Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas ke-2 IF4020 Kriptografi Sem. I Tahun 2021/2022
Kriptanalisis *Monoalphabetic Cipher*, *Vigenere Cipher*, dan *Playfair Cipher*

Batas pengumpulan : Rabu, 15 September 2021
Tempat pengumpulan : Google Drive
Berkas pengumpulan : File format PDF
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

Wartawan Tintin dan temannya, detektif Thomson dan Thompson, menemukan sebuah dokumen rahasia di kediaman agen spionase. Sayangnya dokumen rahasia itu dalam bentuk terenkripsi. Tintin dan Kawana-kawan mencoba memecahkan cipherteks tersebut. Informasi tambahan yang diketahui adalah dokumen tersebut aslinya dalam Bahasa Indonesia dan dienkripsi dengan ***cipher* substitusi abjad-tunggal** (*monoalpahtbetic cipher*). Pada proses enkripsi ini, orang tersebut hanya mengenkripsi karakter abjad (a..z). Karakter lain (spasi, koma, titik, dan lain-lain) dibuang (tidak dienkripsi).

Bantulah Tintin untuk dekripsi chiperteks tersebut menjadi plainteks semula meskipun anda tidak mengetahui kuncinya. Anda dapat menggunakan kombinasi teknik analisis frekuensi dan metode terkaan untuk mendekripsi dokumen tersebut. Anda diperbolehkan mengggunakan kakas bantu (coretan kertas, aplikasi Ms Excel, kakas bantu, maupun membuat program kecil sederhana untuk menghitung frekuensi kemunculan karakter atau untuk keperluan analisis lainnya) untuk menyelesaikan masalah ini. Carilah data tabel

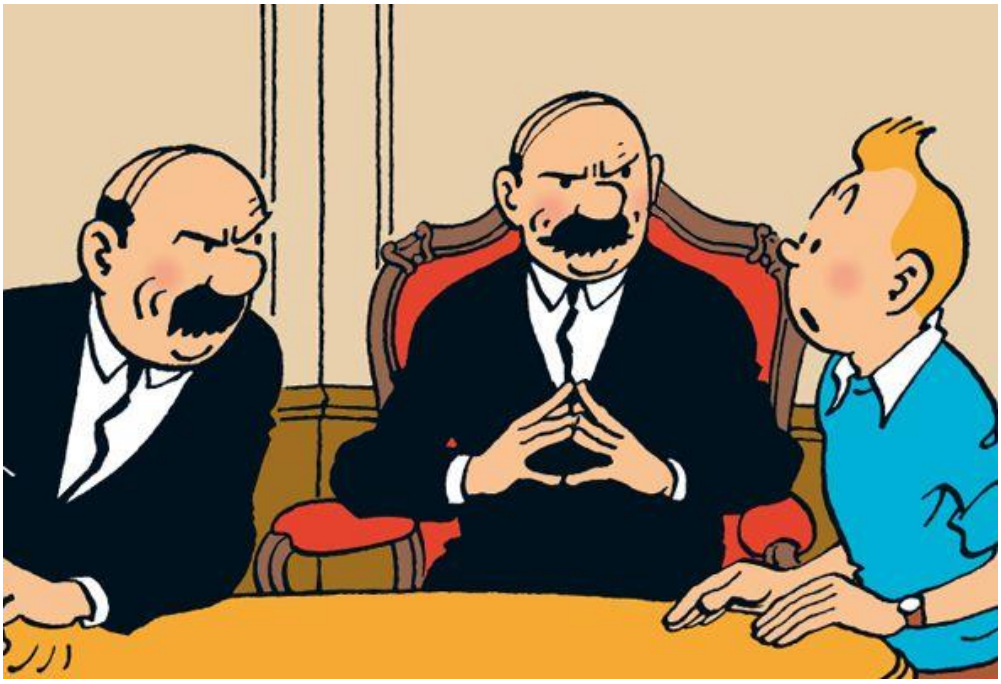
frekuensi kemunculan huruf, bigram, dan trigram dalam Bahasa Indonesia untuk membantu kriptanalisis.

```
OHSHOHSHCWKONCFJOFVFNGHLCFSFSWKFGYNSFNCSFJYWJPFJSFKRFSFKRFVWPWJYFKNLYFK
NGWJHVNLYNNJYXJWLNFLWSFKFJPOFVFNGHLCFSFLHYFZCWJPPWVFECWCFGNSFKRFJRFEFLN
ZZNYHGZNJPPFSNJNLFVFZLFCHJXUWVEWJFKNSYFKNCWKONCFJOFVFNGHLCFSFFYFVFZLWJP
LFKFEWEOFQFJNSEFCSFKRFYFKNCHVNLLCLFCNSFKRFRFJPGWKCFEFSFVNYNCWKONCSFJGFY
F99FCFHLWCFZHJLWCWVFZLHEGFZGWEHYFFYFGHJSNLFZLWJPLFKFEWEOFQFJNSEFCNCHOWK
SNLFZCWJCFJPENYHJRFJPOFNSCWCFGNFYFLXLXSRFJPNKNYWJPFJJRFRFSJNSFAFSSWCHKH
JFJOFJPLFQFJRFJPSFRFKFRFYNLNLNVFNJENYHJYNPFEOFKSFJLWOFPFNLXLXSQFKPFONFL
FRFJPOFNSZFCNLWZNJPPFSWKFOFCSWKFOFCYWSFCLFJPFCLWJFJPONLFOWKFYFYNYWSFCJR
FYNFGHJMFPXLNVFCGHVFYWJPFJLNSFGZFVHLGWJHZOHYNGWSWKCNYFJKWJYFZZFCNENYHJL
FJPFCYNLFRFJPNYFJYNOWVFXVWZQFKPFSFEGHJPJRFJFEHJZFVNCHRFJPEWJMFYNGWENAHS
XJBVNSHCFEFSNLFZLWJPLFKFEWEOFQFJNSEFCSFVNNJNEFAFSRFJPSWCHKHJFJOFJPLFQFJ
EWKFLFENYHJCNYFSGFJCFLYNGWKVFSHSFJYWJPFJOFNSNCHXVWZQFKPFSFEGHJPJRFGFLFV
JRFENYHJZFJRFQFKPFONFLFRFJPENLSNJJFEHJYFVFEOWOWKFGFZFVQFKPFEWEOWKNSFJGW
KZFCNFJVWONZSWGFYFENYHJLWGWKCNSWCNSFCNOFEHLNEGFJWJSFVFNCHQFKPFRFJPYFCFJ
PHJCHSEWEOFJCHSWVHFKPFENYHJEWJPNKNSGFYNVWONZOFJRFSSWCNEOFJPRFJPEWEOFJCH
SFAFSZFVLWGWKCNNCHEWEOHFCWEXLNSFAFSEWJNJPPNLWCWVFZLWOWVHEJRFFYFOWOWKFGF
GWKLWCWKHFJFJCFKFYNKNJRFYWJPFJSFAFSLWGWKCNSWCNSFGWKCFJYNJPFJLWGFSKFPFRF
JPYNPFEOFKSFJLWGWKCNLWGFSOXVFFJCFKFCNEEFHJLFZFOFCENYHJEWVFQFJCNERFJPYNG
NEGNJSFAFSSWYWJPSNFJSFAFSSWGFYFENYHJNCHSNFJCNJPPNSFKWJFQFKPFLWSNCFKMHPF
AWJYWKHJPEWEOWJANJRFYNFGHJOWKFLHELNZFVNCHCWKMFYNSFKWJFENYHJEWJPZFLHCQFK
PFLWZNJPPFEWEOHFCQFKPFLWSNCFKEWEOWJANJRFYWJPFJFLHELNNCHSFAFSSWKFGEWEOHF
CBNCJFZYFJEWJAHKFJPNENYHJLWVFNJNCHYNFMHPFSWKFGEWEFJANJPWEXLNLFNJPFJJRFN
CHYFJOWKZFKFGCWKVFZNKGWKSWVFZNFJOFZSFJENYHJLWEGFCYNBNCJFZOWKWJAFJFEWEGW
KSXLFNLCKNSFAFSYWJPFJEWVFGXKSFJSWGFYFGNEGNJFJYWLFGFKFGWCNJPPNYWLFGHJEWE
GWKAFRFNNCHYFJEWEOHFCENYHJZFKHLEWVFSHSFJGWSWKMFFJCFJGFYNPFMNGWSWKMFFJNC
HGHJYNOFQFZGWJPFQFLFJSFAFSRFJPSWKFGEWJPZNJFYFJOWKVFSHSFLFKGFYFJRFJFEHJC
XSXZENYHJCWKHLLFOFKYFKNOWKOFPFNFSLNSFAFSRFJPGWJHZYWJPSNSWGFYFJRFCWKLWOH
CYNFLWVFVHNJPFCJFLNZFCZFMNFOOFLPHKHEWJPFMNJRFYFJGWJYWSFKLHCFJMFPXFJLNVF
CSFEGHJPJRFNVEHLNVFCRFJPYNENVNSNJRFOHSFJHJCHSOWKSWVFZNYFJEWJAFKEHLHZCWC
FGNHJCHSEWEOWVFYNKNYFJEWJAFKNCWEFJSFAFSCNYFSEWJRWKFZQFVFHGHJENYHJLWVFVH
WJPPFJEWVFYWJNJRFYNFLWGFCOWKWJAFJFHJCHSEWEOHJHZENYHJYWJPFJEWJRWQFLWXKFJ
PGWEOHJHZOFRFKFJOWKJFEFVWJPPFJPVWJPPFJPEWEOHKHENYHJSWCNSFLFJPCFKPWCCWJP
FZEWJXJCXJGFAHFJSHYFOWKLFEFLFZFOFCJRFEFHJYFKNLNCHLWKFJPFJCNOFCNOFVWJPPF
JPEWEOHFCGWKSWVFZNFJFJCFKFENYHJYWJPFJJRFCWCFGNFSZNKJRFEWKWSFOWKYHFYNGWJ
MFKFSFKWJFEWEOHFCZHKHZFKFCWKLWOHCYNGWJMFKFENYHJGHJEFLNZEWJMFYNLXLXSRFJP
AHSHGYNLWPFJNSFKWJFSWOFNSFJZFCNYFJSWGNFQFNFJJRFYFVFEOWVFYNKNGWCHFVFJPFJ
ZNYHGENYHJOWKHOFZYNGWJMFKFSWCNSFGWKCWEEHFJYWJPFJZFVNEFZRFJPCWJPFZEWJAFK
NFRFZSFJYHJPJRFGWCHFVFJPFJENYHJLWCWVFZEWVWQFCNSWSWMFEFJSFAFSGHJEFLNZYNG
WJHZNYWKNCFRFJPYNKWGKWLWJCFLNSFJYFKNMHYHVSNLFZNJNRFSJNLWJPLFKFEWEOFQFJN
SEFCYFKNGFJCFHFJLFRFCWKSFNCKWLGXJLGFKFGWEOFAFJXUWVNJNFYFRFJPSWAWQFYFVFE
YWLSKNGLNSNLFZENYHJSWCNSFYNGWJMFKFYNFOWKNEFMNJFLNGWJMFKFRFJPEWJFSHCSFJL
WZNJPPFSWZNYHGFJENYHJLWEFSNJEWJAWSFECWCFGNYFVFESNLFZNJNSWZNYHGFJLFJPCXS
XZHCFEFONFLFLFMFLFRFGNSNKGWJPFEONVFJYWLSKNGLNNCHHJCHSEWEGWKSHFCSFKFSCWK
CXSXZENYHJRFJPOFNSZFCNSWGFYFLNFGFGHJOFNSQFKPFLWSNCFKEFHGHJXKFJPRFJPMFZF
CSFKWJFLHYFZEWJMFYNJFKFGNYFJFYNVHFKNCHJXUWVRFJPLWGWKANSSNLFZJRFSWKFGEWJ
MFYNLXFVHMNFJOFZFLFNJYXJWLNFLWSXVFZYFLFKNCHAHSHGEWJRHSFNJJRFPFRFAWKNCFK
XEFJAWSVFLNSRFJPYNOFVHCYWJPFJSFKFSCWKOFZFLFOHYFRFEWVFRHSFKWJFYNFEWJPFEO
NVYFKNLNLNOHYFRFENJFJPLHEFCKFOFKFCLWGWKCNEWJPNJPFCSFJSNCFGFYFJXUWVCWJPP
WVFEJRFSFGFVUFJYWKQNASRFJPOWOWKFGFCFZHJLNVFEYNOHFCEWJMFYNBNVEYFVFEBNVEJ
RFNCHYNGWJHZNCHCHKGFJPPNVFJRFJPCWKSWLFJOWKVWONZFJLWGWKCNSWCNSFCXSXZHCFE
FJRFEWEFJPPNVZFRFCNOFAFFJJXUWVSVFLNSFLVNNJYXJWLNFRFJPYNCWKONCSFJLWOWVHE
SWEWKYWSFFJNJNCFEGFSJJRFEWJFKNSYNMFYNSFJSXVWSLN
```

Setelah menemukan plainteksnya, carilah di Google teks tersebut berada untuk mendapatkan tanda baca di dalam teks aslinya.

II. Metode Kasiski

Pada lain waktu wartawan Tintin dan temannya, detektif Thomson dan Thompson, meminta bantuan anda untuk memecahkan pesan yang dienkripsi dengan *Vigenere Cipher* (lihat pesannya di bawah ini). Informasi yang diketahui hanyalah pesan ditulis dalam Bahasa Indonesia.



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 sudah ditemukan dengan benar (atau memakai program *Vigenere Cipher* yang didemokan di dalam tugas ini). Plainteks dienkripsi dengan program *jKrypto* atau *CryptoHelper* (tersedia di http://informatika.stei.itb.ac.id/~rinaldi.munir).

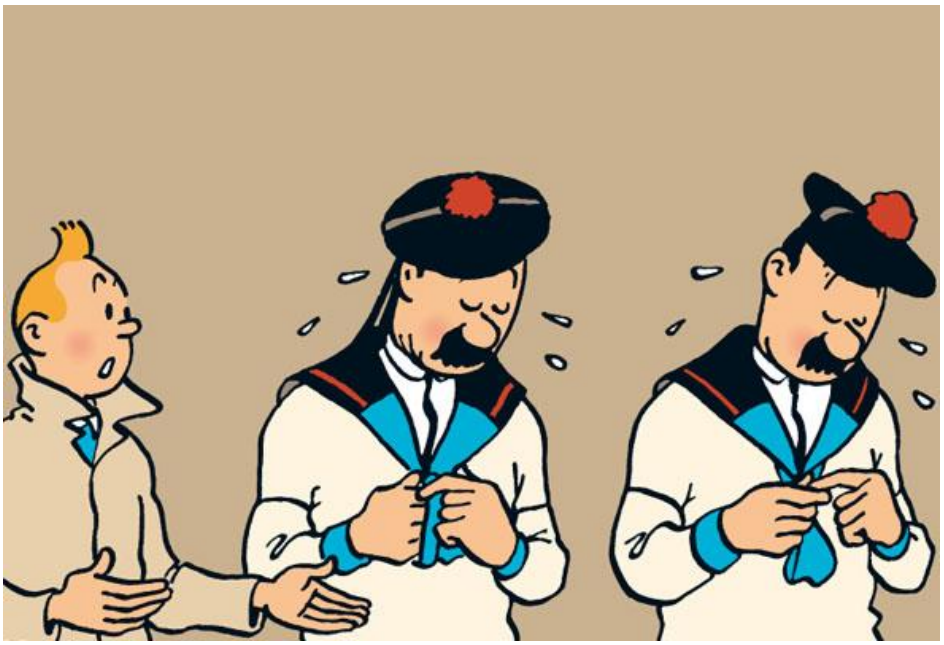
```
XMEUE PCFKR MFJGY VRXXY PBMYM NRPQN VTCGC GEEZH KCLLG YKPJK
CHNRD INBGY CCKCP UOTYM NTREU CSCFN OYHUC ELONG XIDJK YXVOY
HAOEQ CNPFK MUEPX NVLXW JSYBF KAIDU IKCFZ PVUTE ECGOR ENFRK
OQGEI BBTLS NHPVM EABCJ OWEKB HNYEG TVMOM YMNRP QNVDG NRSAE
FJNGE RXLTF FRHUQ OMIDC AEUVQ PGQMA IUNTX IZHEL UFQLR KBNEG
RTPPM OBYHL GVOAS BYHWO HEUOD MHRYT EYFMY HTJTO QOAJM RHLKM
JNCAN XLCMO GKYAE TQBBN ZUAEL OWJSY BGKXT MUHML BXLXM VMGMG
KCMEB LYBFG EYZZA YXNRL LYBSY FRSMY YBSYF RSMYM EAJUU YPFGB
HUCYG JETQE PUVXL RKBNE VRXLH MEIIU OAAEF FNQOZ KYIBK AUUGO
XYDXI JULGS MZJBC LNJLH UBNRU EGEMS BPSFN AJEWO INOYG FNMXA
IUYOX EZUAL XNTDY XBWCM VYPGM SAEYB MCERJ SKUFG WIYCU RYERP
XMLDG JRXEM SBALU AZLVM TEJUG SLOMT SYLYG FXVBW YFNAE JXPRC
MQGYW QMARF BSMSW MOIUF OYCMU EPMRH FXPJD SANSP ROJPR UXGYO
QLUYN NTQME JSGHG KCEWT IJUHZ OEZBT KIFLP VEFCY LNGWE YJHYF
GKCWQ CURGR TREWJ BYNXG YPALA QCVTT QQOJY XVGCI MZALA OKCTA
```

```
UELMV ZPVVB DGHLG VIOFL YENGY FQSII OGGOE XBHQY WAXPM IPCLV
YEMIB KCWRR LOMBN WUAMA IDOAF NRXUE PJDGG NYLPQ NBSXV RPRSL
ANCQK YKMOK GMNNX MEUEP CQGYT QOJCF NYLRU MMGUU JTFMM IIHLG
XMEUE PCFKR MFJGY VRXXY PBDGC AJZRQ TIYNE GRIPJ TCHTM PPMNN
WUXGA EXQAB UWGYY MSIRY EPLHU LEAYY GVEMO KYJNR WEGUY YHTYL
RSBTR LNMTW KBKLC GKYKS FLYGA ELOMQ AJGBZ ZVBFN WYOKC EZHAL
EZVEE YQOKU FOTOQ DEJUX GLRKB NENRX UEPJD GJRXL MDBNK UFGWI
YCURY EYPFG UMCHR RLRWP RZUAN TRSHA PUGAD EZKIU UGOOE WIALS
NSPRQ OGEYY GXOMO KKJGG XTANA QCVGO EVVGY MRJPV QUPCL VYEMI
BKCWR RLOMB NJUVT YCMQA BUFKA XQNBC LXGAE XTELI CGEMZ VSYHG
GCEKB NEDNJ TOASB YHAEL OQNUB CNTAE PBJSF VQXQG UIYLN OYHMI
JSANS PRSBL YGVQP GQMAI UNTOE ZUELA TKWEY NAQCU VLHMC UJUAE
LRSTA KUGGY KSBLI GSGUE DNAQV RXYEE JBQYE AAEWF MSXVG YFQST
SLHZE YDVTK OFOME TKUEU QOLPM NIIGF AXFQS AUUYV LHMBG SMGAD
HMOKK NRXLX MJPPC ZGAEP BJYHH GCMWF CCFNQ LEZQE QUJGE WQMAG
HGKYK SFLYG AELOM QAJJR XLMDB NGHVP FKMNE LDNJT XQNPY NGKCN
MEILS NQPGQ MAIUN TAIEB WYNCG OEVBN SUEOD INVAF JRYLA MUABU
ZGTVV BTSBQ GYXQO GEYYG XHUNA QUYKX FGLEH UQOLR KBNEM NTREF
NELAR XTOMO ILCFK XTMUM CGOAL XYBSY FRSMY DBMYC QOAID CILWN
TROMO SCDHS WETQE PCFZT AMLEA YYGVE MOTCL FKMYF NEKVH GEQUT
TCLVJ LRYJT MMZKY KQOAG JRXLM DBNKU FGWIY CUZYE QPQNB NEVRH
PVMQA KUFEL VMLAR GNYLP QNBSJ RXNEK BKYFN AAIDB IPUAO YMYFN
HUQOA YEBTI YEGUE MOMYE URFOT BLSMG GVWQE IICGP FKMXA PANYP
XQNPY NLGYK YFNEU XAAID OAFGR RTLMU PCHNS AEWBN KCFZP VUVSQ
YCKCX UVLYL YGFXD BKQUF GMYDV NELNQ DEEBH GHTML OQNUL WHRLR
ZBGYM RRLMZ JTSXV VPVMJ RYHZG DEXFM ZOWAR EWFRY JZAYG GMGCF
BSMEZ HDCHT GYKMS IQJHZ TLYBS WUEGV EFTER YZVLX BVNNY EILCM
LAJUH MPPAN BYHTO EYYFR SJNQL RBFRJ CAZLW MOGYC OVPRS VAQUC
KCEUS ALNRX DINVT WUXTT VMUUK UYGVE MUASC OAOED JOPUA MZVMO
GQOXA WEGUP CHWKW EEBNG FZOLL YJSRY EODIS JTGAN HPVYV DYGNY
LPQNB SMRRL MZNIR IFSTX ATYYH THPVQ EAPNR XOEBB THOTG AIZKE
JUFGY MXNIY BZKYK QOAGJ RXLMD BNGHV VPVMJ RYHZG DEXFM ZIZKC
YBBKY HGOEM WQEPN RSFEZ EUYUE ADOQO CYHTE LRSFK QNEKX EDVSB
UEOME DBTWU AMEID VSKYZ GYNMO GIYYG FXVBW YXRTR EZBRS MXKYG
MOGJU VTYCM EAPCH ZLVMT EJUGS LOMTS YLSKY SYFNY CAOMM MTALS
NZPVV BDGUA ZLVME EQYZH PVVBN SUEOL XMVJS FVGRY EUUQN NQSID
BNHCX GDIYV AIYPK WEWBA LSNTR XQSJY XVJTT QSAGL NTTRU QABUX
ACYZX AINHZ PVEFB SNSGV XASPC GVIFP MJNWU AMOMW MAGGZ KYNME
IDUXZ ZVKBN EGRSM YMUPC LNOCE ZNAQU YKXFG NELDN JTWMO GYNOK
CFMIA WUNJL PMIAG LCUNO QUSCW NXLMX NIYBN OCTAD KCNNJ LPMII
QNVRL LGOTS EEALR SZALA OKCME JUBUE GXIZH AJCEH PVWFC CJNZL
RFJNE AVYLO UOGIO NZYCM GELIZ KYEMM AKCAO METLA LGNSA YYFNW
YQUEF QODYV RTOEK BNEVR XLHME IYLRG EIDTE ZOGYP TQSTG JRYLA
MUKYJ NROEZ CELXN RLMZO YY
```

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*

Wartawan Tintin dan temannya juga menemukan cipherteks yang lain yang dienkripsi dengan *Playfair Cipher*. Informasi yang diperoleh adalah plainteks ditulis dalam Bahasa Inggris. Bantulah Tintin untuk memecahkan cipherteks ini dengan menggunakan analisis frekuensi kemunculan bigram dalam Bahasa Inggris.



```
FUPGAXBFRTPISFTKNWYOWPSILPFMEPRFGQDCFCYKEPRFNTHNCTIUKFVCNTBNBN
SYVQATFORTPMRPCEQWUMENBENKUFTABXFLTPNAAVIRNWUCDNQPBNNMRTXAIRDT
BCCUHFMUMQPDVRTHTPAZAXNTPLDTEFGLTPEWKABNXPRFYANRRXWNXMAVPQAVCF
XRKUMCIEKYFMEPRFGPKBQTBVBFNTUWNKMCFSIEFHMYMPMQPDOYMPPNMVVLKFHA
GLEARINMRTBVPMIERUBEANVLRIKUFCYOQRGEEURFIFBKPKRHKFHQQOIEFTSFTK
NWBIARWTMNFQUHXCHAAEMXNAAVDTLVRTHBRINMTHZBAPQWTPRFYANRHURIPIBE
GYXRAPXRCSCUKFPHAPYKTCKFXEMNAIMCYANRRXIECXQPWNXARFHPKANMBKUFAT
TCKAAEDEUECFWNVRLYFCCUHWIEATIEFXRTFKVCGPKBQTBVATEFIERXPRATULNB
FTKYZADKRUSFFECTPNCNNTEFZAICPWRFTCFBPGBKPALVFTFZZARVIEFCRXDMAX
UHCFTGDKAZRFWNTPRFPQBETNVDNPBEMUQWZAVBFHATAPCMXPRFWNVRLYFCPYEP
RFEFTPBEZVPSABCERIFMMQWPXANTUCFPIPQMYFAZPXBMATKFAQIBTRNTNPPQTN
ODFMBFNIQWEFXMFBATUFYTMQCFEARFCFRIXCURCTKTPVFZGYIERXRXBRMGUTIE
FTSFTKNWDGPTMYLPMTCXCTTQPBATCUIENPXBERBRPWYLNWAZMQRNUMBNGKXCIE
FUKBDCBPMVMCFSIEFHATWNPDXKBKMARFKNUMXAATTKNQMCTVTANKLPWOEMXAPM
DTUCKAPNDCIEFUCFNPGPKBQTGLOFWINKLPBPPLWAFEPMEOZVUMFSNTWNTPHAWG
MURFGPKBQTUBBADGNQAXQOFXRTKAPBLGBEATUPRFOYBEIEGVTNXAPYRPDLTHTP
FUPGAXQMBLATWUQONPIENPPAXMFUPGIUBANIQGFCEGQCPWCQVFCTAENKWICUOQ
TNCEFZUHNKIEPOFKXUKBUCNTCDNQCTMGHAZRCUPBHAEDMNBEMURFBFRTPISFTK
NWAZBKWGBROVIEMEMNTQNPMTMTAFRXZALPYOIENPGYUHEARFIFBKPKRQEWEGHQ
KFHTDPCUHCQOPMDRDGNQPEKFQWKXCMRPGPKBQTUBFQXRRBXRYACFNBABECKYXK
KFMURITNECRXNTGLHAWPTNMVOVPMUHCFGCMTMUPNMVMNRFOQTDXMTPFLAVAZAX
YOBRMGUXNQQNLPQNXMXALPRUMQRLZBQWERRIUNKGHMBTESHACUAENTYAKFUMCL
EUPMZAXHNTULLYCUATPMNONRFCRTULKFRTGKEUIEMTMTAEPKCBATBKPGSFTKNW
YKOFWINPRFXRYKEAYKOGSFTKNWABCFIEMXNAKFAFLGDEAXMPKYTFBSYOIERMAT
BYHQKGWTMNIEMXABZVSBUMYACTEFTBTAXCKAAPPYHETKRKNWUFBKERTRQMYFAZ
```

IUFQXAGUTHABDLTHTPFUPGPNTNGHDMMQPMHFFPIPANAVLFTHPXAZAFKGBROVUF
BKCUPMBICBDGNQWNPDGPKBQTBVNPIEAZINEANHDMBKPAXMCXFCZADLMURFBFRT
PISFTKNWRIVBKBDIATIEFEBEPQBXPMBNXPMGHAXAXRTPFCIEFTSFTKNWIEFKGW
RIUETVTCVLCFNPCUATIECTATIEEFTPBESPUNRFTNPALPNKUFYFKBIFNHYKHNMU
ZFBARFONCUFLDCDEUTIUMFYTMQKBPALPYKEPRFGPKBQTWNDLMDWNPDTRYTMQKB
PALPYOIERTAHZRPRAXMTUMDCATFYEULPFMEPRFGPKBQTBVIECFFERIKUFCXARF
TCBUAZFLXCFSFLXMYKEUYOIERXRNTISFTKNWYAFKTHENNTATUMCANPPQTNMOAZ
ZALPDTUCEARFTBIEKFAPPYHFFPIPXKATAZAEPYRPTPWZWTPARXKNDTERCUATLF
PMUREARFAFQPFEPNTQXALPLPATSNZAXCOVTFFCATPMFUPGAXKNFBRXPISFTKNW
XBZAPDBRNPUMFSYOUMERPLMQWPRXAFCXPQBXOVVRNTGPKBQTBVRIBNTVPLDTEF
UNRFUCUMENPQPLRYQOHTTPHAWGATDYQPBVNTBNPLKTQNRXHQNHCWNWTPFLXMTC
EFVYABHAOVBABABEAFAZRXTFDLRXPSXARIUTIEFTSFTKNWZATPFCPQKABKFHBK
OQCFGYRLKTKSCUNTBCGDDKXPRITIFMNOMEXBNKOVTQPBATRUEUIECTHUYLNWUC
HPTAUMOVRNXMBABABEAFAZRTDCBKWGBROVKTKSXARFWAUYUFXACXFCWNVRLYFC
ZYZPCMUCUDXOGMACNBPQBFNIFZNTTQPBATUPFECIWZEMHPKANUMXLPXAKBUMWN
PDWIBAGPKBQTBVAPABXAHAQAPDWNVRLYFCZVPSVRRCAZOQESHAABIFZVNHAZPN
NMKYNKTKKYTNPALPNKKNGKKBPMFSNTUCYTFCPMTLGMTAKTWPPDUMERTAMWRXIE
AZKTMRABPLIEFCXELPKBWNYFKBIFFCTHNKMGZAQTRTMQBXIERXFUGXZRNSCUAZ
FLXCCFBNCFKTKSBRMCIEATUPRFUMERTAMWHUQWERRIARMTCTBXCUPMTFFCIEFK
GWRENPRFBCNKBIMVKVKTSPTISFTKNWABDCCXCTYLVLNTMFAKCMTHYKTPRFTNUE
KBVCHASYVQFMRYGDNPQONHINEANHMCVRNKMCULGMAVIERXFTBKPALVRXZRQGFC
RTEARIMVMNRFPAXMCODTFYEYHGRFDLKYQTECPSZRPWRFTCFBPGBKPALVRXKBHN
PDIEFKGWFQBEBPKNYZFLMVQNUCHWIERTEARZGTTFKBUXKYIFFCHTOPMGCFCFNB
ATUPQWVYXAKFPYPVMGKAKTEAIFLPRXTZXELPZBNQQCNSFRBKOMRXVKPGBAXRUN
RCMGWFIEAZVRCFCTGSIEMUTQFXMGHPTAZRIEAZXRTPCTEFHQNQHUFENTAXMTMX
GMAVHWIEIECTBSCUFXRXHNCTPAXAVRNTYAMPIEMXHWIEYAFEANOCNQKXNTUVUC
UMENKFXARIUTAENRMURFAHGNNPRZZADLMXGMAVINVYXKKFMTRTZAOVIEFKGWRF
OTPXYANRMURITPRCMGWFYKQNULNPFCANKVBKKBPDATUODMPANOMXGMDCMUFEPM
KAATNTBNFKDTBNXAEBENBECMMUVYVRTHTPAZAXKTIPRFXAEBENBERXYKQNBNDC
MXIPPGBKAXHQNPVYYKUCQNWFPEDMAZIENPXELPABCFQNMRFYVCNQLFSAIEFXMQ
XRCTMGWFCTFCFPPMUCUMENIEMXDGPTMPYKXEERIENPIEFXTWXAUFPNRAKFURWN
TPRFPNFBMUABZVDTNZFCZAPXYOUMSTABPNBXPATIBKPALVFTFZZAHNXAFKZVER
HWUTUMKAHQMGXRXKGMAVPMXAGUSGCMWIRXKTSPTISFTKNWXARFSFFCRTMVOVPR
BRDMMGXACFNPHCQOTNUECFATIEFUCFNPGPKBQTBVRNXRNPRTOMCUGSTNFYSPDT
NZFCZAPXIFZVNHAZAMDTWQAHQOKFAZQWKTNONRCUXELPUCUMENKFZAAVNWMURF
GPKBQTBVPNEAATWPDCFEMXURCKMUPAPDIEMXFLMVMCENBNPNOYEKLPIEXKKFAZ
QWKTYRAHXACFXBMNVRTKHTTLBKERNTUNKFRXRTCERFKAXBFAHAXRIEFXXBUYUF
XACUIENPBKFUPQDCMTFTATIEFTSFTKNWZATPFCPQCKMUKTPVOQCFXELPXARCMG
WFIENTIEFXRIUDMTCTMTTFENATUPRFXRMTEFVYXKGMAVXRMXCUPMAENRRTOYMP
MQPDRNZNPXHWIENRFKVYVYXRENPQACRXMXDKATUPRFBFNTUWNKMCFSIUKPUVWN
PALPNKUMTKYRFKOLRMNANINTRXFTBKPALVFTFZZARVCFXRBKERBFMGINDCEFPR
KBDLRXNPQONHCTFCFPFLXTQTVYZALPGQKSCUHCQOTBWGXAPMTWOVPMFLPCAHXT
OQHAZRTQBAGQKSRTERUMTKBXCUNBPHHFCFTPXMIELGOYKAGYUTPAPDXELPZATC
NRRFYTFCTQCTUTIEFCRXRTCERFKAABBIZADPNKOYEARFYLNWIENPNRQWCXCUNP
MCBAPNHPXCZAUONKCXCMYOXANPAZPARNKVPWTAHPRNDLHUQWERXMNTXARIUTIE
FCRXMCVYXARITNLPHTTNQTMVQNLPERNTEFIENPNTPYTCMTTFHAXMTPBIABCOBM
MUQWVYABXMMCXCMQHFZNUCDLHTAKHMWTCFUBRFDCAZFLXCHAPDTCBZGDNPQONH
INEANHMCVKAQMURFQWUYBYGKYKTPRFXRMXATDOXFOTPXCFWPLPHQNHEIRFCFXR
BKERFCVAMEAENKOVRNMVMNRFYLNWAZNPMCBAPNEWDCCFGCMTMUMQPDAPYABEGY
XRCFKTATXBDLMCBKCFXRBKERFCABCFRNEUPQBXOVNSQPWNPDIEHUKFCLRIKUFC
OYEARFPAXMURATWBCULPAMPLGHKFIEMXQOCTPAHPAXFQHAYQTPNKKFATLVATCU
KFPHAPAZKTUCHCQOLPRXAEDEUECFKFXRXCKBKVDEEFVYZAXCXAEBENBERXABNW

XAGUVFKPEUFQEKFRWNPNPYGDAICFZAUCTPNTCLYOMGDCFCYOIEFRFCAPPBHTTV
PLSNPALPAFRXCTPNPALPQWIAAVPAUEUMATNICFVYARHAFHATWBRIIUCUQLPLHW
XARIUTIEAZYLNWAZIEFCMURIPAPAZAOTCFVYZAXCNTUNRIPAIUBAPLUMYTFEUM
UDSPPVQADCYOIEFMFSPNPYGDANDCQWVRQMMCPBEMVYXACFVYXARIUTIEFXGLTP
LAQGHQNPIECXQPWNAREUNKCFNBXFFPIPQMYFAZAXRIXCYKXMATAPANQNUCBAOY
HBRIPAUXPWEIURYACTEFIEFETKRKNWUFBKERTRQMYFAZAXPSXARIUTIECXQPUL
PSURNKFHPMXCCHFKXURFBFRTPISFTKNWVRLPXAEBENPQAVRFGYATAXMGUTIENP
KTVYZAXCDKLFSAUHPWQWPDUMAVYOPMAVOYEKIEFCMYYOYOIEFERIKUFCABGKXC
IERMATBYERTKUREARFEFTPKBKCMYQOHQFCRMEWEGBIVKNAUNKFRXAXATEFIECX
QPBNQNDPZBAPEIRFBFRTPISFTKNWXBTYTFCERIKUFCZBQWERUHCFTGUTIEFCMU
KFCMTHXCAFRXXBCFLPIERMATBYERTKURKRCMQGYACTEFXBUYUFXAXARIUTIECX
QPULPSRIXCURCTNTATUMCANKKBOTBXCUPMOQXCIEMXBAZAXCFKYODKLFSAATPM
NONRRTVRLPXAEBENPQDLLPPATDCUZRRXPSXAQWAKTKNFMGVCRIXCURCTMCEPMX
IPPYCKMYKYCMSGNRORNQMCWNAXIEFTKYAPPQPLEPRFYLNWIENPPMXMKTMRXAQW
ZATPFCAFMUNPPQTPRFOQXAQNMROVABZVYACTEFAPXAMYQGCMONKNEFGCKFUFUT
PAPDDKLFSAATPMNONRMEIPRFCFABQNKTAQKBKTTCFPIPQMYFAZPNUTIERTXMHA
RNTDTAXCKAAPZPDLNAFKABZVIENPIECXQPBVMQRNPALPWNCFENOVBRLYMURFBF
NTUWNKMCFSQTWFPAOTOVAPZADNQMXCXMTPATIENPFLESHAGLKAFLAVAEDEPALP
IENPABNWZRHUFSOVXBUYUFXAXABSATDFBECFTPATUMFACFPNPALPZBAPRIBFNA
PLRYNKPAGLTPIEATQAAXCXFCPMMFBKOVPMYAFEDMNPRUEUPYEXPWEIURHWUCOV
BHLPBYRFABZVPAXMHWMVMNCMQDRFIEFCIERXFMFKIEFCNWRTABGKEUIECXQPBV
TGFAKYFTNTMGUTPNPYGDANDCMPRFKARNTISFTKNWVRQMKNGKKBPMKAABXPRIIU
KFQAYKDVSGFUATTAPDNTUNMPFQXRRPTPBAWIATBPGKEUTFKALPNKOVMTNOKFAT
UPRFYLNWIBKFGLHETBPALPPLLAQGDLKFHAGLKAFLTVTCENPMIERXINEFNTBCRX
RTCERFKANTGLEUZAUCMTTFEAABQNMRXACFVYXARIUTIEFCRTCFPLEGUECFNONT
XALGHAMVQNTPMPRFYLNWATXARTUNRFZVPSIENPATIECTRTEAFCXURFZGNQVCQG
RIUMXCEARFVFNTPMTFFCATPMIERXINEFPLTADNBANZCMXPRFCFVKMPYKHRRTXZ
IENHSKLFSBDCGSBCNQQNPDYKXMIEATFPMGGLTPLAQGFQGZMGHWMVKNEYHFENIE
MTCTPACFIEATBYPSZASKTKPHIEFCRXYKXMIEATWDFRATUNRFOQTNQNABGQDMGV
MGBITPPMHWTFRFCEMCNTNTBVMTHURIAXURQWDCRFFSMGCFNKOVRIXCPMAFRXFC
XCIEHTTPFUHAPXYOIEMXLPEXCTUT

Plainteks dienkripsi dengan program *Playfair cipher online* yang dapat diklik di sini:
https://planetcalc.com/7751/

IV. Kriptanalisis *Hill Cipher* dengan *known-plaintext attack*

Pada bulan Desember, wartawan Tintin dan teman-temannya yaitu Profesor Calculus dan Kapten Haddock pergi jalan-jalan ke Jakarta, Indonesia. Di Kemayoran dia menemukan secarik kertas yang berisi tulisan terenkripsi dari seorang agen negara Moldova bernama Bob. Tintin mempelajari bahwa surat-surat dari Bob kepada Alice selalu dimulai dengan kata 'Hallo Alice My Love' dan diakhir dengan "Bob". Bantulah Tintin untuk memecahkan ciphertext tersebut dengan *known-plaintext attack*. Surat tersebut dienkripsi dengan Hill cipher, 4 karakter setiap kali enkripsi.


```
NPZMLQNLKGGAQAPRBCDVNJHVDTGDZYDMNMDVDPNZXMSEITWHCNNXSIGCYWSYXLAHVADG
QTDJPJAOCSFPFZOJXWPHKEBXZZCRZBMRCQPHPQJRBBQWBGWYUPABGPNBSSZTBHJDLLAV
AVVDTNDYXKACUQFZPWVVRGLUSIUOWIJPEJFKJDYZELHTLVMTRGLUGGJJRBUVTBUGKUSE
GNIDDBGZXMRYKSKYNLYDCQPHTAHHCIPTRONXTSIIEDWSCCXXWRRHWQMIZSRXVMJBLDZM
VKVEMJJPAPBXRARTIIDFELHTLVMTVZWOGYNZZYDTAEBJEUKMLQFUKQMSUIFDHLKFRCSE
TBMJWOWCQZATIWMIZEZRSKVFZWNLYIMUNWYKJJJTNEESRONITILVUKPAZUHTAAJLM2TX
HCTHZUKEAETEHYIMUYYDHPEWMSCIYOYRZWCBZICBTKUKQIJDZGXLJGOEMPOZHKFNDBEP
ABIDYOGEGEACWDKRKOWIQJLJMGQYGJNEXJQLMICHNVYMWUQHHOMLJHDWEVEKITWDAASM
AUGTRQLKFBFYQEMUSHLKFWFXJYIMUZSPRNXQANOASDADCBTWVPPPMFFSZKIGCZQFLEUW
SWNUVFOQOAPWPRCNAPLMBTYJXCSFPRMVS
```