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

Tugas Kecil II (Tucil II) IF3058 Kriptografi Sem. II Tahun 2011/2012
Kriptanalisis Sederhana dengan Metode Analisis Frekuensi dan Metode Kasiski

---

Batas pengumpulan	:	Rabu, 15 Februari 2011, pada jam kuliah Kriptografi
Tempat pengumpulan	:	Ruang Kuliah (7606), Pukul 12.00
Berkas pengumpulan	:	Kertas A4
Anggota kelompok	:	2 orang

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

I. Teknik Analisis Frekuensi pada Cipher Abjad-Tunggal

Detektif Sherlock Holmes menemukan sebuah dokumen rahasia di kediaman agen spionase. Sayangnya dokumen rahasia itu dalam bentuk terenkripsi. Sherlock Holmes 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**. Semua angka sudah ditulis dalam kata-kata. Pada proses enkripsi ini, orang tersebut hanya mengubah karakter abjad (a..z). Karakter lain (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.

(*soft copy* tugas ini dapat di-*download* dari http://informatika.stei.itb.ac.id/~rinaldi.munir)

```
znlcxkrxbczwfewknafjnjynfjl

yhknjpczwexlckwawjcxbczwnawfpwl,vflcnjpbkxecznkcrczxhlfjy
cxcwjczxhlfjyrwfklfpx,fjhjywklwfknypwowcqwwjlnowknffjyfvf
lsfwewkpwlbkxeczwlwf.sjxqjflczwowknjpvfjyoknypw,ncvnwlgfk
cvrlxhczxbczwnawafg.ncywuwvxglflcwggw-
vnswwaxvxprxbpkfllvfjyl,pkfdwyorvfkpwfjnefvllhazflzxklwl,
kwnjywwkfjywuwjefeexcz.

pkfyhfvvr,njefjrlwgfkfcwnjahklnxjl,czwzhjcwk-
pfczwkwklxbczwlnowknfjlcwggwlghklhwczwnkgkwrfakxllczwvfjy
oknypwfjynjcxfewknaf.qzwjczwewvcnjpnawlhoewkpwlczwoknypw,
foxhccwjczxhlfjyrwfklfpx,czwlwjxkczwflcflnfjlowaxewnlxvfc
wyflczwfoxknpnjfvfewknafjl.
```

czwlnowknfjzhjcwk-
pfczwkwklgkxofovrefswczwnkqfrfvxjpczwjxkczaxflcxbfvflsffj
yyxqjczkxhpzczwufvvwrxbczwefaswjdnwknuwk.fkazfwxvxpnafvwu
nywjawlzxqlczfcorfoxhcbnbcwwjczxhlfjylrwfklfpxczwawjckfvg
vfnjlxbfewknaffkwqnywvrnjzfoncwy.ckfawlxbzhefjfacnuncrfcc
znlcnewfkwgkwlwkuwynjczwkwefksfovwvfokwfcfkgncnjvxlfjpwvw
l.czwpvfanfvaxjyncnxjlbhkczwkjxkczewfjczfcczwawjckfvgvfnj
lfkwfccznlcnewaxxvfjyexnlc.

yhknjpczwjwicbnuwczxhlfjyrwfkl,qznvwczwpvfanfvgwknxyaxjcn
jhwl,zhefjlgwjwckfcwbfknjcxlxhczfewknaf.

czwkwckwfcxbczwnawafgl(lwwnawfpwl)efswljxkczwkjkwpnxjlnja
kwflnjpvrzfoncfovwoxczbxkvfkpwfjnefvlfjybxkczwzhefjlqzxgk
wrxjczwe.orwnpzcczxhlfjyrwfklfpxzhjcwk-
pfczwkwklzfuwexuwyhgczwwflcwkjlnywxbczwaxjcnjwjcnjcxjwqbx
hjyvfjyfjyczwgkfnknwgkxunjawlxbafjfyf.

bkxefoxhclwuwjczxhlfjyrwfklfpxzhefjpkxhglfyfgccxczwaxjync
nxjlxbczwjxkczwkjaxflcxbafjfyf,vnunjpefnjvrflzhjcwklxblwf
efeefvl.czwrlgkwfypkfyhfvvrwflcqfkylfvxjpczwwypwxbczwfkac
naankavw,wuwjchfvvrkwfaznjppkwwjvfjy.czwlwzfkynwlcxbfvvzh
efjlwccvwkllhkunuwcxyfrflczwwlsnex(xk,njczwnkxqjjfewbxkcz
welwvuwl,njhnc-ewfjnjplnegvr'czwgwxgvw').

czwahvcnufcnxjxbakxglnjfewknafowpnjlnjczwcwzhfafjufvvwr,l
xhczwflcxbczwgkwlwjc-
yfrewinaxancr.lthflzfjyaznvnfkwczwwfkvnwlcgvfjclcxowpkxqj
-lxxjbxvvxqwyoraxkj(xkefndw)fjyczwjorowfjlfjypxhkyl.

czwlwfkwfvvlgwanwlqznazjwwycxownjynunyhfvvrgvfjcwy,kfczwk
czfjczwnklwwylownjplafccwkwyxklxqjxuwkokxswjpkxhjy.cznlnl
fynlcnjacnxjxbnegxkcfjawnjfewknafjznlcxkr,bxkczwkwfkwjxfj
nefvlnjfewknaffccznlcnewlckxjpwjxhpzcxghvvfgvxhpz.

fcbnklcczwlwakxglewkwvrlhggvwewjcczwbxxygkxyhawyorzhjcnjp
fjypfczwknjp.ohcorczkwwczxhlfjyoaczwgwxgvwxbcznlfkwffkwlw
ccvwyfpknahvchkfvnlcl.njcznlywuwvxgewjcczwrfkwbxvvxqwyorc
zwzhjcwk-
pfczwkwklxblxhczfewknaffjyczwj,axjlnywkfovrvfcwk,orlxewnj
czwjxkczwkjgfkcxbczwaxjcnjwjc.

czwwfkvnwlcsjxqjlwccvwyaxeehjncrnjlxhczfewknafnlfczhfafgk
nwcf,fcczwexhczxbczwaznafefknuwknjgwkh.orfoxhccqxczxhlfjy
lfjybnuwzhjykwyoaczwgwxgvwzwkwzfuwflrwcjxaxkj,ohcczwrahvc
nufcwlthflz,pxhkylfjyaznvn.czwrfvlxpkxqaxccxj,bkxeqznazcz
wrqwfuwfaxfklwavxcz.

czwwfkvnwlcanunvndfcnxjnjfewknafywuwvxglnjczwaxflcfvkwpnx
jlxbczwphvbxbewinax.yfcnjpbkxefkxhjycqwvuwczxhlfjyoa,ncnl
czwfaznwuwewjcxbczwxvewagwxgvw.czwnkahvchkwnlaxjcwegxkfkr

qnczerawjfwfjyczwckxmfjqfk,qnczczwlgkwfyxbczwfkrfjlczkxhp
zjxkczwkjnjynffjyqnczczwlzfjpyrjflcrnjaznjf.fcfggkxinefcw
vrczwlfewcnewczwzwokwqlfkwexunjpbkxewprgcczkxhpzlnjfncxqf
kylczwgkxenlwyvfjyxbafjffj.

czwxvewalkwgkwlwjcczwowpnjjnjpxbanunvndfcnxjnjawjckfvfewk
naf.czwrfkwbxvvxqwy,foxhcczkwwawjchknwlvfcwk,orczwwfkvnwl
canunvndfcnxjxblxhczfewknaf-czwazfunjahvchkwxbgwkh.

czwlwcqxbnklcfewknafjanunvndfcnxjl,njewinaxfjygwkh,lwcfgf
ccwkjqznazqnvvvflcbxkexkwczfjcqxczxhlfjyrwfkl.flhaawllnxj
xbznpzvrywuwvxgwyahvchkwl,fvvlckxjpvrnjbvhwjawyorczwckfyn
cnxjlxbczwnkgkwywawllxkl,bxvvxqlnjczwlfewcqxvnencwykwpnxj
lxbczwaxjcnjwjc-
njawjckfvfewknaf(fvlxsjxqjflewlxfewknaf)fjynjczwlckngxbvf
jyowcqwwjczwfjywlfjyczwgfanbna.

fkazfwxvxprgkxunywlwunywjawxbczwlwufknxhlahvchkwl,ohcczwx
jvrxjwlsjxqjfoxhcnjfjrpkwfcywcfnvfkwczxlwlhkununjpqzwjczw
lgfjnfkylfkknuw-
cxefkuwvfjyywlckxr.czwlwfkwczwuwkrfjanwjcefrf,fjyczwkwvfc
nuwvrhglcfkcyxenjfjcahvchkwlxbczwcnew,czwfdcwalfjyczwnjaf
l.

czwxknpnjfvgwxgvwxbjxkczfewknafvnuwnjfqnywkfjpwxbwjunkxje
wjcl.xjczwwflclnywxbczwaxjcnjwjcczwkwfkwqxxyvfjyl,qzwkwcz
wrsnvvwvsfjyywwk.xjczwpkfllgvfnjlxbczwenyqwlcczwrzhjccxwi
cnjacnxjlwuwkfvfewknafjlgwanwl,njavhynjpczwafewv,efeexczf
jyzxklw.njczwywlwkckwpnxjlxbczwlxhczqwlczhefjlholnlcwjawy
wgwjylxjlefvvwkfjnefvlfjypfczwkwylwwyl.njczwfkacnajxkcz,q
zwkwczwkwnluwkrehazexkwzhjcnjpczfjpfczwknjp,bnlzfjylwfvlf
kwgvwjcnbhv.

czwbnklcckfawxblwccvwyunvvfpwvnbwnlnjczwlxhczqwlc,qzwkwor
czwlwaxjyenvvwjjnheoapxhkyl,lthflzfjyaxkj(xkefndw)fkwahvc
nufcwy(lwwzhjcwk-pfczwkwkl).

czwjfcnuwlxbcznlkwpnxjywknuwczwnkakxglbkxeczwexkwfyufjawy
anunvndfcnxjcxczwlxhcz,njewinax.czwlfewahvchkfvnjbvhwjawo
knjplfahlcxewuwjchfvvrlzfkwyorefjrxbczwcknowl,czfcxbexhjy
ohnvynjp.bkxefoxhcczxhlfjyoapkwfcohknfvexhjylowpnjcxowaxj
lckhacwyfkxhjycxeoazfeowklxbvxpxkqxxy.

czwwfkvnwlcohknfvexhjylnjjxkczfewknaffkwczxlwxbczwfywjfah
vchkwxbczwxznxufvvwr,avxlwvrbxvvxqwyorjwfkorzxgwqwvvcknow
l.czwgwknxyxbpkwfcwlcfacnuncrnlbkxeczwbnklcawjchkroacxczw
bnbczawjchkrfy,orqznazcnewfuflcjheowkxbexhjylzfuwowwjohnv
cczkxhpzxhcjxkczfewknaf.

yhknjpfjyfbcwkcznlgwknxycqxkwpnxjlxbjxkczfewknafywuwvxgth
ncwfyufjawybfkenjplxanwcnwl-
czwenllnllngnufvvwrfjyczwlxhczqwlc.bfkenjp,faaxegfjnwyoru

```
nvvfpwvnbw,lgkwfylhgczwwflcaxflc,qzwkwbnwvylfkwavwfkwybkx
eczwqxxyvfjylbxkczwgvfjcnjpxbefndw.ohcnjexlcgfkclxbczwaxj
cnjwjcczwcknowlaxjcnjhwcxvnuwflwen-
jxefynawinlcwjaw,njczwckfyncnxjfvefjjwkxbzhjcwk-
pfczwkwkl,wuwjczxhpzczwrvfasczwxjwfjnefvqznazefswlexuwewj
cxjczwgvfnjlwflr.

zhjcwycxwicnjacnxjnjfewknaf,cznlhlwbhvakwfchkwqnvvxjvrowa
xewfufnvfovwfpfnjcxczwnjynfjlczkxhpzczwwuwjcqznazywlckxrl
czwnkqfrxbvnbw.czwlgfjnfkylfkknuwqnczzxklwl.

czwfkknufvxbaxvheohlnjxjwczxhlfjybxhkzhjykwyfjyjnjwcr-
cqxnlfynlflcwkbxkczwxknpnjfvnjzfoncfjclxbczwfewknafjaxjcn
jwjc.czwaznwbfpwjcxbczwnkyxqjbfvvnlynlwflw.qnczjxkwlnlcfj
awcxjwqpwkel,cknowlkfgnyvrlhaaheocxhjbfenvnfknvvjwllwlxjc
zwnkbnklcoknwbaxjcfacqnczwhkxgwfjl-
njefjraflwluflcvrkwyhanjpczwjheowkxbczwfewknafjlqnczxhcfj
rxjwwuwjbnknjpflzxc.

qzwkwczwcknowlywuwvxgfavxlwkkwvfcnxjlzngqnczczwjwqfkknufv
l,czwrfkwbkwthwjcvrcknaswy,cxkewjcwyfjyefllfakwyorczwnkun
lncxkl.cqxwvwewjclefswczwwhkxgwfjloxczlckxjpfjykhczvwll-
czwnkgxllwllnxjxbphjl,fjyfjhjlzfsfovwaxjunacnxjnjczwknpzc
jwllxbczwnkazknlcnfjafhlw.

czwwuwjcxbxjwczxhlfjybxhkzhjykwyfjyjnjwcr-
cqxczwonppwlcchkjnjpgxnjcnjczwznlcxkrxbfewknaf,zflzfyczww
hkxawjcknawbbwacxbywbnjnjpczfcznlcxkrnjcwkelxbcznlxjwexew
jc.znlcxknfjlywlaknowczwgkwunxhlfewknafjahvchkwlflgkw-
axvheonfj.fjyczwxknpnjfvgwxgvwxbczwaxjcnjwjcowaxewsjxqjfl
njynfjl,lnegvrowafhlwaxvheohlnlhjywkczwnvvhlnxjczfczwzflk
wfazwyczwnjynwl.

njkwawjcrwfkl'jfcnuwfewknafjl'zflaxewnjcxhlwflfjfvcwkjfcn
uwjfew.ohcncnlfenlvwfynjpgzkflw-
ewfjnjp,ohcbfnvnjpcxlfr,foxknpnjfvxknjynpwjxhlfewknafjl.n
jlgncwxbnclthnksrxknpnjl,fewknafjnjynfjlkwefnjlczwexkwynk
wacfjylnegvwcwke.
```

II. Metode Kasiski

Sekali lagi detektif Sherlock Holmes meminta bantuan anda untuk mmecahkan pesan yang dienkripsi dengan *Vigenere Cipher* (lihat pesannya di bawah ini). Informasi yang diketahui hanyalah pesan ditulis dalam Bahasa Inggris. Anda tidak mengetahui kuncinya, namun anda diminta memecahkan pesan terenkripsi ini dengan metode Kasiski. Gunakan program *Vigenere cipher* standard yang anda buat minggu lalu untuk mendekripsinya dengan kunci yang benar (atau memakai program *Vigenere Cipher* yang didemokan di dalam tugas ini).

Plainteks dienkripsi dengan program *CryptoHelper.jar* (tersedia di `http://informatika.stei.itb.ac.id/~rinaldi.munir`).

EHYIK	VRMPO	SIYQK	PPAEH	YKQEI	EUZMI	KQJRM	VFSUG	OMVNA
DINXE	AZTOT	NYZKT	KOYQO	LMTEK	MHETY	KQPJE	DSELX	URKHL
HOLEP	XYAUE	HYZDI	RTWJR	UFUHJ	AARIT	TFLVY	HCEQB	FLFUA
BUYLF	MFNAS	ECVAR	DOZEA	MLAGZ	AAPDQ	BFLKH	LPGSI	FXYEF
SAPXN	IVNIZ	TBMTI	DAPYD	YLFME	AATOH	YAVKO	BCIMM	EEEDH
DOOKO	IFFPX	AABZE	KICPT	BHGKY	TAZTB	XISIL	KQOLH	HIITO
CEYMT	SLSHY	DSXMV	JHVHE	PXDXY	EYPAL	XMGKU	HWLSH	HIIOU
PHOGP	VVDWJ	RUFUH	JIUPG	SIFQR	NFZFQ	AUGYA	YPRYE	MXZVL
WYOGW	RFWUE	OUGKS	EEDSO	CLZSK	AULNW	BQRKE	NJPNX	ZXYUZ
TAMMM	PCBBE	APXDC	WEDLR	YZDSL	PLOAL	HGRUA	UONYT	DXYEJ
TTSHR	GRIYZ	JOLFW	FUASO	ZMTIE	ISPDY	EFEFT	OPRQB	EIFNS
JOHXD	SPASA	YLTYM	UIZVN	IPZME	SVFTB	XDRVG	FATUM	MFPDV
DTBTF	FVIUR	TBXAR	VBBTL	NUKEY	MVDEZ	HGRUE	YZFNA	QIZGO
EEYGF	LUYUL	SNRMR	UENJP	NLZIN	KPYGX	HYMKM	HJHUO	QECSV
MEYGF	LVLHD	TLHKE	CPFCA	GBPFL	ISEIH	XSCGT	OPNWX	YEAOY
AYLTY	MUSDP	RYGAX	SUPWT	NADSL	GOZUN	XSCGT	ZLNWB	QRKHP
DTIKK	XYEWJ	RUFUH	RGLME	ATZAZ	TOLBO	KEXFF	IFIFW	URXSA
LRNBZ	KNIAS	TBXFL	ZRKOY	HTEXP	RLTGH	HRHAO	ZPRMH	YIFFA
SEYTD	PPKPY	GMFAW	KSWPC	CYUGR	LSJSH	XRVLB	BTLNF	AVVTO
LNIGQ	TPRHX	IXTXQ	FSALL	FHRXY	ERTNA	LMHUE	KEONA	QMINB
XBYKF	LIOBR	HNAQI	EDVQT	BXYMU	DSPKC	GSHFM	DTTBM	TIGOZ
DIVEQ	IOCLA	TCHZS	WTOPF	CKEXZ	NAPRG	XPMRT	LAELB	AHSEA
HEYGF	LVOSO	AHWYM	UDSPK	CGSHF	MZLFN	XDXYE	MTRMM	BLRRH
ZHIYQ	KPPAD	NYPWM	EGKZM	UAYSJ	EYZYU	EBCIA	TTDVN	UPUIU
RBSXS	CGTPL	NMVQE	JEKPN	NBDIC	YZZMY	PTEKA	ICUJM	XCKHL
VIHZE	SWTOP	NYPWM	EGKZM	WAAWV	RHEHY	KFLRN	TLKCG	SXYEP
CTIFN	WTOTA	LYMQP	POIGI	INEXF	HPOEN	AQQZN	ASEBB	XPJOM
EHYPQ	WKBHY	KIYFL	VBLDM	IWQVE	LBIOL	AAAVV	LCSGT	XPVRW
JRUFU	HJWLC	EWHZW	KRBNT	YWRSI	EELMJ	EQMET	OPDYB	DICML
OIHTZ	ITRVA	OFBEF	PPYTV	UMQME	DPGIX	NMPJT	OPLUM	QTVRP
ZDHNN	MRNZH	HIKGP	VDLRY	JMMPJ	OIFIF	MDICA	ATVYE	KWDAS
WPSKM	QZDZH	INAYY	THZEE	YIQVJ	IKPSN	AAYXH	ASEMX	IIIEP
YFUVF	GFNZE	ROVFI	UIUYU	VBMMK	SLWFN	AUWKR	HOINB	ARNAZ
NALKU	IUOUT	NHNNM	RAMEE	LMTIJ	EZZUN	AQVER	BWELL	XSJTJ
ZNNKA	PFFLR	YJMMR	UECPN	NNMPC	YTZRY	IKVRM	POSQX	DIRCA
FAFEK	FLISE	IHGGF	ZAASA	HXSCG	TASOO	ZTSEA	TFCBL	YECLL
CSWTX	IFTOP	RJRDE	DIKDI	HMTIN	OYWDW	XDXRI	UWYYQ	UWKBB
ETBXU	VGUYA	OMXRS	ITOPM	ILFTR	RAHAM	WUJWE	YPNNM	TEETO
ZSYHR	EECPP	NNXSC	GTASE	GHEXW	ATZUM	HGXJI	KPEAR	BXRRL
ARIUM	FCYAS	OMXXS	TAAPD	CGYIO	IJZAH	WFSKH	LDOOM	TSWML
IIWHN	YKTOP	SYTBT	VAYEO	BTHIS	ELYBO	BXXDO	YPAMM	QQGLL
DIHXS	CGTHW	LVNFE	JESPC	NYQAF	FASEJ	RDEDI	KDWYK	QFLIS
EAMMA	QSSZZ	MYMUQ	VSAZH	IEPXY	EWSYM	BOECB	VOYIY	MTYAY
LOBTE	AVLSL	SIMTI	IIUOI	PBPYR	LZZRN	HTSCD	ASEMH	GPFFA
SEXXO	IRSLO	AMBZX	YEJLS	YHRXY	EZXAF	EOYCT	WJRUF	UHJBB
TLNGQ	BKTVE	HYEMV	XEYZN	YLAXY	EYHIM	XFLVP	BCPIL	QSWOU
WYUYQ	AJMHW	LLXSM	FNHWS	NXBTV	DWJRU	FUHJR	LXACG	EICUZ
TVYPT	MCEWJ	RUFUH	JWLCE	ZHDXY	ETZSN	IMVKT	VXBMY	AVKHL

AHUKM	SYSVQ	EARBX	FNLXU	MMZIM	EYEHY	EQWJQ	BPSNB	ARKHL
CEULA	RKHHE	EARBX	ZAUCU	FXDWT	HVDEN	AUWGA	YEIWN	XEISO
LPYTZ	HWOYE	HUMYE	KTLCW	BRFLV	YIFIF	MFLVM	ZZLUK	SIKOK
LYQXN	ICILG	ENAMX	KHLJC	BHEIK	HLDHU	IQMEO	YOELM	AQZMP
NTBXN	IEBLY	AJRDE	DIKDH	UIQHJ	TVYEZ	HGRUI	UEHYX	MVCIL
DTIYF	IDPSP	SQAUG	YIADE	FYUWK	HVFGB	MFSJY	TMOFB	LIKHL
ARCFQ	ZRLTZ	UHWRV	FMDSI	WAFLV	ENJPN	BMRJB	LWIYO	QHCIM
PEGXD	KVDAS	IMTXW	FCVYN	YVFIU	TOPPS	KMQZD	AZRYM	TIJUU
ROXTE	MKWHD	HYTOG	FRKTN	AMAWF	MLZFN	AQEEC	PPNNX	SCGTT
JTBHX	SXYDS	OLHEI	WRVXT	BXBVZ	MLGAF	FAYED	AZCLX	MXVLP
QEULR	EITOP	GLXMX	JIGPO	ZFMRP	OMEHY	IKVRM	POSCG	QKPPA
HEWTZ	VVASW	YIGXC	JUYXI	MXFLR	TASEJ	AMVRO	ODWYK	QQRKP
YGULF	EKETP	NNTNS	LTASE	CKAAE	PVHEL	TZHGE	YSAJL	MFFUA
EHYZX	SIYHY	DMMDI	EGASO	ZMTIZ	RJZUH	MDCYO	DPVYK	UXJHV
FLXTX	WFBLC	EGXYF	VRLOT	BTFQR	NFZFN	AQPRT	APRJR	DEDIK
DWYKQ	RFTUP	ALEKE	JLHCG	YTEXY	ENCEU	MBCIA	TTDMT	FKZZH
LNXXX	WVWOP	RYIKV	RMPOS	YOAPM	EKEHY	YUVJT	VQTBX	YARSU
ZTUIQ	VWEJE	LSYAV	DEKAY	LTYMU	IUQAW	MFLVF	PCSNI	KVRMP
OWYUQ	PZECP	TBTFA	RSIFI	FMURV	GFATN	AMXFF	KUOMX	DARSU
ZTUMD	YVPFC	AGBPE	KASWW	CMTWD	OVEHM	BPIJA	UOAJH	URKAA
EHYMA	TIAAS	ELBFW	JIKPS	QXDIJ	TLAPY	WMRUT	OPTII	AJKHL
AYLTY	MUTYF	NWTFI	UWPEH	UYXEK	SBCFU	VQEJB	LDTQX	WRFWH
DTBXQ	KPPAT	AHIKV	RMPOS	YOAPM	EKEHY	KQAVR	LQACE	GVVSH
DWYEX	KCOYT	OOLRE	ZLBCE	MNZXZ	LMTNU	EXCKH	LJGIM	UXIIN
STQBF	LNHHE	WULBV	FBHML	SMTIW	IYDTM	FASKH	ZTDYW	FVLEW
JRUFU	HSUPW	TUMYI	ZDBXI	HYMGK	PFCAG	BPWTO	UEIHN	QHKOL
GOFOQ	XYRVF	GBHGX	KHLTR	BBEXF	RFAEL	AMTJN	VEAFP	MCJIU
ZUNPM	VUAWA	EUKMR	TEZMU	NBZXY	EDLYN	AMXKH	LJWYK	QFLIS
EAHWU	RKHLE	HYHXS	XYZFR	LHGRU	IURTB	XUVTO	UDTLN	OXZOU
QOLXJ	EDPSP	TIPMV	USASE	FTFXV	RWLRN	HRIXY	WESJR	DEDIK
LGYHE	MIIHY	BYEUI	WSZPE	GMALR	VLSAX	FAVVA	UOMIK	QMDPH
NTIGF	LVAYC	AHZQQ	VNALN	XEMCF	UAZFN	AQWLB	APRLT	ZIRNJ
SAGUQ	VJHVH	EPXDW	FOULF	NXDXY	EMTRM	MBCIA	TTDMP	QVVBB
TLNMT	IZRMZ	RGUQG	RMLDO	GXILR	TZEAH	WMVUI	GPDLH	KECPF
CAGBP	GFMWW	ERXEM	ECSFD	YWFLV	MHTNJ	RDEDI	KLCIN	DXPAY
OSOKD	SLNKT	NAMTI	DAPYP	SKMQZ	DHXUW	AEQRL	SPRWN	XXGYY
LMCWR	SITOP	KCGSW	JOBWA	GHDXL	AYJTY	FBPVS	PEUUM	QHEEE
ETIMT	IDAPY	PSKMQ	ZDHYE	HVXSJ	UYPWU	EXEED	HNAOL	QARYA
SANEQ	HUODY	TITHE	CLLJT	YFBPV	SVXEJ	RDEDI	KNOGI	XIOEZ
TNWEG	HVDZF	BMBPM	RRFDM	UEXII	PFCAG	BPWWO	YQAGB	XCDET
MELLM	RUMVD	TQXDI	JUYCO	OGPIU	BFDOG	XESIT	VQTIF	NWWOY
QAGBX	CDETM	ELLAY	ITOTN	EBZKF	NWJRU	FUHJH	HDEPH	XZVDJ
ZNMBP	IIAIW	YIOQV	KHLJE	UKEQR	NFZFO	LILFA	YPAVB	FSCDL
CWYKQ	XRUNS	TNAMX	KHLAY	LTYMU	SDPRY	UGMCT	BDIHZ	VINIZ
SSFTH	ICAIZ	RQAUG	YIZLF	UUDMT	AATOH	HRMDM	LYSYI	DSGOY
EIIGE	QFSAZ	FNAQT	PRHXI	XLIII	EIFIF	MXSEG	IPFIK	QXYEQ
PWMFM	HVTOP	ILTBT	VAYLN	WXTMJ	TVCIW	TXPPA	UOCOK	DIETS
JMUGK	MWNVE	MILFW	THVWA	LLNIC	ILGEN	AQCNE	YPNIM	NYZLA
FSCGS	WCACP	LUUAV	RTHWL	IKBII	HHASU	GAQZN	HWNOF	NIIOM
DLUOQ	WFTOP	RQBEI	NEJLN	UEESU	IZXIM	LAJWH	HYDUE	FIINH
EIPXF	LVOYT	EMKQP	RTLOT	ITXMV	NZZRM	HYICO	ZECOE	FYIEI
PIHZD	IJPVY	SCUXI	WOYAY	LTYMU	BBTLX	BZKKH	LCECL	VYJTM

```
LRNHA QLCOP VCWQR TEPYC FNPME GAZOF LPVRW PYGMX HSCUA
TOHTD CTHHY GYLMR UECPN QHDOV RCTLF TSIJT OLTLN XIKHL
DEZTD JVTJS EXBPI RSVMS IEQXV HVHEP XDWFM LXYMM QVZEZ
CEGTU RVVLY IHLAQ VOMEH YUQWK WLWLE GAAEP FCAGB PWKHL
XOMMR EDOBD OZMTI DASWT BXSVV AAAYL TYMUO MVHOY GGFNA
TNOXE CVAYL FNXDC VAYEO ABHIL PHQEQ FAVVS LNRYM EEEDA
SELXP SLBAW EMLDI DAPYS GNOLK OSPAL GRVFM ASEMX QKPPA
TAHMD IRSBC EMMTI IETLY YOQRS EVYEI KYSIE WJRUF UHJYL
ETIUQ HZSJZ VYKQH
```

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

Sherlock Holmes 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. 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)
2. Pada hasil dekripsi, penerima pesan harus membuang sembarang huruf X yang tidak memiliki makna
3. 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)

```
ON BR BU NR GI SU CI TN KB SF IR WA MQ SU CI TN KB DP GH DK IA
GK DF VD UB CH QA GO RI VA VB ON RP TF ON FI TO BU HG QN GH PG
LB AQ DO OP UO KF GT GP RI TO GO RP VA DH BU CD IV KA AL DP HT
PU AR SF DO ET WQ PT RI MX KA AN GK DC IR LG FP EF KU WQ HC GK
RI YC DP IO WQ FI FD LG RP VA OM KW OD MG IC BD FD UO ZQ KF IO
BW RP VA ON UP ED GH CN FI UB IU KU FD QB MX RB KC FW RI OP RB
RB DS RG DH CI KD BH SF CG CV GH MY GH GE GH TE BU OP ED AQ ON
BF QR VH DM VA IU TA FD OK CD HG KR YM PF TM PO UB AQ NT GW UP
KF RB DS RG GO ED GH CN FI OD HT BV EA DC CH HG KR ON BF TM HF
RM PF TM PO RB KC FW UP KF RB DS RG GO ED GH CN BW BW DP OT GP
DP UB QP US RI ON GO QB HQ RM TP BH TH AS TZ KF VP BM MY KB IG
GK DN DF PI OU SF TQ BI CI KC TO GK TR FD LG RI PF TM PO AL DF
IU KA AN BU SE RK GE SY AV FY RP YQ BK TO FD MT GP GK NZ KA OM
FI WA MX SU HF BK RI DF FI ON RK PT OU DH TF TR TM HF XM PT YQ
RP VK CD LV OH WF QA BL FU YB RI GK ON FI UB IO PQ BN DF MX LH
PV HG TO KF RB DS RG GO ED GH CN FI UB RT YQ DX LQ PQ PD HN DF
AL GH GS KF IC BD FD UO VA VB KC AN PG MG BI RK RB US KF OM KW
WQ FS FC CQ RY GH PK HG TG KU WQ BI PU MY OP DS GH GS KF IC BD
FD UO FD HT GZ VA VB FB HC MG DB DO KF GC TZ PO KF QA FI LZ HT
OK RY CD CH SU ID RP VA ON RK OH WF WB WF UR BW UK AV GT GI HT
ON BU EI QB ML HT ZK GC OD QW WI DF GH IB DP ON BI AW CK CI TZ
```

GH PI DY YQ HD ED KU TR KQ NF BS FB WB LG DF YB WD TN RF ML HS
NQ UK TR HB FU VK CD MO GH PK HU BR UF DF VD NQ OV GN NO KF YE
BI HP RH DF GK RP BN OK FU TB BW UK OH TM PO RB WB HM QA GO RI
CH AE IW UB PR FY BU GH AS ON BU BH VH PG TN DF PG AH GQ PY BU
BU BI VF BU RI ON RP RI DP IO WQ FI FD LG RP OH WF RB WB TG PR
GS PQ FS WA IR DB RI UK IB OP ON IW PQ BN DF RB KC BE GK ON RK
RY PU DR GH IS FU QP US RI TR WI UM GO FU CH TB CH GP KI TP UO
KF RB DS RG GO ED GH CN RP GK IB ON RI DV TP EB DF MX DC WA KC
VG PG TH HD MZ ON TF OD MG TP RO KA QT OH WF TR HL GH GM SF GC
OD QW WI DF RI GK VI PU DY DF TF MG ON IE SF MC YC FB OP HG WA
AI PG TH CH GH AS ON BU NF HD KU BY FS DY YQ OP DS TQ DE ID VR
DE RP GH MY SU BG ZG FD HC KR AL GH CD CH AH CK FU RP IC BD FD
UO DF RP FR KI GQ ZQ PO KF OD KR SE QF KB SY GH MS GH VS UO KF
NK HF BI FD OM RI GO PR CV DF TF MG ON UI HQ RB VA PU TZ KF UB
EI UB HT KC WA TN EK ZT RP YQ RP OP ON RP GK PK TN SF DB DO OH
MG KF LG UP KF WB VC GQ DI RT FP UO KF HQ QY OD MG ON BK QA GO
AP HT UO KF HQ TO OM KW SF IC BD FD UO DF BF HL HT ZK CH DF IU
TG LR BU VA QK FI TR UB FQ GO TO FD WF NQ KF VI PU DY RB PZ BW
UK BH SF CG CV GH GS KF FC OH HD OD QB NQ QV QV VA PU LG FS QY
PD TN OD UB GO ZQ RK QO RI EK ON OP VQ YS CH BQ CF VH PG MT FE
VB CD KI TZ LH PV KB GA FP UO KF DF FI OM GV DF MY GH GI HC IL
VA AT VQ MY FI HD MT KA QW

Plainteks dienkripsi dengan program aplet Playfair Cipher yangd apat diklik di sini:
http://www.simonsingh.net/The_Black_Chamber/playfair_cipher.html