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

Tugas Kecil II (Tucil II) IF3058 Kriptografi Sem. II Tahun 2009/2010
Kriptanalisis Sederhana dengan Metode Analisis Frekuensi dan Metode Kasiski

---

Batas pengumpulan : Kamis, 18 Februari 2010, pada jam kuliah Kriptografi
Tempat pengumpulan : Ruang Kuliah (7606), Pukul 11.00
Berkas pengumpulan : Kertas A4
Anggota kelompok : 2 orang

## I. Teknik Analisis Frekuensi

Detektif terkenal Sherlock Holmes 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)

pcpsw:lmcpuhpbgzjonmbcpjg

chweplpjwuwhprwpsvpousnrwykbwuhkzuh.tmcchwvpcwbufsnuwcneplpjhprwjnchwsyqpjokzuhknbywfpywu.uncnkwwychweplpjwuwlnlmspcznj,kzuhzjitnpcuinctziiwbpjyvwjckpbchwbchpjwrwb.chwkpbchwbchwkzuhwbqwjvwjc,chwsnjiwbzccnngcntbzjizjchwkzuh.
zkchwbwcmbjcbzlcnngqnbwchpjpkwvypou,chwkzuhvwbwjnckbwuh.chweplpjwuwyzyjncszgwchwcpucw.cnunsrwchzulbntswq,kzuhzjifnqlpjzwuzjucpsswykbwwdwbunjchwzbtnpcu.chwovnmsyfpcfhchwkzuhpjykbwwdwchwqpcuwp.kbwwdwbupssnvwychwtnpcucninkpbchwbpjyucposnjiwb.hnvwrwb,chweplpjwuwfnmsycpucwchwyzkkwbwjfwtwcvwwjkbwuhpjykbndwjpjychwoyzyjncszgwkbndwjkzuh.

chwkbndwjkzuhtbnmihcpsnvwblbzfw.unkzuhzjifnqlpjzwuzjucpsswykzuhcpjgu.chwovnmsyfpcfhchwkzuhpjyucmkkchwqzjchwcpjgu,kzjcnkzj.pkcwbpszccswchbpuhzjipbnmjy,chwkzuhucnllwyqnrzji.chwovwbwczbwypjyymss,tmcpszrw.mjknbcmjpcwso,chweplpjwuwfnmsyuczsscpucwchwyzkkwbwjfw.

twfpmuwchwkzuhyzyjncqnrwknbypou,chwosnucchwzbkbwuh-kzuhcpucw.chweplpjwuwlbwkwbbwychwszrwsocpucwnkkbwuhkzuh,jncusmiizuhkzuh.unhnvyzyeplpjwuwkzuhzjifnqlpjzwuunsrwchzulbntswq?hnvynchwoiwckbwuh-cpuczjikzuhcneplpj?zkonmvwbwfnjumsczjichwkzuhzjymucbo,vhpcvnmsyonmbwfnqqwjy?

puunnjpuonmbwpfhonmbinpsu,umfhpukzjyzjipvnjywbkmsqpcw,ucpbczjipumffwuukmsfnqlpjo,lpozjinkkonmbywtcunbvhpcwrwb,onmqzihcsnuwonmblpuuznj.onmynj'cjwwycnvnbgunhpbyunonmbwspa.onmwalwbzwjfwchwupqwlbntswqpusnccwbovzjjwbuvhnvpucwchwzbqnjwo,vwpschohwzbuvhnjwrwbibnvmlpjytnbwyhnqwqpgwbuvhniwcpyyzfcwycnlbwufbzlcznjybmiu.

Szgwchweplpjwuwkzuhlbntswq,chwtwucunsmcznjzuuzqlsw.zcvpuntuwbrwytos.bnjhmttpbyzjchwwpbsojzjwcwwjkzkco'u."qpjchbzrwu,nyysowjnmih,njsozjchwlbwuwjfwnkpfhpsswjizjiwjrzbnjqwjc."-s.bnjhmttpby.

chwtwjwkzcunkpfhpsswjiw:
chwqnbwzjcwssziwjc,lwbuzucwjcpjyfnqlwcwjconmpbw,chwqnbwonmwjenopinnylbntswq.zkonmbfhpsswjiwupbwchwfnbbwfcuzdw,pjyzkonmpbwucwpyzsofnjxmwbzjichnuwfhpsswjiwu,onmpbwhpllo.onmchzjgnkonmbfhpsswjiwupjyiwcwjwbizdwy.onmpbwwafzcwycncbojwvunsmcznju.onmhprwkmj.onmpbwpszrw!

hnveplpjwuwkzuhucpokbwuh:
cngwwlchwkzuhcpuczjikbwuh,chweplpjwuwkzuhzjifnqlpjzwuuczsslmcchwkzuhzjchwcpjgu.tmcjnvchwopyypuqpssuhpbgcnwpfhcpjg.chwuhpbgwpcupkwvkzuh,tmcqnucnkchwkzuhpbbzrwzjprwboszrwsoucpcw.chwkzuhpbwfhpsswjiwy.

bwfnqqwjypcznju:
zjucwpynkprnzyzjifhpsswjiwu,emqlzjcnchwq.twpcchwhwfgnmcnkchwq.wjenochwipqw.zkonmbfhpsswjiwupbwcnnspbiwnbcnnjmqwbnmu,ynjncizrwml.kpzszjiqpgwuonmczbwy.zjucwpy,bwnbipjzdw.kzjyqnbwywcwbqzjpcznj,qnbwgjnvswyiw,qnbwhwsl.

zkonmhprwqwconmbinpsu,uwcunqwtziiwbinpsu.
njfwonmqwwconmblwbunjpsnbkpqzsojwwyu,qnrwnjcninpsuknbonmbibnml,chwunfzwco,wrwjqpjgzjy.ynj'cfbwpcwumffwuupjyszwzjzc.onmhprwbwunmbfwu,ugzssupjyptzszczwucnqpgwpyzkkwbwjfw.un,lmcpuhpbgzjonmbcpjgpjyuwwhnvkpbonmfpjbwpssoin!

## II. Metode Kasiski

Lain waktu, detektif Sherlock Holmes 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 bisa menentukan panjang kunci dengan metode Kasiski, lalu gunakan analisis frekuensi untuk menentukan kata kunci, kemudian dekripsi cipherteks tersebut! 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 dienkripsi dengan program *CryptoHelper.jar* (tersedia di `http://www.informatika.org/~rinaldi`).

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| UCBNO | QIEFA | GGUNE | RPLJG | LPNZV | GZPHP | PRNVV | RUWIJ | CNRTU |
| HAPEW | LPNCY | WKTCG | XHIKJ | URICN | ACCVU | TYXAI | MISNY | ZBAGK |
| KUZZR | SCTZP | YDERT | BZUNH | APCVJ | WDLNR | HWIVB | PTYKZ | KAMPV |
| VPGVC | LDOCF | VZEEY | ADGLJ | WEWUM | KAZVC | YGKJQ | JTYXA | IMISN |
| YNOLP | BIAQL | SZPAG | KLTNX | KARYU | GEIAJ | VCOEI | WWTRP | XSERX |
| MENSD | CVPMN | JYYMP | RTRPY | MEXCV | KQFLN | UKBNC | MDUTJ | IKJLT |
| LCKVX | OIXEE | VNFTG | JMZPL | RPXXY | JQCCU | OVLLU | IZFNS | EIGNC |
| GWEIF | PWWVB | PSLPA | YKHPO | EVPVU | HZWPJ | QDCFL | YRPXV | CEDWR |
| UNFTM | FKCWT | ZMYLG | CKBKG | LTNXF | QROIY | DRPIV | UNSEK | KKRPX |
| DPZTQ | KWUWE | ORMIK | YYCVV | PVUCR | HKYIJ | UIDTL | PVZPA | SETQC |
| CFIYL | PVPZP | ETNKK | UVYIC | NGJZR | UYDIJ | VPZUN | SEJVI | ZTQLY |
| KQPVC | PPNKJ | MVZJP | RZGVT | GBLSC | GLKQU | YEOJQ | SKNTO | EQNGC |
| CYTZP | OJHLZ | MWKNK | GYYTY | QNRWA | FSKVP | IQORH | WKNKG | YYTYQ |
| NJGJE | EDDMI | CNEHV | MWDCH | PKRHQ | EGUCT | XCTCG | LJIEW | JLFMF |
| KCWAR | KXSIJ | DZZGZ | UOLTV | VANZN | VRICJ | UOEEN | QXJNP | NVFPZ |
| OBPWV | PBKJY | CERHB | VTUET | VPLZP | AEHVD | QVPHL | LVZQR | TNPVV |
| PBZPV | LNXNI | UGMSI | KYIJC | MSOIV | DZUCE | BLVQK | NYQTD | GEZVB |
| DODCV | POYXO | ICJCG | YIPVT | QVPWP | SNKBY | YBTCY | VWVPB | LNTGU |
| PCLEI | JVQTE | LPAKK | WEUBP | SRKLN | KNSIE | VPIGY | OAPUW | WTYEU |
| IPQEI | MFKCW | KIGUE | EUCJF | WNZNV | JCEFL | PDJMM | KEBPS | RDWLV |
| YYTZT | MCAHP | WJWJA | GWESZ | HQEKM | SEUCT | CVBPW | FTSRV | BZMVJ |
| MJCCO | FFTPZ | OHPPR | NIEFC | ESGGW | GNYLR | VUBZN | FQICN | MUYCE |
| HDAAK | GLJSL | TZFWH | OEUDG | DQOYT | RKVJE | UAPVF | EZVBP | TVTVR |
| NMYON | UVVRU | WRVOI | ZPMLH | VCDVP | CYIKU | XCCWP | OEVWG | QZEHV |
| YWINX | DUBNC | JCCOW | YKTVV | BPCFW | VKTSH | AJEWC | FMEIW | HIEFM |
| PRVPM | ZVQLS | WKTCG | XHIKJ | IJGWC | EKCMJ | VBPTZ | EJVCO | EYZYI |
| JKGAR | VUAVF | VJKRV | URPXF | NVRIC | UWLPZ | VICVB | PCZVG | ZUBZM |
| VVWEW | GPRFW | ASWXO | HZUBR | PXSIE | FCKGG | ALVUQ | WGFEL | ZMMZY |
| UDAKJ | WDGCY | BRNQY | GMLIU | JMWGF | EHRRX | PCHOT | ICVHW | CWWYG |
| VMKMT | TZPOK | JYDEG | NITGM | ZFNQZ | JJCAE | JRMTK | UWLPR | ZRACY |
| GRVJL | FXSAE | KSRMU | YTRUC | BNODE | ENQXJ | NPNDG | VKKMN | LVCZC |
| AGLNZ | HMJVC | YHZUT | RVYDT | NQZBE | IXPRT | MUVIS | IJRZV | XCZUJ |
| EZVCN | TOEUQ | KKMZB | MKWLU | BPHRU | CEFYC | GFPMR | FLLMR | VQTEB |
| LNXGE | YKFPH | ZUMRT | FTEIY | WIMWZ | NTGVK | TUEEU | QVKJY | QEDCT |
| VHICM | YKADQ | MERVE | MEVCD | NFYIE | KGLTV | FEZVB | XEUKB | RVCGE |
| RPLJR | CCIKW | ICVBP | MVUIE | FIMJV | EBJFY | AITVQ | EIQZM | VPALM |
| FFAUO | QKVYO | WRUVF | VUMUI | FMEVB | PRVYM | IGMZM | RPGZF | YLSXQ |
| QEINS | RFWOY | OSSER | FEYGH | TWRPB | VFNZC | IGIKG | UHOIM | EZVBL |
| FVOIC | GNSED | GPVUU | TDEQE | YQQPV | VTPVJ | UDTFE | WEVYX | PCCBV |
| KNCEH | WQIGM | LLFVU | FTYPN | VTOPR | UEIVP | KVCHO | PVTAV | XYCAE |
| EMYGM | LIUDM | TCODE | YKAJW | VUETV | LVOUY | DVFVF | UNLNU | CZUHI |
| CMFTK | FOJZS | ZVQFP | MFKCW | ARKXS | EYCLK | JCYKV | ZBIGG | PLPJI |
| IFNZP | IQLLE | YQRFO | PZUGT | NUCVU | JCDHV | CZKHI | CSLMT | LELPA |
| KKVXT | YAEKK | BZXYQ | OIOAR | PXNOC | QZJYU | DIEFC | CICYG | YKUJG |
| FQIKY | IJCET | NUQNY | GUWIE | IXIQW | PSJJM | JCCOH | ZUKLT | LPNKY |
| WIMMC | EGTMJ | GHETY | GBICH | DFFTU | RVCZN | FHPZU | CYNVT | JVKHR |
| HZUEF | TEPNK | KBCGX | UEACS | FTZZO | KRZZP | NDAKY | WYWHO | RVFKD |
| DSLHL | PLIGX | NMDKF | VFGPD | ZCWEE | UYVRU | QJFIX | IECBV | FQTTY |
| AMCNI | HAEFW | ICHRE | KJMNQ | LVIJE | WDHIC | TZPOJ | AGMOC | KHZPA |
| EHVPM | MGLPN | UKVXL | IFREG | GKQNS | EJVIK | GIQMF | MAYCF | TBVTI |
| KKIYA | EFVZT | PLNRJ | MRXYY | IKKAR | NMZAN | CGKQN | SEDQU | VPNZF |
| KTCKJ | UYOKJ | MIYIC | KGKVX | ICCTV | DQEII | YTYGM | UIYZF | KJMIC |

```
PTNVC UZZYO MVFQR QHNAE XIJUB ZWJVE FTUGI EGAWC WTNXG
ITJIE HVTGV NFZWZ UPICS DSYKV VDYEW VGVKJ YEWFT IMKHP
SRUQW RLZMZ UQEIB ZPVCV UGHWI XJBVP GPNKK VDGGZ RZLIE
WUCIA CVLCL JMVOW IAMFK CWXIG MPNKU IWKAF RRVQM GJLTK
GZEKH EHVHW IOIQA SQFYG JLIEV ARPIM STWZV HCRUI GQEUC
OEKJM SQRLS ZHPVJ COEJC UPUNP RPVPZ UJLIE VQEIB LSXKD
VPGPA JYMVV GPMFT GJWEW UNKVE GLZFK JMGJC WIGOW ITCDC
GQXVP VTEEP ICGUY DKJMZ PXZFF QLRTN LWRTL JUUTD JWSCW
UWSFF QJRFL YJUMM GLLLR VBICW EIMGE FTEDE EVQKN YOADC
VUCCL MRPLR KCLNU CURPX LIZKN VCNFR ZPORN UXAEF IWNIH
EIUBY GNTTC GQJYL ZNXKB ZUMFP GQAVF NZBVC TROUY DRPWK
CGLNU CPVUU TDKQI TEIXP RPGKJ YPXYK JZVCZ NJWSC WWZLC
CJFTU EEUYQ KJUCT ZUBEA IXAEU CICQS OTTMR VYOAJ RMTKU
WDRPK VRYCF FTUVF UEAEF IIQOY DKJMX CFWEI AQEJC DCYQZ
VQACA GJGJW LLTIK MUVIN AGVCI GNSEW GMCKH RAEFB YGUEM
FUXYG LPOWP MGCFL SVZXV TCPNT GLSAM FKCWJ VHICE GGZWQ
LXIEI ALMFF PRKVK GXDUI CASQX JTIGI KKHRI KNQBG UNAEX
IJKHE HVFIE EYDUI CJVIC YSKQE RNEEH VRIKJ MZFKJ MIKWP
FZGTU PYLRK JMXCF WEIAP ZUVZD PUERA MMERW BZHOW LPQVR
PIAEE CQIUN LGVCA ICSDO WUCEU CWHFW MKVYS IDCAK JYDUE
UMKUC YTYGE VUNDU ICEIC JDHZU JFFSH IKJIC QHRBC CKBEF
ZTYCV UDYRI EUBFF UYCVX QXQLZ UJNGZ JUGEU TMROY OOWYW
IMCYG KQOVV BPRNK BYUOC AWQZJ WWSAC QVXVC XEJWS CWMLI
UUCBN ODWFT SZUNS AKQNG GLDOE CTTJU YGVCV FPAZI EIQDC
ATNRV QMGUY DTTMR VCGEG TWTGM DIWCA RPUCT ZUBJW EWUEG
DVTZT NUUPZ UJPRJ QVRNU AEOJM NKFWC FPBZP OPTFG VAQSE
HVUMR TWS
```

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

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