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

Tugas I IF3058 Kriptografi Sem. II Tahun 2008/2009
Kriptanalisis Sederhana

Batas pengumpulan : Jumat, 20 Februari 2009, pada jam kuliah Kriptografi
Tempat pengumpulan : Ruang Kuliah (7606), Pukul 8.00
Berkas pengumpulan : Kertas A4
Anggota kelompok : 2 orang

I. Teknik Analisis Frekuensi

Agen FBI, Fox Muller dan Dana Scully -- dua tokoh utama di dalam film *The X Files* -- 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)

```
wugoftvkeaffxnodmumbovnnlopudmnbtdnapfavrtkfadvuvzmntvruvztnnlomntnuavr
ombunonloctdvuvzm,howuojuvznltntfudtewofuzlnltbbovtvrfkndtuvfuzlnmnuwwt
ddujonantgofoavnlortuwkndubnawavrav.ctneluvznlocotnlodaxnbxntvrntwguvzn
aeawwotzxomclaftrounuvnanloappueo,unctmewotdnltncocodooiboduoveuvztvxvx
mxtwojovn.rombunonlomntnofovnmnltnunctmnlocadmnmvacptwwuvmaxnl-otmn
ovzwtvrpad18kotdm,unctmvanxvnuwnlumfadvuvznltnudotwumornloftzvunxroapmv
acnltnltrptwwov.avfkqaxdvokpdafnlogovneatmnnlotfaxvnapmvacwkuvzqxmnuved
otmortvrzanroobodxbxvnuwnlobauvnclodonlondtegmcodovanjumuhwoavnlowuvomn
ltnltrvanhoovewotdor.komnodrtkftvkeafbtdumavmcodoftrocunlanlodoxdabotve
axvnduom,clarombunonloudbdawavzorcuvnodmtvrlotjkmvacptwweavnuvxonadxvnl
oudbxhwuendtvmbadntvrzanacadg.utmmxfonltnupconaaoiboduoveornlomooindofo
eavrunuavmdozxwtdwknlokcaxwrhoeafonlo"vadf"tvrcocaxwreaboptdhonnod.
nlopadoetmnmpdafnlohhecotnlodeovndotnnloovrapwtmncoogeavntuvorotdwkfovn
uavmapnlobanovnutwpadmvacptwwnlumcoog.mboeutwzdtbluemcodoeaffummuavortm
"tnnovnuavzonnodm"naftgomxdonltnnlobanovnutwpadmvacctmbdomovnorewotdwk.
tmnlopadoetmnhoetfofadoeodntuvtedammnlocoogovr,nlozdtbluemcodoxmoroinov
mujowktmnlooinovnapnlomvacptwwhoetfoojurovn.nlocotnlodeovndonartkumtluj
oaptenujunk,cunlojodkavopoowuvznlooppoenmapnlohxmkrtkkomnodrtk.ueoummnu
wwtbanovnutwbdahwofuvftvktdotmtmmvacfownmrxduvznlortktvrpdoosomajodvuzl
```

```
n(nofbodtnxdomuvmafodxdtwtdotmpowwna-
8ewtmnvuzln).avnabapnlumcotdoctneluvznlopadoetmnewamowk.umbagonaftnnntk
wad,hhehdatretmnfonoadawazumn,otdwuodthaxnnloaxnwaag.lomturnltnnlocuvnd
kcotnlodcaxwrwtmnxvnuwnlocoogovrtvrmafobtdnmapnloeaxvndkcaxwrmoopxdnlod
mvacptwwwotruvznarumdxbnuav.unumropuvunowkcadnlgoobuvzuvnaxelcunlnlopad
oetmnavnowojumuav,dtruatvravwuvo,tmcoltjoewotdwkvanmoovnloovrnanlumbtdn
uexwtdmbowwapeawrcotnlodkon.
```

II. *Vigenere Cipher*

Lain waktu, detektif Mulder dan Scully meminta bantuan anda untuk mendekripsi pesan dengan *Vigenere Cipher* (lihat pesannya di bawah ini). Informasi yang diketahui, pesa ditulis dalam Bahasa Inggris. 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!

```
XEQYZ ROYAX OBBID IYKQG XEEOD WYKWR YKJVZ WBZEB PNENP
CMRZE QFOBG KPHPY VRZDI YQQEK IEXLM ERAAC XQAME SERQF
CDEYS BPUIE DDWPR ENVSV TCENP QTNYO EDKBN LKRXK TEKYE
ADQBT ETDZW YOPEE YUNQA SFBMG NWTER MEOIO QIWHX CLLCA
VYHOH OZGNW NERIG UBTSO XRXOO YIWHX ACWSV XOJGH SBUZD
EZDPR XZAJS ENYWT LMPVT ASPXM JEAAC BMPKL TTYVU UOTPN
JLZDE DDIGK XRZKL PGOTP BKPZR AEDWN YPIYQ BVSAT SOKPZ
REIOK HZEVP CNNTJ EOKKE UOSER MEUKM HSBUZ DETBE VTAGW
KAFKO HPVLB APAEK JBAPW LSAGR AVPVU NQENR SBVSL ODCQO
RAFZB IAEKF FCBBM ATZEZ TRWSD OAYUS ECDPN TPHPS ZFZDE
JGWAZ DEAYT VZANP CAOGP TWOJH ZZOYD KBTBU DOMGO MUPDB
RCETS KTNIG OQKUO OPIZX BUOOY PKZPI PVTCX YGJNT XOGUK
PPXZH YOILX IAJWR LLQPR WNREI TKYHL XVRRO RPZWE ZOAWC
WFGUT SKBGN ASEKB RXQNY OEFGC EYMGK OJHFK PNYLL LXAGU
OTLBB HVETD YEAOJ TPBVN ZEOYK TAKSS NRIAT ALNRQ AGESO
OBRXI IYOLG ULRZT MPZET DYEAO IAROI AJLEC CXRIP IGOIF
LWRLC QGIWN DYBUO OCZEV GXUST WITKI AVOZF SWYMO QAZAR
PCBRJ ENERM EKOUW DABLW NZZQA OKNAY TYIKN OEKGK ZFZBB
UKXBN GWERZ SPBDV IATSO XBRHS FQORY PSERI GMHOM KTNZP
IEELR YPOHK ZQYYH TXINT ZRFCA VGWRP GWEYA TSKVG NAYHO
ZRGUE LBITU WLERW HMDCW OIERU TSOZR GNELR CTKJU XLMEU
BCLFM NZOTZ DPEUS AEKAV TCLPZ WYRSH TMPGG GEDLZ BGZCZ
XKYAO IZXAS XKMLV QZOPE OXCZH ARZPQ AZARG SMJYW STWAH
XAMLX GBLUO FGQYR XEVOM AZKTP VTZKX UERWJ ZDEHY ZYJOE
PCKUO JALXL UUSCS SVNYA EDDPR CKRWN UNZPE CACVZ AAMSB
NTWMP BQPGJ WCSBR XFODR CNQQR WKVGF ECVQW RYPHC YCTNO
OXOWS IDIYK AVSWG PWIXO JGPPN BXPST XPVYX OZUKU GNMZP
NRTOI GOPBC YHTXI FYKFE ZWJKN IDDZN TOFZB UVTCT SOEBX
HDERM JXETP BTVYP SERMG NENRC BUGPC SSVNY ZOYOQ AUNDP
BBBCE NQBQR TZSLB WHTZT SOEBX HDTDA RTZEO LWEJA ROSAC
APEDG QGNET DXMVM DBZEZ FOPPW KGFGJ ANDQI KLACD QAMHO
MKTVT OTTDC GOKND CCPNW SERMH TWNOD PRCKR WNBEG ZEZBO
NTEZL DQBTE TOYMF TPIYD MEBAN PEVVR WTPBI YRUIY YBUKN
CZEVG XEEDS VGKNN LVENX OAYNQ GYPOA ZMQLQ NOSVT SWOTC
```

```
BFZUL PBMIU HUESW AYWLZ XOGOI ELQWZ XGUCV IAZVI NUIYY
KACQC RYPHL DKUOJ ADWWQ KHOQK CGNKR TDIEO WNNKX VZWLT
CUCXK VTNMF GPEXZ BVTCA WDMET WTTFM GUCOG OZASA NECCA
YQRPY NGNAB PXMSO PSZPE RYPEC XAGEH EOOUB INANI BUKYH
TXMFK COGOZ ASANE RIFIK MPEXJ OPHLZ PEGOE EYMKV HATXE
UGPIE CLBOJ GLXLJ NUNZY VRTAE OGWEX UHPZQ AMFUP AQCKW
CPPCY XESPR IIKYH TXIFK BFZBB FCKNJ YCBBA R
```

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