Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas I IF5054 Kriptografi Sem. I Tahun 2006/2007
Kriptanalisis Sederhana

Batas pengumpulan : Kamis, 14 September 2006, pada jam kuliah Kriptografi
Tempat pengumpulan : Ruang Kuliah (7602), Pukul 13.00
Berkas pengumpulan : Kertas A4

I. Teknik Analisis Frekuensi

Detektif Sherlock Holmes mengirimkan dokumen kepada anda, tetapi sayangnya ia mengenkripsi dokumen dalam bahasa Inggris tersebut menjadi chiperteks 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) tidak dienkripsi.

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

Yang dikumpulkan adalah: laporan yang berisi
a. Berkas cipherteks
b. Langkah-langkah yang anda lakukan dalam melakukan dekripsi
c. Plainteks hasil dekripsi

(soft copynya dapat di-*download* dari http://www.informatika.org/~rinaldi)

```
xnznriknaavekvntecwkxnkebwgagbfrwct--
nlvna?avnnpekexwtgkxavek?avnaelewtb
gljvwtejtb?

tvegkbaelbtntvebeqrebtwnkb,gkxhrbtgfnrtgkzntvelznrywovtjgletngbigfnrthg
igltg'bvwbtnlz,jgkfeeksnrkxwktvekeatvlee-
mncryeekbwicnpexwghgigltg:jrctrlegkxvelwtgoe,
cgrkjvexaexkebxgzkwovtgtjwtzvgccfztvehgigltgjrctrlgcgkxyrberygoekjz.

tveekjzjcnpexwgwbjrllektcznkczgmgwcgfcewkfgvgbgwkxnkebwggkxwbkntsnlbgce
.hrbt500jnpwebvgmefeekplwktexgkxawccfexwbtlwfrtextnbjvnncbgkxcwflglweb.

hgigltg'bvwbtnlzgkxjrctrlgcbwteb,wypnltgktsworleb,cwtelgtrle,glt,ekmwln
kyekt,gljvwtejtrlegkxemeksnnxglejnmelexwktvetvleemncryeb,xecwmelwkowkte
lebtwkowkbwovtbtntvebnjwgcpgbtnstvejwtz.

tvevntecwkxnkebwgwkjektlgchgigltg,snleugypce,vgbgcgloeektlzxexwjgtextnw
tbvwbtnlz.v.w.,gbtvevntecwbynlejnyynkcziknak,agbtveswlbtcrurlzwktelkgtw
nkgcvntecwk
wkxnkebwg.wtagbfrwctwk1959rbwkolepglgtwnksrkxbslnyhgpgk.bneiglkn,plebwx
```

```
ektgttvetwye,nsswjwgccznpekextvevntecnkgro.5,1962.

gyelwjgkgljvwtejtbgfecgkxaekxzbnlekbekxebwokextvevntecwktvetvekpnprcglw
ktelkgtwnkgcbtzce.

xrlwkowtbvezxgzfesnletvekeanlxelelg,v.w.agbtvenkczfrwcxwkowktvejwtzkntt
ncnbepnaelxrlwkofcgjinrtb.gkxgttvefeowkkwkonstvekeanlxel,wtagbpnprcglaw
tvtveaegctvwebtpenpcewktvejwtzgkxfejgyetveygwkyeetwkopcgjenshgigltg'bbn
jwgcwteb.

tvehgmglnny,tvevntec'blebtgrlgkt,agbsgynrbsnlwtbsnnx,wkjcrxwkotlgxwtwnk
gcfcgjitrflrijnssee,fgllgyrkxwbtegibgkxlwjepnllwxoe.

wtagbtvebnltnspcgjetvgtpenpcexlebbexrptnontn--
xlebbeb,brwtbgkxfgtwibvwltbaeletvejnxe.wktveywx'70btvevntecagbavelepenp
ceaekttnagtjvaebtelkynmweb,avwjvvgxfeekfgkkexrkxeltvencxnlxelleowye.

frttvevntecwbhrbtnkensvrkxlexbnstnpwjbwktveekjzjcnpexwg,avwjvjnyebawtvf
ntvjncnlgkxfcgjigkxavwtewccrbtlgtwnkb.

"tvebefnnibgletveswlbtnstvewliwkx.vnpesrccztvezawccferbesrc.aeglexwbtlw
frtwkotveytnyexwgjnypgkweb,exrjgtwnkgcwkbtwtrtwnkb,jrctrlgcwkbtwtrtwnkb
,tvekgtwnkgccwflglzgkxygkzntvelb,"bgwxhgigltgjrctrlgcgkxyrberygoekjzveg
xgrlnlgtgyfrkgkgttvecgrkjv.

bvebgwxtvebjvnncbwkhgigltgtvgtaelelgkiextvevwovebtgjgxeywjgcczanrcxleje
wmejnpwebnstveekjzjcnpexwggkxgxxextvgttvejwtzgxywkwbtlgtwnk,avwjvvncxbt
vefnnib'jnpzlwovt,vgxvecpextvegoekjzfzplnmwxwkosrkxb,lebegljvelbgkxalwt
elb.

"tvwbswlbtexwtwnkwbnkczgmgwcgfceeujcrbwmecz(slnyrb).frtvnpesrcczwkawtvt
vebejnkxexwtwnkaeawccfegfcetnjnnpelgteawtvgknrtbwxeprfcwbvelgkxbecctvef
nnibjnyyeljwgccz,"grlnlgbgwx.

"aeiknaaeyrbtvgmeygxebnyeywbtgieb,brjvgbtzpnolgpvwjgcellnlb,wktvefnnib,
bntvebejnkxexwtwnkawccfeyrjvfettel,"bvegxxex.

bvebgwxwtagbvnpextveekjzjcnpexwganrcxyntwmgtevwbtnlwgkbgkxlebegljvelbtn
anlivglxel.

onmelknlbrtwznbnbgwxwkvwbbpeejvgttvecgrkjvtvgtfetgawbkeexextnfeynlewkmn
cmexwktvewltlgxwtwnkgcjrctrlenlwtanrcxfejnyeeutwkjt.

vegxxextvgtvetvnrovtbnyenstvewljrctrlgcbzyfncb,brjvgbnkxec-
nkxec,tvevrygksworlebyegkttnaglxnssfgxcrji,keexextnfewyplnmex.

"avzxn(nkxec-nkxec)vgmetncnnibnrocz?"vebgwx.

awcceye.yercekfelo,tvekeaczgppnwktexxeprtzxwlejtnlnselgbyrbvrwbwkhgiglt
g,bgwxtveekjzjcnpexwganrcxfegbwokwswjgktgxxwtwnktntvesnrkxgtwnk'bcwflgl
z.

"gctvnrovwjgk'tlegxfgvgbgwkxnkebwg,wiknatvgtygkz(ntvel)xrtjvjgk.tvebeaw
ccfeankxelsrcsnltvnbeavnglewktelebtexwkwkxnkebwg'bpgbtgkxtveketvelcgkxb
'vwbtnlzwkhgigltg,"vebgwx.
```

II. *Vigenere Cipher*

Lain waktu, detektif Sherlock Holmes mengirimi anda pesan yang dienkripsi dengan *Vigenere Cipher* (lihat pesannya di bawah ini). Anda tidak mengetahui kuncinya, namun anda bisa menentukan panjang kunci dengan metode Kasiski, lalu gunakan analisis frekuensi untuk menentukan kata kunci, kemudian dekripsi cipherteks tersebut!

```
SSQYN ASXES RBFOR SOUYK VTAKO QVKSZ WOQSF VNOBB BRWKB BRCQS
QSOSF WJYSX FHKYS YGODI FSUMD BJJOD FQCWN IBSDO HSPBW XBDIL
MWQGP FZNVD DOSGO NEZSB JJSBQ FSXUW QOIOZ VLBIN TSBTP VBKUV
OXKOJ KDFMZ UCUBB DVITS PKTHC ZPZCB FWZVZ YCLMW HJOSO VBQCE
SGSSO BIWCS FDISC BZOBN DFMZU CUBBD VIORS NJHWY OBSGZ CFUTD
FSOUS BWSFV BUAOO SNOTO ZPSSR FBBCY SGQRP HDKVZ OXEJO XTHCX
FGQYU HVKOR PYPYC PBDDV JSRMS MDDPU FKQVM MSQDB FGGBP GSXLS
BXFHV OMSAO OHOBZ BIWCS FDISC BZOBN JHGKQ DZSDO HSPBG LPGHY
OORNJ GCXXS GVFMF YTWBQ NWQRB SZSND ZONSB DJBUO MZWZU WQMVF
JODFM ZUCUB BDVIH FSOOK WMIAO XOWBQ TAWDI FWMIO FNJBH OSBSD
DFMZU CUBBD VICCG DPBON EWGYO KSCMS MCUOZ VJBUC XWZVJ OAMSM
DDPUF KQVMK ORBOU KCBLG SMVFW DZBRO EWHSP BIZQS FCBRR VFFWF
FFDBF BHSDS VKMZG DFDSX TCBXF OZMSM DDPBC WJQCX OSKIP FYZFF
SXOWO VUFOZ QSKKE SOXEK OCIWB QUCBV BKFOO QSSOH FYEIQ DJCBD
PQFIQ HCQSO DRZKW DIQCN JBUDI SCBZI DZFFG KERZO SWJOS DFOOH
WMFVO VMKOI OSFZF HSBEW GKQDS KSWBQ DFMZU CUBBD VIDVS CUBID
IWZVB DDBPT SCTWC XBZ
```