhzcwhnbuwufpbrwyzjchwfhpsghzssu,
pjyucnjwzbfswu.

nchwbywpunjchwzbnqpcznjhprwtwwjlbnuwyzjfsmywcnbjpynwu,kbwpgv
zjylpcwbuju,tpsssihcjzji,pjyunqwhzjifpsswy"lspuqprnbzfwu".pjmqt
wbkzvz
jwuuwufspzqcnhprwntuwbrwyfzbfswutwzjifbwpcwy,upozjichpczcp
gwupkwuwfnjyupjychwfnbjkpsukspczgwpkjtwzjinlwjy-
chnmihchwupffnmjcupbwpvpoujwfyncpspjyhrwjrwbtwwjumllnbcwytop
jowrzyjfwtonjychwfszqpcju'puuwbcznju.

fbnlzbfswwjchmuzpucufspzqchpcchwbpbnchwkwpcmbwunkfbnlzbfswuc
hpcmjywbmchwbnpachwnbo.chwoupochpctwjyuzjchwfnbjzjqpjofzbfswunffm
bpchwjnyw,vhzwchwkwpcwzjinkchwfnbjtohpawbulbnymfwupfbpfgpcp
jolin
zjczjchwucwq,pjyunqwfzwcjzkwfucmyzwunjplzfpsjnywutwpbchwqnmc.

psunchwoupochpckspccwjyfnbjkncwjszwuzjibnnqwyspowbu,bpchw
bchpjbpy

nqfbmuhzjiu.vhzwchwbwhprwtwwjfpuwuzjvhzftwszwrwbuywfsbwfybnlfzbf
swucntw"chwbpwpschzji",njsocntwfnjkbncjwyunnjpkcwbvzchchwlwnlswvhnfb
wpcwychwzfbfswpjyynfmqwjewychwkbpmj,chwtywjjzuumwbwqpzjuzjzulum
cw.

wswfcbnjzfwxzlqwj

chwbpwbwjmqwbnmubwlnbcunkwswfcbnjzfpjyqwfhpjzfpwxmzlqwjctbwpgzji
ynvjzjfbnlzbfswu.fpqwbpukbwxmwjcsqpskmjfczj,pjywrwjvhwjchwoynvnb,
chwbumscuqpotwnrbwalnuwy,ucbwpgwy,uqwpbwy,nbwjczbwsotspfg.rzywn
wxmzlqwjczupsunrbormsjwbptsw,pjynkcwjzlfzumluwrwbwzjcwkbwbfw.tp
ccwboybpzjzizuxmzcwfnqj,pjywrwjkbwuhlnvblpfgufpjyzw.fwsslhnpjwunke
wjkpzcennlwbpcwvzchzjpknbqpcznjmcunqwcwqwuwnbglwbkwfcsopipzjkcpwg
jnmcuzywzc.

qpjwczffnqlpuuwukbwxmwjcsotwhprwwbbpczfpssotnchzjuzywbnlknqpcznju
pjyvhwjkszojizbwfsonrbchwq.vzcjwuuwunqwcwqubwlnbccc,fwsslhnpjw,u
qngwpspbqpyuwfmbzcoywrzfwzjcwkbwbfwnbqpskmjfczjuymbzjjizhcvh
wjfbnlzbfswknbqjwpbto.chwjzihetwknbwchwplwbpjfwkchw1991tpbtmb
ofpucswewcbphwybnj),bwuzywjczjchwjwpbtorzsspiwnktbnmihcnjwalwbzjw
wyplnvwbtpfgnmcpjyqjobwuzjwucwlnbcwytpssunkfnsnmbwyszihcksozjpt
nrwchwkzwsyvhwbchwknqpcznjpcwbpjzkwucwy,psnjvzchpsnmbmqtszjijn
zuw.

II. Metode Kasiski

Lain waktu, detektif Muldr dan Scully meminta bantuan anda untuk mendekripsi pesan dengan *Vigenere Cipher* (lihat pesannya di bawah ini). Informasi yang diketahui, pesan ditulis dalam Bahasa Inggris. Anda tidak mengetahui kuncinya, namun anda diminta memecahkan pesan terenkripsi ini dengan metode Kasiski. Gunakan program *Vigenere cipher* yang anda buat minggu lalu untuk mendekripsinya dengan kunci yang benar (atau memakai program *Vigenere Cipher* yang didemokan di dalam tugas ini). Cipherteks ini dienkrpsi dengan program *CryptoHelper.jar* (tersedia di <http://www.informatika.org/~rinaldi>).

DCNEK	QZWKQ	LBWHI	TDZED	XAFPG	GKSHN	CJFYU	YPFZL	QSJWB
WRQPF	RYJQY	FWQPQ	PSITR	GQHEE	TCEBK	SHEMM	MLVPJ	OKWDZ
RAVST	CWBZE	LEPGN	KYJUH	YPVTY	HXSWY	PFZLQ	SJWTR	UGPWJ
DDUBL	HLRTA	GLNNQ	BHEEE	COEOE	EAYLL	MERKW	KDGMP	CTRUK
QFBJZ	MRWKW	EMKBV	VQAUK	PLRRD	OGAHZ	CVMSK	FADCL	QQQSG
HSMWH	JHKQL	KHQVC	JHVCW	TCOTX	VPOCW	EKQRJ	BEEEH	SKSHK
BALEG	NAOIQ	RDCNX	VWMNC	MPURM	JMCPC	WFJEK	QZWKQ	LBWHI
TDZED	XLRQX	SVYSA	NMEEI	JUYEZ	ZZDGK	WLNLG	JPGXW	HTVRL
KFDLO	PGKTT	GCWFR	YFQQG	YFFYP	GRYGM	GJVVR	DPHYT	VUKSZ
MEYNM	KCLML	YEIRJ	OCBYR	ILSLH	VTEZJ	EUUYF	ZPVFW	GZEVF
FJXIG	MEBKD	DFKAT	QZNQS	IERDG	UHEEB	XSIXX	PYSVX	LYHZP
OHENA	MIJCR	SILOR	YUMSI	QSVZN	KEFGN	PUAKB	KCLNS	LXXFF
EUYPU	DYXLW	FDWQT	TGQLL	LMERD	SIPJU	MFMLV	ZAFDF	GMRJB
EEEHS	YLVNC	WGJFS	JRKZE	QLGFS	ICOHR	ELERA	VECJU	RRYJQ
PGNWK	FWBFE	KQPSK	IRQKT	KSHAN	WGSTC	WBKSH	BMHNP	RPHSX

PQPMX	MLVZA	FDFGM	RJBEE	EHSSP	JMLOB	XYYJW	EPWQC	FLMOR
UTFFU	MPLBG	CCEBK	SHYYY	TDZLA	OIRRE	WLAEK	BAGTC	LNCVT
RULWA	VOWTC	LKMRL	CZVQX	DRZXV	RPPWT	WHEYF	WVVNK	FKDLZ
QMVLD	YCOQT	QQQSL	RRREC	ELOSC	GZVRN	DWTLQ	PNDTC	SMUAV
CHXWJ	XTVYP	SUEKQ	JWZIE	BSWKS	RGRSW	HZREC	ELODC	KXEIA
DARYB	ADLAI	UGOOG	AHMPS	GGVQZ	WJNXE	QWWME	RDSJP	DDRAV
PVQWB	UZWTC	JLHZZ	JCKPY	QLGVG	LPEBK	SHMPW	TSWRD	SKCLM
LYEIP	MQKFY	WRGFW	MKMJO	EJRRD	AVMRJ	IOGLQ	PWGNA	FLPYE
ZZIFW	GCFSY	FFDVF	FWEME	CXIKL	FOMJW	MEEPC	JZPQN	WHTCC
PVVMH	DKMWE	KPEOE	ROQ GK	TZVPU	FVLOB	JSVIN	FAFVO	RLCFH
JJFED	JAOML	WLEEB	LSFAO	QFSOI	UGOOG	AHMPW	WAZRD	BFERRA
BWQTC	YJOKT	RZQAG	GVYIO	XLCUL	WYMIQ	PQFTQ	QBLAI	GFNOJ
PEQPE	NHRRN	WRYJX	CAGRZ	LAHVP	QEGPM	CWMQF	KSHYW	KMIIW
DOJNR	ZRAGY	VBPCR	EWDYU	MEKRA	BKTRZ	UZXRZ	MQRZR	GQCHX
VZLPC	DZVFA	SLIJR	DCLRK	FFWRV	VKQOY	WHEQE	RWKN	WFFVQ
GLAII	RDSPH	HDCFX	ZVPEB	KSHMP	WTFXZ	AUZYZ	URZML	VWSSI
PDORM	TPCWB	CLYGA	PLAII	COOIP	DEMFT	FCCAL	GWDZY	LBSED
KFKSH	UPVBW	RNLSR	CDZAW	WSVQP	VZDPQ	YFMLV	PAGEZ	WTGFZ
XFRDS	TWDUK	KHJJM	IOEJZ	TMZTZ	VFWRZ	OGQVH	XVZCJ	QVDLZ
RZXFV	PIIUL	WDGSG	KCCJC	KYHOC	KLEIG	HMJNL	QLLBW	KQDOM
PGAAM	FIERA	RUPYU	YLBSE	QBFFX	WTCFH	VDGJH	YPDDC	STRUF
WJVQR	GLVLS	DCEBK	PUQQL	BRXDK	FDLWU	MFLSE	RDSJP	DRJGH
VNGPV	ZYWTC	TXVDS	ZOKCL	MLYEI	JZKIE	ODDGW	LWFDK	FKSRE
COASC	GGSKZ	EQJAX	ZVGJW	KEKQP	WBWGJ	ABKJI	GCDYS	IRDSW
TUQGF	MLZQW	FKTFX	COXPC	JKCBL	WFFWY	ETROG	LCUAS	FMREE
SVREZ	QBGDR	FUWPF	FWFFW	TVVYW	GNPOX	YKLSD	CKTKS	HYMKM
GFKIC	EWBDC	UBXVB	OHFCL	QOQXP	CYHGF	PABJG	KIKFA	PZKDD
PWMLV	MNWVD	OUIWT	PZCJG	RYGEN	SVIGM	NHRWV	MQOXP	CYOHY
PPGLV	TRVCT	DCLQM	RAHRJ	KWBPE	KULCH	JKFAP	VCPGB	SMVZY
JUCPD	XQGDR	FUJOJ	EKQBW	OMCQP	FZLQS	JWTWR	LEARR	LZYJR
EICWH	YPXEZ	GTVUM	BUVZJ	DYHAM	TLWAV	DGACK	GSKPA	QFRQU
XWMLV	ZAFDF	GMRJB	EEEHS	RYGPM	WLRFR	IOZYW	MGFTR	FDBWT
TDXDA	EIFLE	HYZZQ	TWKAZ	RDWEE	KUQAF	EXGJO	IJDDC	SFEEW
NSRWY	QOKXP	JYJRK	SHBCG	IPVYX	CRCGF	FWFLR	TAGVP	PULYE
CUGOO	GAHMP	WWAZR	DCLEH	JNDTR	RRECE	EKQZW	KQLBW	HITDZ
EDXMJ	JKQRE	HPMXY	XYCOC	LEKQY	KMIIL	YCRDW	ADLAI	LLEHV
OVFYL	XWZLP	VVLWX	YFMMT	MYSRY	ZURZB	XJYLS	OPVUL	LAIMG
YWETW	UCKHJ	SCNAL	ODYGS	FMWJK	FZODM	LVLEE	HQOEA	XQPLH
VZAKW	KNRHC	JLVFS	CVCJI	UTWAY	EBNSU	EKASK	TRUQO	ELLUQ
KAIEIJ	RDSRC	HMKSJ	LRTAP	VPQZY	EXHRD	PSITW	EZWKQ	LBWOG
PAEGF	VISCN	ALODI	YKHRT	CGBFH	QMQLA	IZQHS	FQGQT	AEWKP
AOTSH	DMMLV	VCBCK	SDFFS	OIVLO	BRCHP	QZBTJ	QWWCT	QSRGH
GCMOS	KZLFQ	KASIC	OGLCU	ASFWF	VPIIU	LDZBL	AIICW	FVSXZ
BXJHJ	MBGYT	SIPWV	OJGJH	YPZMR	WKWKF	WHJFU	DMMGH	ZR

Editlah hasil dekripsi tersebut sehingga enak dibaca, tambahkan tanda baca yang relevan jika perlu (karena program Vigenere Cipher yang digunakan mengabaikan tanda baca).

III. Kriptanalisis Playfair Cipher

Mulder dan Scully juga menemukan cipherteks yang lain yang dienkripsi dengan *Playfair Cipher*. Bantu mereka memecahkan cipherteks ini dengan menggunakan analisis frekuensi kemunculan bigram dalam Bahasa Inggris.

Catatan:

1. Cipherteks di bawah ini dalam format pdf - diambil dari sebuah *e-book*, jadi tidak bisa di-copy langsung menjadi teks. Perlu program konversi dari pdf menjadi teks, atau anda ketik secara manual ke editor teks.
2. Sedikit berbeda dengan yang diterangkan dalam kuliah, di sini disisipkan huruf "X" jika karakter di dalam bigram sama (bukan "Z" seperti yang saya jelaskan dalam kuliah. Contoh: AMBASSADOR → AM BA SS AD OR → AM BA SX SA DO RX (huruf X disisipkan jika hanya terdapat 1 huruf pada bigram terakhir)
3. Pada hasil dekripsi, penerima pesan harus membuang sembarang huruf X yang tidak memiliki makna
4. Penerima pesan juga harus menentukan apakah huruf I/J pada hasil dekripsi adalah I atau J (karena huruf J dibuang pada bujursangkatr Playfair 5 x 5)

PK QT OX OK KR QK ZX BI OZ BZ ZO EK KQ KP ZO IB ZO KG ZS VL HR
OR HY EK RK RU PH BO OW IH KR YK FW EK OI NR KR YK FW EK AF AX
AT VA KU GX OW YH VM EI FL HT QT XG AB LO LZ RH EK KU AE MF QH
AI EK HY KY QE OW IH KR UG FT ZN AI ZS FC LO TL PH TF BZ LZ RH
EK RQ OR RH OL CI ZS XL OF VD RE IK KR HR QK OD VK RO CI EK RH
RQ LO OD VK KZ LI OL NR RL KI EK HU XZ KE AF XK SI LI OW VC KU
QE FW OR HY EK HU XZ KE MW AZ EK HY FW TB KU GX ZS VL LS DS HY
EK HU XZ KE FL FU CI EK HY FW TB KU GX KR WL SD UH IC XZ KE OW
IH KR HR AF UK PH OZ BZ OW IH KR HR AF AG AT OZ BZ EK RY FT OK
FL FU CI ZS XL OF VD RE IK KR HR QK OW KY MU BO KQ RE QR YK ON
KR AF ER KA NI UK MU WF ER AF ER WM TA RA OR RH OU ZS FV LF RE
KR YK YG OW UK OW XL QE FW OR HY EK RQ OR RH OQ YH HE KR YK YG
OW UK MW AZ EK RQ OR RH SW LZ TY RO CI ZN AF XG OU ZS VL LS DS
HY EK KY KY MU BO KU EX OW IH KR HR AF UK PH OZ BZ OW IH KR HR
AF AG AT OZ BZ EK KU HQ IO XI FL FU CI ZS XL OF VD RE IK KR AF
ER EA CI RH EK KU EX QK MS EK RH HY NI IS QT VU LW RU CI UH HI
EF MK UA CI UM YG RU WF CI ZN AF XG OU ZS VL LS DS HY EK HY EF
MK UA CI SL CI OW IH KR MS EK RH HY AF ER KA KR WL SD UH XL RU
OL CI ZS XL FA EK OR ZN AF XK SI LI EK TQ ZS XL OF VD RE IK KR
SL CI ME LI LQ HP KP RE OR ZI BO KY HY QK FW ZO ZM SL ON OL CI
EH KY KU IO EK HU OW IH RL KN RU WM EA ZN NF EK UK YK XY OZ RO

BD NL HF ZO ZK IN KR FT ML TF UA XB ZO XL OW XY RN LO GX IN KR
SL CI ME LI LQ HY PH PK RO NZ IO VU OW KO QK FW ZO KX KY HY LW
DB AT XY BZ NI EK TY HT ZO XL OW IH HR YK XS RU TF BZ MW OY RN
ZN KL KY HY ZO ZN LW DB AT XY BZ NI EK TY HT ZO XL OW XV LI OL
NR RL NZ RN LO ZS IS FL CI EK RH RQ LO HP TQ ZO MS CI EK RH RQ
LO ZA TW ZO ZK KR EK FT XI FL FU CI ZS XL OF VD RE IK KR HR QK
OD VK KO ZO EK KY KY MU BO TU IR KR XB IE UO QE FW OR RE KR FL
FD TA ZR KR OZ VK RO CI UH KI EK RP UK HM RU XG OX ZB OK AZ FW
BX RU OU BO OW XI FL XU OW XF RU KA OW VD RE IK KR GW HU XZ KE
OX ON KR YK YG OW UK AI EK KU EX NI ZX PH OD VK NI ON KR YK FW
EK OW XY RN LO GX SZ LI RF YH RN SZ HR OR OD VK KO EK KP HR OR
RH OD VK KI NI ZS PH TW EK HY UF OW IH KR UH XG UK HA XZ KE IK
SZ LZ RH ON KR OZ VK EK RU SO AZ LF RE KR OK FW XK LI UK KI EK
RP ZO EK KY KY MU BO TU IR KR XB IE SZ DZ HU XZ KE IO EK KY RU