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

Tugas I IF5054 Kriptografi Sem. I Tahun 2007/2008
Kriptanalisis Sederhana

Batas pengumpulan : Kamis, 6 September 2007, pada jam kuliah Kriptografi
Tempat pengumpulan : Ruang Kuliah (7602), Pukul 13.00
Berkas pengumpulan : Kertas A4

I. Teknik Analisis Frekuensi

Agen FBI, Fox Muller 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 kriptanalis 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 mengggunakan 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.

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

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

```
nwnbngeapndkazietregtltwaujnplnmtrtnb

nbyprg-snrgzsnpjnplnmtrtnbhnjetregtltwrhtapndkazizcrhtnwnbnge
ngepgsterhnrdenjhtwgsfnrtejzccjypnftjgnrrhtjrnerzcrhtutnetsezyrtcezbjye
nanunrzbnsnwz.rhtapndkazigjhzvtrzetltnprhtdnyjtjzcrhtons.1nddgwtsrrhnrk
gpptwnpp102vtzvptzsaznew."rhtrtnbhnjjyddttwtwgsjnplnmgsmrhtapndkazi,fhg
dhdzsjgjrjzcrhtcpgmhrwnrnnswdzdkvgrlzgdtetdzewtejcezbrhtazrrzbzcrhtbnot
stjtn(ftjrjypnftjg),"snrgzsnprensjvzernrgzsjnctrudzbbgjjgzsdhngebnsrnrn
smkyesgnwgjngwhtetrytjwnu.gsltjrgmnrzejatpgtltrhnrrhtetdzewtejnetjrgpp'
etnwnapt'wtjvgrtstneputgmhrbzsrhjyswtefnrte."ayrgrfgpprnktbzsrhjczetivt
erjnrrhtsnrgzsnprensjvzernrgzsjnctruaznewgsfnjhgsmrzs,y.j.,rznsnpuxtrht
gsczebnrgzs."y.j.ltjjtpdzbvnsuvhztsgigsrtesnrgzsnpnjjgjrtwrhtrtnbfgrhne
zazrgdjnplnmgsmjujrtb,rnrnsmjngw,njrhtdzbvnsuhnwnpetnwuhnwtivtegtsdtgs
etregtlgsmbydhpnemtegrtbj,jydhnjjyabnegstjnswhtpgdzvrtej.rhtgswzstjgnss
nluhnwvetlgzyjpuregtwrzcgswrhtazi,ayrwgwszrhnltrhtstdtjjneutqygvbtsr.
rhtcpgmhrwnrnetdzewtenswdzdkvgrlzgdtetdzewteftetczyswnazyr30rz50btrtejc
ezbtndhzrhtenrwtvrhjzc2,000btrtejnsw1,900btrtejetjvtdrgltpu.grrzzkrhtez
azrjnezyswrhetthzyejrzetryesrhtbrzrhtaznr.azrhetdzewtej,fhgdhftetaezymh
randkrzrhtjhgvzsbzswnunswrytjwnu,ftetgbbtwgnrtpugbbtejtwgsndzsrngstezcf
nrtegszewterzkttvrhtbcysdrgzsgsm.rhtapndkazifgppatjhgvvtwrzrhty.j.cezbb
```

```
nknjjnevzergsjzyrhjypnftjg.rhtjnplnmtrtnb,fhgdhdzsjgjrjzcvtejzsstpcezbr
hty.j.ngedencrbnsycndryeteaztgsmnswrhtctwtenpnlgnrgzsnwbgsgjrenrgzsnbzs
mzrhtej,wgjdzltetwbzetwtaegjcezbrhtdenjhtw737-
400,ayrszhybnsetbngsjzerhtvpnst'jdzdkvgr.rhtgswzstjgnsmzltesbtsrhnjjvts
rnezyswev20agppgzs(bzetrhnsyj$2bgppgzs)rzcgswrhtapndkazi.nwnbngedhngebn
snwnbn.jyhtebns,hzftlte,jngwrhnrrhtrzrnpdzjrzcrhtvezotdrfnjnezysw$3bgpp
gzs."fthnlts'rdnpdypnrtwrhtdzjrrhnr(zyedzbvnsu)sttwjrzvnuutr."rensjvzer
nrgzsbgsgjrteoyjbnsjuncggwonbnpjngwrhnrcgswgsmrhtdnyjtzcrhtcngpyetfnjgb
vzernsrgszewterzvetltsrcyryetnddgwtsrj.njregsmzcngevpnstnddgwtsrjgsgswz
stjgn,gsdpywgsmnmneywngswzstjgnotrpgstedenjhgsuzmunknerngsbnedhrhnrkgpp
tw21,hnltvezbvrtwrhttyezvtnsysgzsrzvezhgagrgswzstjgnsngepgstjcezbcpugsm
gstyngejvndt.nwtptmnrgzscezbgswzstjgngjdyeetsrpugsaeyjjtpj,atpmgyb,rzdz
slgsdttydzysreubtbatejrhnrpzdnpdglgpnlgnrgzsnyrhzegrgtjhnltbnwtjnctrugb
vezltbtsrj.
```

II. *Vigenere Cipher*

Lain waktu, detektif Mulder da Scully meminta bantuan anda untuk mendekripsi pesan 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!

```
SUAJZ XOSBL JTYDH TOKPS VJMGE SSRWV VEQZW MSEOU ALNHN
UJLPR IGBHC YVTTX XBNTO GZRGN JTYDH TOMZC NZKAL GYOUI
DEBLB APTBZ IEWUA GZXNL VVAXZ NGAML OALUJ LPRIG BBZNN
IBBGI GOMLH EEKNH NUFYM WLTGN MOLNN RJTOA PKVMP RNTLT
TRRJT BGEOE BOCIF ZIMPR HTBXW EIOAB ZNFZI MTOAZ PXPIT
NBUZS FIPTL SGXWG ZMRXA PSOPU VWFCG KLMSE BHAXC VNZQH
YSNOL MSELC MKPSN ZQLQI RJIEE HBAOA EHRZM EPSPU XXDWR
XMHYL LKNYP CGODX EEASQ GFTRY QGEOG NMIPA XUNMS EGUBT
WLHTI KPCYO XLPWV ZPMCA SLQVM APQMW FPBTM DTLBS MMPRN
RWGRT UKZHL DYKIW TNTZW MSEBH AXCVN ZWKJA FZZHY OZKZL
HEEKN HCCRJ BHDHN XMMSE IOFXY TRRML NOCKE BEHIO ABEOE
YWUDE EBIMT OAYEX CEPUV WFCGK LTEOC ZPXGA AGTUL DNIMG
EEEHG NDIAM BPZCR RMLER BTBXW EFIWI PSNTL HYEJO TETAZ
UXMTC FSMTD UEOVZ EWRTB RNMNT LLPVR TKFTN QOIFP TRXZX
DPRIB BGEYE QMHAF ZPXDE PUVWE IZKIL ERBTW FPRFN IWTNI
OBXOT UKXNM LVIBH LNRBM GEAAJ IEWOJ KLBET BHZHL DPGAM
WIIKW GEVNL BXCTU KXKPV VUCLX AEYNN WLZUW GAHRT WFPNB
TWGLU TAAML GRMMK VAYUV ZCEFO LXYTE OVWLC NSMPT TUYQQ
ZFUKZ KZOZS IMPSO EXNML VIJND TBCQM YEFYB APSCK KMLCY
K
```

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