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

Tugas 1 IF4020 Kriptografi
Semester II Tahun 2022/2023

BAGIAN A (CIPHER)

Buatlah sebuah program kalkulator enkripsi-dekripsi berbasis web (web based) dengan bahasa pemrograman bebas (Javascript/Python/Ruby/Golang/PHP, dll pilih salah satu) dengan antarmuka (GUI) yang mengimplementasikan:

a) *Vigenere Cipher* standard (26 huruf alfabet)
b) *Varian Vigenere Cipher* (26 huruf alfabet): Auto-key Vigenere Cipher
c) *Extended Vigenere Cipher* (256 karakter ASCII)
d) *Affine Cipher*
e) *Playfair Cipher* (26 huruf alfabet)
f) Hill Cipher

Bonus: *Enigma cipher*

dengan spesifikasi sebagai berikut:

1. Program dapat menerima pesan berupa *file* sembarang (file text maupun file biner) atau pesan yang diketikkan dari papan-ketik.
2. Program dapat mengenkripsi plainteks. Khusus untuk *Vigenere Cipher* dengan 26 huruf alfabet dan *Playfair Cipher* dengan 26 huruf alfabet, program hanya mengenkripsi karakter alfabet saja. Angka, spasi, dan tanda baca dibuang.
3. Program dapat mendekripsi cipherteks menjadi plainteks semula.
4. Untuk pesan berupa text, program dapat menampilkan plainteks dan cipherteks di layar.
5. Untuk plainteks berupa text, cipherteks dapat ditampilkan ke layar dalam bentuk:
    (a) tanpa spasi
    (b) dalam kelompok 5-huruf
6. Program dapat menyimpan cipherteks ke dalam *file*.
7. Kunci dimasukkan oleh pengguna. Panjang kunci bebas.
8. Untuk enkripsi plainteks sembarang file (khusus untuk extended Vigenere Cipher), setiap file diperlakukan sebagai *file of bytes*. Program membaca setiap *byte* di dalam file (termasuk *byte-byte header file*) dan mengenkripsinya. Hanya saja file yang sudah terenkripsi tidak bisa dibuka oleh program aplikasinya karena header file ikut terenkripsi. Namun dengan mendekripsinya kembali maka file tersbut dapat dibuka oleh aplikasinya.
9. Beberapa pustaka untuk menghitung balikan modulo, matriks balikan, aljabar linier, diperbolehkan.

BAGIAN B (KRIPTANALISIS)

1. 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 Inggris 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.

```
CZWKWFKWUFKNXHLCZWXKNWLFLCXQZWKWCZWCWKEUNSNJPXKNPNJFCWYXJWV
XXSLCXCZWBWENJNJWGKWBNIUNSEWFJNJPNJVWCXKOFRQZNVWXCZWKLAVFNE
CZWZNLCXKNAJXKQWPNFJLWCCVWEWJCXBUNSWJNLQZWKWCZWJFEWYWKNUWLZ
WJAWUNSNJPLQWKWCZWXKNPNJFVYQWVVWKLXBUNSWJFVCWKJFCNUWVRKWAXP
JNLWYWCREXVXPNLCLLHAZFLFJFCXVRVNOWKEFJGXNJCCXCZWXVYJXKLWQXK
YUNSFEWFJNJPLWFENVWCZWLGFAWVWBCOWCQWWJCQXKXQNJPOXFCLNJAXJUX
RQZNVWXCZWKLKWBWKCXCZWCZAWJCHKRFJPVXLFIXJGXWEQNYLNCZQZNAZKW
BWKLCXLAFJYNJFUNFJGNKFCWLFLQNANJPLKWPFKYVWLLPNUWJCZWLAFJYNJ
```

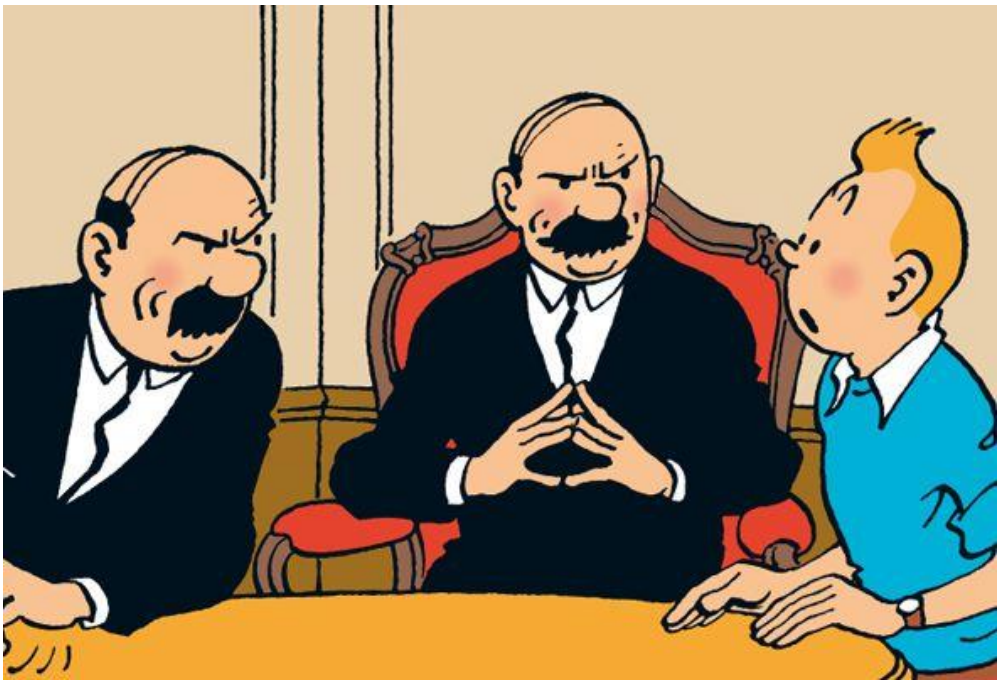
FUNFJLYXENJFJAWXBCZWLWFYHKNJPCZNLWFKVRGWKNXYNCQFLJCVXJPHJCN
VAXJCKFLCNJPJFEWLQWKWOWNJPXBBWKWYHGORUFKNXHLXCZWKAHVCHKWLFA
KXLLCZWGVFJWCCZWFKFOLLVFULFJYORDFJCNJWLBXKWIFEGVWSJWQXBCZWL
WKFNYWKLFLKHLXKKZXLKWVFCNJPCXKXQNJPQZNVWCZWPWKEFJLVFOWVVWYC
ZWEFLFLAXEFJJNFLZEWJFVVHYNJPCXCZWNKFLZQXXYOXFCLXCZWKJFCNXJL
LHAZFLCZWWJPVNLZFJYAWVCLLWCCVWYEWKWVRXJYFJWLZWFCZWJLXKGFPFJ
LQZNVLCCZWNKNLZKWBWKKWYCXCZWEFLYHOPFNVFJYBNJJPFNVYFKSFJYBFN
KBXKWNPJWKLXKTHNCWLHNCFOVRJXKCZEWJPNUWJCZWAXEEXJAHVCHKFVGKF
ACNAWXBCXKEWJCNJPAXFLCFVLWCCVWEWJCLFJYEXJFLCWKNWLNCQFLJCVXJ
PHJCNVCZWUNSNJPLBWFKLXEWKWGHCFCNXJLGKWFYCXFVEXLCFVVAXKJWKLX
BWHKXGWFJYEWLXGXCFENFCZWKWNLWUWJWUNYWJAWCZFCCZWUNSNJPLKWFAZ
WYOFPZYFYCZWAWJCKWXBCZWNLVFENAWEGNKWFCCZWCNEWCZWUNSNJPFPWFL
AXEEXJVRKWBWKKWYCXVFLCWYBKXECZWWFKVRLCXCZWJXKEFJAXJTHWLCXBW
JPVFJYNJCZKXHPZXHCCZNLGWKNXYCZWUNSNJPLHLWYCZWJXKCZWKJFJYOFV
CNALWFLCXCWKKXKNLWJWNPZOXHKNJPSNJPYXELWICWJYNJPCZWNKNJBVHWJ
AWCZKXHPZAXEOFCFJYAHVCHKWHJCNVWUWJCHFVVRUNSNJPLAXHVYJXVXJPW
KOWEWKWVRYWLAKNOWYFLAXFLCFVKFNYWKLAXJLNYWKCZWBFACLCQXUNSNJP
SNJPLLQWRJBXKSOWFKYFJYAJHCCZWPKWFCQXHVYFLAWJYCZWWJPVNLZCZKX
JWVWNBWKNSLXJFJWFKVRNAWVFJYWKQXHVYLWCCVWLZXKCNUWYAXVXJNWLNJ
JXKCZFEWKNAFLAFJYNJFUNFJLQXHVYWUWJLWKUWFLEWKAWJFKNWLBXKCZWO
RDFJCNJWWEGNKWNJLZXKCCZWLWQWKWJXEWKWGNKFCWLOHCCZWBXKWBFCZWK
LXBFGFCAZQXKSTHNVCAHVCHKWCZWEXCNUFCNXJLBXKLHAZWIGFJLNXJFKWL
HOMWACCXYWOFCWBXKEXYWKJZNLCXKNFJLCZXHPZCZWKWFKWAVWFKNJAWJCN
UWLFLCXQZRCZWGXGHVFCNXJXBLAFJYNJFUNFENPZCZFUWFACWYNJCZWQFRC
ZFCCZWRYNYYHKNJPCZNLRWFKGWKNXYXJWKWVFCNUWVRFGGFKWJCKWFLXJNL
FLAFKANCRXBKWLXHKAWLCZHLBXKANJPCZWUNSNJPLCXVXXSBHKCZWKFBNWV
YWUWJKXOONJPFJYSNVVNJPAVFLLWLXBGWXGVWOVWLLWYQNCZFEXKWOXHJCN
BHVZXEWVFJYFJXCZWKGXLLNOVWLCNEHVHLNLCZWKHVWXBAZFKVWEFPJWFJY
CZWKWVNPNXHLGWKLWAHCNXJCZFCQWJCZFJYNJZFJYQNCZNCQNCZAZKNLCNF
JNJBVHWJAWLWWGNJPWUWKBHKCZWKNJCXYWJEFKSLQWYWJFJYJXKQFRNCEFS
WLVXPNAFVLWJLWCZFCCZWUNSNJPLQWKWVXXSNJPCXGKXCWACCZWNKGFPFJO
WVNWBLRLCWEKWLNLCMHYWXAZKNLCNFJUFVHWLFJYWUWJCFSWKWUWJPWBXKC
ZXLWLWCCVWEWJCLFVKWFYRVXLCCXFEXJXCZWNLCNAYWUXCNXJCZNLNLJXCL
GWAHVFCNXJCZWNJCKXYHACNXJXBAZKNLCNFJNCRQXHVYAXEWCXYNUNYWJXK
QFRBXKFVEXLCZFVBFAWJCHKRAFHLNJPHJCXVYOVXXYLZWYFJYAHVCHKFVCK
FJLBXKEFCNXJNCLZXHVYFVLXOWJXCWYCZFCYHKNJPCZWUNSNJPFPWLAFJYN
JFUNFLAVXLWLCJWNPZOXHKLQWKWWIGWKNWJANJPUFKRNJPVWUWVLXBNJJWK
CHKEXNVCZHLPKFJCNJPCZWUNSNJPLFJFYUFJCFPWQZWJWIGVXNCNJPCZWLW
VFJYLBXKQWFVCZLVFUWLXKCWKKNCXKRCZWLWFKXHCWLHLWYORCZWUNSNJPL
QWKWFVEXLCWJCNKWVRBKWWXBXGGXLNCNXJVWFUNJPCZWKFNYWKLHJNEGWYW
YFLCZWRCKFUWVVWYBKXEXJWYWLCNJFCNXJXBGVHJYWKCXCZWJWICCZNLOKW
FSYXQJNJQZFCZFYXJAWOWWJFGKXBNCFOVWJWCQXKSXBCKFYWKXHCWLBXKWH
KXGWFJSNJPYXELAFJOWZWKFVYWYOFASFLBFKFLCZWAXVVFGLWXBCZWKXEFJ
WEGNKWNJCZWCZAWJCHKRFJYVFCWKCXCZWKFGNYCZAWJCHKRWIGFJLNXJXBN
LVFENAGZNVXLXGZRCZWWJYXBCZWUNSNJPFPWAFJOWGNJJWYYXQJCXFJHEOW
KXBBFACXKLBNKLCXBFVVCZWBFVVXHCCZFCXAAHKKWYBXVVXQNJPCZWAZKNL
CNFJNLFCNXJXBLAFJYNJFUNFQXHVYZFUWHJCXVYWBBWACLXJCZWKWPNXJLY

XEWLCNAFJYBXKWNPJGXVNARORCZWCZAWJCHKRYWJEFKSJXKQFRFJYLQWYWJ
QWKWWBBWACNUWVRAXJCKXVVWYORYNXAWLWLVWPNCNENLWYORCZWAFCZXVNA
AZHKAZFJYZFYBNKEVRWLCFOVNLZWYCZWELWVUWLFLLWGFKFCWSNJPYXELCZ
NLEWFJCFJWJXKEXHLAHVCHKFVLZNBCNJCZWGKNXKNCNWLXBLAFJYNJFUNFL
VWFYWKLZNGNJCZFCLWJLWCZWUNSNJPLQWKWJXCYWBWFCWYOHCFKPHFOVREF
YWCXOWZFUWNJFEFJJWKCZFCBNCCZWANUNVNCRXBCZWNKTHNASVRCKFJLBXK
ENJPZXEWVFJYLBXKWIFEGVWCZWEWYNWUFVAZHKAZEFYWNCBXKONYYWJCXCF
SWBWVVXQAZKNLCNFJLFLLVFUWLPNUWJCZWBFACCZFCLVFUWCKFYNJPQFLCZ
WJHEOWKXJWLXHKAWXBGKXBNCBXKCZWUNSNJPLCZNLKWEXUWYFPKWFCYWFVX
BCZWWAXJXENANJAWJCNUWCXCKFUWVFJYKFNYXUWKLWFLCZWJWQVWFYWKLZN
GFVLXAZXLWCXKWBXAHLCZWNKENVNCFKRFCCWJCNXJBKXECZWSNJPYXELXBC
ZWQWLCFJYNJLCWFYGFKCFSWNJLHAZAFEGFNPJLFLCZWOFVCNAQFKLFJYCZW
FCCWEGCWYAXJTHWLCXBMWKHLFVWEBKXEZWKWXJXHCNCLWWEWYCZWUNSNJPL
QWKWJXVXJPWKFKWAXPJNLWYBXKAWNJCZWQXKVYCZXHPZCZWNKOKHCFVNCRO
KFUWKRFJYLCKWJPCZQXHVYVXJPOWKWEWEOWKWYORCZXLWQZXZFYXJAWBWVC
CZWLZFKGWYPWXBCZWNKOFCCVWFIW

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

2. 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.



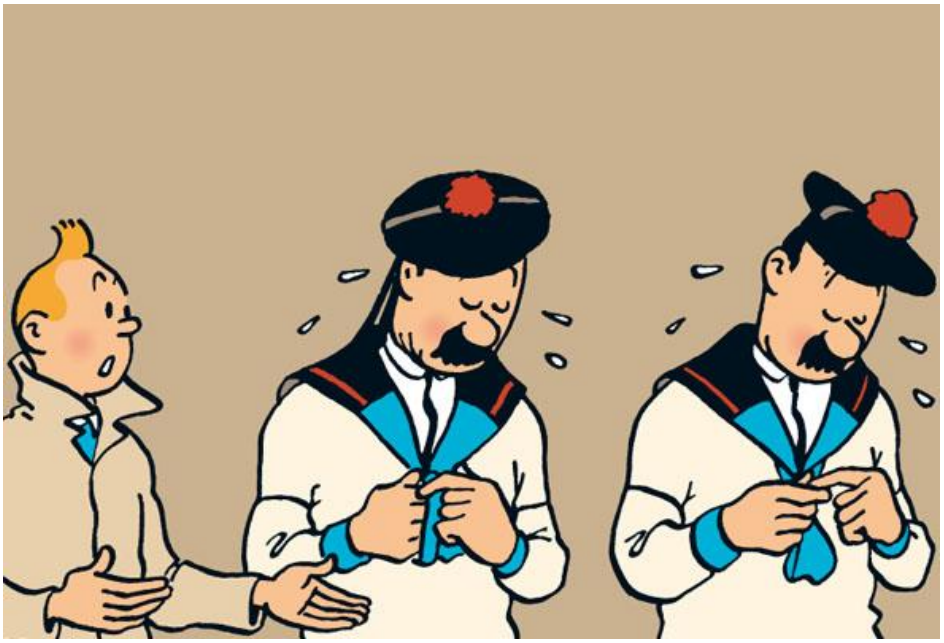
Anda tidak mengetahui kuncinya, namun anda diminta menemukan kuncinya dengan metode Kasiski.

FSIKTSZDRCZEUGPFPOJWXRKCXVPVOQGSNESTECHYYEGKPCNOZCQMJTSFEVY
SZEPXEDCCBGAGAHYHQCXRUSOKSTJCAUUSZURCEYTMJXDKWHZFEZRLETHHSS
LMEQWZMCYCLJNOAZSPLHNGFXESIHSSXCVWOUQSTBLMEQWZMCYHNYGAERPPP
ROQPYOYIRNIXGBYOGWKSOZPREZOXRZKTRBFWREYPWYMAIKLXVPZGPTIOZPO
VSYGAWKAXVPOYRNWEGEBOWYYISHIEBTQRYXIETXVPAOBQPAZLSCSOQNREYP
OYRIYYPAJWOXCYGEMOREBOHNCZEFUVWEMUDGLAVSDFZGRVSJGVCFBJRBFWR
EYPWYZNXWQXFTPKGGMOKWHTAGRRHPNEHECHYYEGKAODTUPZIZJYFTBMYAIT
VPCDWULBJWHSIEMKYEWWMSKSWIFVWWTIFFDZGBROATSCJUJPEJUWIASXTBP
YGRCEVGRVWIUYBEHUZNAETHPWCCLISHIEBTQGQULWYWDCSGBGSDGPTEVKCN
VPNJFZAIFVRWZSGZIZFNJNOGOPJKLDYEZIGFFVPVWETKPPQGSFIEZXICBYM
HXPNIGAFKYQSBZLSOIYRGSXKVSNCXBRHQVXCEVKLBVPNTCWSZFRINATHTCT
MPGQXVSOTUPBRACISVOTBGLAJYGEPAPFXNKEQSSJIVPKSIHPFYYOSRKWSLZ
KTRPPNISGWJCAGALSIYRGJFSNKMBQCXARWPNIBZHOMAXDGXHSSLMEGAUJHS
SKPHTPOSBLBJGGWKIIOYKGTRWYUYZOOTLVLEREHPZODRMJGXZLBZGFXDOWW
YQOBRRPIEIDSJKNWOJIOEVLMYPKCIRMMZFRITZMBNHOMASBYSAPGVCPMAYE
QNCXBVRCZSRYOKTVHATGSEVOQRVQVXWZBGJFSONVOYYZFRRQSFSCCLNRSLR
IHZOHMHX%KLXVPHURNPDAQOYDUNHPWZMCYCLRUIAGVHSOZRUEPZMAPOHMHX
IOPZTCTNRSLRIOQHKPGLAKVIAHOMAEYGPRPFGUNWBUVAPRCFVGDZLSYTOJY
IZCMHSKGRRVWTHPPQGKRADGXWDBUUXRKCRODHUZNPWQIIAKGPQTNKWGFFKZ
LXDKQORAGRUEPNEGYCZWRXYUQSZIZANYOKWHSSKKRVCKRQPCLQNQKYMFTGR
YAHPNIFPWYYYWKLSZVZUPREXUYHECHYYEGKMGDOOBUIOGMRLHOKRADKRHSS
XCJEOGJOCAKPAEIKHHZPGUUSSKRHQWYFVRCZSHSSXGIINZSUPHLGFLPUIOE
HUZNKAZWOMWMYAHXKEIEWLSYJEYLPFHNCVWOAVDCWYCQXDGXHSSLGFLYGRH
LZQYCTWXIBEZERUIBOWVTGZFRMJIEFYOZGBRKLEDCWTARWOCLCHOYAHVOKH
TZFBGBPWZMBRHNCEYHKWCQHNCXMJMHCXOYYGLWTOMZILMELWBMBRFKJREOK
HVPFLPBQPNIQFFYCGLAVVWYQKQFAWYQOCFERBFWNSKPJKPGLAXIWDCTCCVK
SMGPHNYGLWYFSPBGEEIAJYDZBZFRCONSIWRTMGXARPOYMULRXDGXHSSVPVR
YKWGTGGDVWDLVCXHNCZENXMORSCYFFKXROMCELNQAJWOXCYGEWWSSGTFMPR
AETXCLJKPLLWTHGZAKYAHOZVCYUHMLFQZXVPFKYEIDGFWEGZFNXWSENPSBC
ECKTIVPORUNCOLISWGNSAKNEEBOBKTRVOGXWDTOCQEHRXVPTUMQVWZMCYGG
PREHCEMDRKTBYNKHKTHNMHXPNIFPGZSAXERSBPRGWFEIUWWCOYQVKJKHHZR
KJVZAXJCZRLMELEYJOEVKPVRPNITTSRBOYPZLSQCUBAIRKVQLAKRBFWGPGZ
OVNESWILSOGGKBWEXEBOOYIRHSNIFPHNCSSKJJCCVOKOYPYEAZGOPNHIOXH
PRZFNXPNITZCJGFEHXIOOMKYGIJZSPLKGQIINEEBRFEYAHQTOBZKOLTPUHV
SLYYFVWLXSATGKZLWWEMBRGULBJWLMGSGGKBWEXMAXSJGNXARCQZAVJNMJK
HHZVOQZSPNIFTTNCPEHRIRLGULBJWLMGSHNCCVETGSDGCYFHEYEDACOLGIZ
HIQLIYCUINNYGMOTBUEOHVCVSTRUILXSATGKQUIYXMSOORMGEJJXCWRYYZS
OOVHZFALGSPNIVTUNFVPHYYROSTJLZAXCVPOBWEEETGOXSJMJRSOXVLHKPE
MXRIZTUNRAMJMXVPKGRRVKBIFQZUURHPUHFZKTRUIATXWCSBGYPWMIHSSVS
QHHKXICBKBVRPUEZLYKRUEPOWBZKIYYPAJXCMORYXIPNIBEVKGFPWTHKSSX
CFEIUWWCGNCYXAXMGNORJRHOGQCDWXGFPWTHHSOZQGLANMGECXWBJPUFOWO
QCGLWZWGZITGDYAXMUSHODLSQBMGTHZMOEHGOSJCAANRBKIZEVKABSHGXAZ
GVFRVAUJHSSRYXIWIGCXDGLVIZHCPPOARVJQRZWPKYMSWWSSGTFOQYEJJ

Setelah menemukan kuncinya, dekripsilah cipherteks di atas dengan menggunakan program Vigenere cipher standardd yang telah kalian buat pada bagian A. Editlah hasil dekripsi tersebut sehingga enak dibaca, tambahkan tanda baca yang relevan jika perlu (karena program Vigenere Cipher yang digunakan mengabaikan tanda baca).

3. 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.



QUKAROQULALPKHBUSHPLIWIDCSCYGRBAUXSHBUSHAGCFHZQCQBWUZCBKECI
VDGFQDGFAEALASHBPKNPOBLHZFXFMBCFBMEALALXDUGWUZHXDFQFTLUSHKN
LVCSANSHXDUGWUVCMOCLCSENMLKFHEQUVFUGZDGDMBZSCZEMZHXDFQFTIDP
WPCGRDQRUQCBLCZGROWVCRVBLHZUQZOSHXKDKFAILKBKGFQKBXDBLBLFBKZ
CHHAFTLUIBKZCHUPQMQCTHPWWOEAIVDTQPBUSHQBWUFTLUSHBKIDPWPCCHX
KABNVROQUBLCZLGBAQBWUFTHOSHBLWCHLRVUMSHBPAHCYWCDIBLLAGLCLCK
LGDIEMZDLRACPZQBWUEMBKLCZEDMWOFTLCZEMLKFEMBLCZPWWOQCBLCZGRO
WYCTKSAMPQUCEBANULEBMSHLELCDGRVAMCHCTHLBAUXDSVCMEOZLGBAEMQB
WUFTLCPBCHEMTHPWWOFTILKBLEPKVCMEZEMLKFEMHEQUVFUGZSCZEMBLKBA
EPUAKLMHAIDLRAMHZUQXYZDLRACUGZDFBBLAKLGDIVCZEPUBUSHONKZFBIG
CHCEBATKZFKTLEIOEMZHLUSHIPFQUMPCUMLGOMAHECUQBLKBXDEAZSCZEME
TACRUGKTDUWVLBTRUXKWCLCUGLENDLBVFUGZSAKWCDIUQUTACNULEALFNQU
KZAHZHZSWCDIOBKXEMZSKBGREHCTNVZSHSCLCVQUHCNKTDDMPCGRIYHDEMM

EUGZDFBZSHZUMWOGRKNQUUMKGALUGDMPCCHLASHBPAHKGRGALUGMEGIDMPC
GRIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPMLUGHPBLAEKLBKMBQ
CLMMASHDMPCGRIYHDEMMEBQZCBKLUDSCWONKZFBKTRVBLAEKLBKMBQCLMMA
SHBQSHVCPZMERLQEHKGCPUZSAFBFVULERVBLAHPWPCGRIYHDEMPZMQPCABS
HUNRUSERUQBWUZDLRCZEMINWUGRDNMKUGINCZOPBKFTLOPUHEACRUGKTDFT
OUSHBQSHVCPZZHZAFNACBPMDHOSHVCMEZEACRUGKTDEMBLCHFVFTLOPUHEA
CRUGKTDBLFTBLFSBCFBSHBPAHECUGQUKAZDFBBLFSBCFBEMFAILKBDMPCGR
IYHDEMMHPWPCGRIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPMLUGH
PBLAEKLBKMBQCLMDGALBQZCBKLUDSTCNUECPKKBBLFTLMDVDSKTHSKBAHCL
NYBCFBTRAVPUHEACRUGKTDMBGDDGPZQBWUZDLRACPHZCFBBLFBBLFSBCFBV
CPZZSWDFALCUGURNBCHZFIVDMVCUGINKZFBXDBLFBWZKNPOBLLADSRNZDFB
AZKBZSAHPWPCCHLAQBWUZDLRHSKBSHKTBLACZAIGBGKBTNACMBZSHSLACHB
LFHPKHMPOCDLEUGFBWZFTIOKPHCINCZLGHLKBFTILGHSHKPBGKBSHKTAMPI
ACZCCHMPBLLAZSHSCLUQSKCKCHFVPURGHLBMSHKCIVHALCDBBUMOFTFTHOK
LLUCFABSHEDGDLCVCXGBUMUSHCQBKMBDXGDGTMDQUHFBILTHSKBGRQVPHHL
RAGDDLKBFTHUKPFQSATEKFSHBIACNUEMLAPCFBBLHSRBBMVLUQEHZFLCUGU
MPCSHTKVCZNRUZDFBSHLEIWIUCVBGHPFRGKACUGVCMEUSRUUMXPKBKAQBWU
ZDLRHZGRUQKABUSHKTBMSHEHLFBUWUKZKSFTHOKLLCLIACBIRBBMVLTGACZ
ASAQVDGEADXGDITRBCVFVGRUMBLCZGDGCPUHZALUGBFZAUKPOHSPOACLFGR
FTLCPZZSCZEMMPEHCTRLCNMASHDBBUMOFTLEIOLRWQBGKBFTHOKLIURBCVF
VBLFBWQROPWPUEDGDLUSHXDDIEHEMBMXDIVHMPWQULEZAHCWMRNCHWQRUDS
NDLBSHFTGWABLRZHASCHEMGKEMUMBFLEHUKZFBUPIVHAGCUPSLHPSHKTBMG
RKALRVCQBMDQUHFNBKZCHCNGAPULGVAPCGDDLKBFTLCMEWQRBHNMCKPBORV
BLFBKCSANRRYRGFQNZSHMBETEHIGALUGDCUMRULRZSACNUFTLUPWPCLRUMB
LFSBCFBEMXKPWQCBLLABLAKLGDIVCOHACLUSHDWPCLELUPMLMRVBLHPFTLU
SHXDKFCHONKZFBLAKHALUGBLWCHLBMSHLEHCLAFBBLHSACNUQCQBWUZDLRH
ERUUQVUSHQPPUEDGDOUEMLMMLDMBFGRBLFHBKLACQBKMBFTHOMUKBKPKGCH
BLLAZSAHPWPCCHLAAZKBVGACCQEAZANXUNKZACUGIGGUMUFRWUZDLAUMOWB
LFBZSHEFHFTUMNRTFUGTKUQZABPLEKXMBQUHZFTLUIBWCHLBLPUBQFTLUSH
XDDIEHEMBMTKRQEMBLKBTRULGISHNBSDKTOMSHTKTFMHQULFZSKBEAABUWT
DIHWCBUGDLRVCMEMVPMBAZARGFQBLFBZSHZCVLMLRAMAKMUALHFFTOUFBRL
BUPDRVUMBKMBSHBPAHEAZANXBLGRHGBUSHDWRVALHFVCPZMOLMHTRUBFLAK
BFTODHAFTKBBLFTKCBTABMDLUSHBKVCMEALTHCSUYLGEDVCMEZDLRAKMWKB
FTHOAZFBDGRVAMKSMLBAMEUGQUACEDMILAACDGRVAMHZQPQUOPBKMWKBBLK
BCZKBHZAZFBDGRVAMAFRGZAMEUGCQKIMEUGZHZATGLRAMASNDMELFGRMBBL
CZLMHMUMWOZHZATGLRAMHECHPZPHHCNZPHHCFTODMWKBCHXDBLQBWUZDLRA
KWCBUKBMKBFMHLRAMHZUQXYZDLRCZEMMPDBFQNXFTLULGBPNVBLLAZSACBA
MPSAZAHFALTHHZFTHUBKCLKNPOACEDMILAACUGIUFTFCIUPQQCXDBFWCUME
ACKLSNDCQBPSHIGGUMUXDZSUMALFALMGAUPOPBFQUGVBLFBEMZSCZEMMPRL
BKHOSHMLGISHBPAHCGWUUQUQBFQCBLAHLRAMHECHZERUUQBFQCBLASOBLRC
HSHUPBFVCMBPWMDQULFUQBLKBUMPMDSNUTRALAMEMBMSHCQRBLULERVBLHZ
AZFBBLQUCZEMKPHLALUGMPZSKBASKLBFIGRGBMKLLCXKFVKBFTOUFBRVUMM
HKZKSZDFBLRVCMSRDBALCKIBLCSYUKBMPANSHDWRVALHFKCSATEKFBLFZZC
BKZHZAUGVCNKOZDSOCLFUGHCMTCHGRBLASWCBUKLBQCQUPBKBLFZDGRVBLK
HBPAZFBKCUGHAMEUGEMLRVCQBWUDGHLUVLRLGBUSHDWRVALHFBLFZMEVULE
BMPOCSBFLEHUKZFBBLKBAEPUAZKBVNLGFQVCQBMUGRBLHZLVCSUIKBGRZDD
KLBSHZGCLHAANLRBLAEPKMBMEGIZDSDEMEHFBPHRVRLFQQUQVEDKLNUSHZH

DWUGZDSDEMEHFBACRLFQQCAQXQMLBABLABLGUIZDSDEMEHFBALIPFQMPSAQ
CQVTNACLUSHCQRNBLZDSDEMEHFBACRLFQQVZAHFALTHHZBLAEGKBLZDSDEM
EHFBBOGRLQNGPUARSHPHVRDZDSLEZEKZFBDCRVRLFQXDBLQVFRGKABSHZHZ
ABUDZDSLEZEKZFBIUGRIPFQWCUMAQVQNDBLFBBLAEPKMBDMPCCHUPRBLCUG
MEVULERVBLKBCZEMLMLRAMHSMDCSBGHPEHLCUGSHMEGIZDSDEMEHFBHFRVR
LFQGRUMQVEHLUSHMUSHBPKCSAROFTHCCKDELMHAOWRUMPSAUSGWLEZEKZFB
GVGRHGTQZNCHUMSURUBLHZAZFBBLZDFBSHDMPCCHLALGZECHMEVDLRAMHZU
QXYZDLRCZDSVCMHXGFQEMHAKSBLKBKHTFUGSHKCIVHALUSHMUSHBPZDWDLV
KBRBRGFQROFTLUSHWFKPCHWCUVLRLEMBQUHPLSFBALUGTNWCHLRVBLKHBPA
ZFBDGRVAMAKFTIDHZFTIDABBLAHGHLBECIVDMTGLRAMHZUQXYZDLRCSIZSH
LTFBMPIZSHLTFBOEKPCHBLFZZDLALMMWAHWFLGDIFTLUSHZXKBHZQDMLLUL
ERVBLFZIGGUMUVCFASHNRSRRUHABLKBMHKZKSQUGRBLHECHFTLUSHZHZABU
LIVCNKMHKSUVLRIZLGOEPOMKRGQUMPBFDSRNXDBLACEDFTHOQDMUBLUPNDL
BSHRGHLUVSHRGUVEMOPNBGRHDLRAMHZUQXYZDLRACUWFAFTOUEMKNGHLBFB
CHZDFBZSHZCVBLHZAZFBOUKTEQTRRVBLFZZCBKKNHKUGGVFTLCPECHSHUXL
EBLKBTFSAVCMONFLVKHPZQBWUZDLRHZSHFTOZKBCHDSZDLTFZWCDWSAUMWC
BIWCZHMEGIBLCHVCNKMBSHBQSHUMDIBLASBLLASHBPBAQOMUSHBICLXDZSC
HUMLEZASHKIGDHAHURUBLLABLHSRBBMVLBGCLMQKTCHSHTIGKACUGBLLAZS
HSCLNRFGPUBLCZDSHALCWNBUGDLAMLMBZSHSCLCQRBLUSHPKOUAHDGFQBLC
HVCNKPZMEGIGKWQCUGDMACFAKKTCSCQRNDSBOAKPWPCVLFABLHECHOZEMSZ
CZFTICRGALUGGKWQCUGDIAKZKSAZKBVNLGFQBFLAFTODHAFTWQCDFTMBFVX
DBLBOFTGWWCZSLMDVFTNAPUUQBLGRQNHZMEGIQBWUZDLRCZLRLEIVMVZGAC
NUFTHOSHMBFVCHXDBLBLASZSAFKSRVBLHSWCZHGRPUHCNKPUBLASGRBLASP
URGFQMBSHZXFBRVUMBLASWCBUKLBQFTIDPWPCCHCQUKPQSKTKUGDQDIGRBL
KZAZFBGRHQBLFZKCSATEKFFTLUSHBUSHPKOBXRSKBICLUMEHBKCLVNSHHGT
IVCMEDMBFBLCZDSHALCZQMUSHDQWOOUKTEQVCNBCHSHTKUGMEGIEHVCBKQC
WQRNMBKSOPBLKBZSCZGDHMPWQUFRWUBLLAWQTCBKSHBKEHOBBKUMHAUBPWQ
UAKPOKHBTRUBLFSBCFBEHDGAZGRLNLEBMSHLEHCLAFBQBWUZDLRHZSHKTUA
WCDIUQUTRUBLGRARLEBMSHVCMELFGRBLAEPKMBFTLOPMUTACRUGKTDQCLMM
LUGZSCZFBRVUMSHTIPWPCGRIYHDEMMEUGMEGIDMPCGRIYHDEMMHPWPCGRIY
HDEMMPBUSHVCIVDVDSGRBLHPMLUGHPBLAEKLBKMBQCLMMLUGBLFHMLPZMEB
QZCBKOWGSBCFBBLWCKTNAKLBKMBQCLMDGZHHERUMWKBBLHSGDHMZDKBABSH
ZHZAUGVCNKOHZCIVHMUQXYZDLRKHPZMBGDMLDGZAFTOUAHMLUGUQBFHPMPE
CPKEMZSABSHBQSHVCMEMBWCUGCHCQBPSHFRCZBLLABLAHPWPCGRIYHDEMQB
AZKBMQPCAELMZHGVFTHOSHFRCZBLLABLHSRBBMVLBGCLEHUNFVCHSHTKUGB
LLADGRVAMHZUQXYZDLRCZEMMBGDMLDGZAFTHOPMSHBLWCHLALUGBLWCHLAL
LFGRDSZOSHPLHLRAGDDLKBCQBPMDQULFPZZSCZEMUQRVBLAEKLBKMBGRBLC
ZDSHAMLUGFBWZHABLKBLEZAUQBKMBFTOUSHBQSHLELCAMEMRVBLWCHLUMEQ
POABLGFQUMOWZSKSKLBUCHSHNKCKACUGIUHZZHILKBZHGADGFAFTMDIOCHH
AUXPOFTFTGUPWQUAKWCDILEZAFRWUBGKBGRBLHPIGQHRDZHZSCZFBUMZANU
SHZHZATQWCBUKLBQUMBLHZAZFBOUKTEQFTICUQKFCHLABLCHPWPUFTODKPC
HXKABNVBLGRHQUMZHIVMTKBWFSHKMZANXEDACMILRAMHZUQXYZDLRAHPWPC
CHWCUMANSHXDUGWUFTODLMHAOWRUDQWOLCVQNQPWWOUWVLUYLEBLLTFZWCU
MZHIVDHPWWOBLGRHQXKABNVBLGRHQZSACBQZCBKHOALVGCKHZQCLMDAMDWC
BPFTHOSHORIVHAOWRUQUCZLGEDVCZETKGICHKNPOZFIVDMXUCHFTHUDTHZG
DIPVLVGABBLCZPUBLWQDIUWVLRGBUDSNDLBQBWUZDLRACUGZSCBBTMDBALU
SHOWPUFTHUWCHLRVBLKSBKRVNVMLKAOELGDIMEGIBLCSDIUWVLUYLEALKNG

HLBWQTDPWPCDWSADXGDIVMLKAWQROUPSKTINGPUQUKAQBWUZDLRHSCLUQOB
MQDKDPBTRUMBPWWOEHCQBKSHTKUGHABLKBZHGAEHMLKAOULRLBSHBFVDCKH
ZTRRVBLCSDIUWVLTGCKCHMPONDKAIVFUGMPRLHLAMVNLEBMUQXYZDLRAHPM
BLKBTNACBLFTGCAHDIWUTFPHCGACGUWULKVASHOPMBEHCTRLCNHMKLLUSHO
NKZFBUMSHBPAHECUGTKTFVCNFMUDMFQCEBAUXKTHOGRBLKZAZFBGRLNSHZH
ZAUGVCNKOELVHSPOHERUDSZODSKFCHBLFZZCBKZDFBBLFZMEVUSHPKHCKTD
GRVAMHZUQXYZDLRAHXGFQQUBLFHUPRBLCUGBLLAZSFBKHBLKBMBPKBKGUPU
OPZALCUGZHASCHUMEHHCCLBLFZDGANCHSHNRMKUGEMBLFZMEVULEBMSHVCM
HCKCHUMMUGHLBGVBLFZDCRVBLAHCKHZBLFBZSHEFHFTUMTNACBLACDGRVAM
ACUGCEBATKZDGDAKLVABMDGKACLFGRZDFBBLCHVCNKZSACUIZDLALEILKMS
KBFLUSHZQKLLUSHMDIOCHHAUXPOFTVCQBPWQUKZAHZHBLFTBLCZDKFAGOBC
FBALFAKCBKFTIDABUQQUAKPOKHUYSHUYACBKUQUVLRGZWCTRRVBLCZDKFAO
UPOFTZDFBZSHSCLBKCKSHILPOCZFBRLFGUPBUQCBLFHMLPZMEUGEMFAIDPW
PCGRIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPMLUGHPBLAEKLBKM
BQCLMMLUGLRFTOZKBCHEMEHCQBKSDONKZFBBLWCKTNAKLBKMBQCLMDGZHHE
RUMWKBBLHSGDHMZDKBABSHZHZAUGVCNKOHZCIVHMUQXYZDLRKHPZMBGDMLD
GZAFTOUAHMLUGUQBFHPMPECPKEMZSCZSHBQSHSHKTLULEALIVDLKBTHPWWO
NRZSCHUMSHBIACNUXDBLEAKTCQBPSHMEXOMLGRGVBLLADGRVAMHZUQXYZDL
RCZEMFLKLTFDGZATRUBWUZSHZKLIGXDIVMALGRFQCMPSABLGRLNLEBMLEIV
IMRUFTFBLUQWWCFTHUVNSHSHIMQCXDUADETKANZDDKSZSHRBHCBPUMWOZSA
SCLACQPHPQUWCOEPOTUSHBQSHIGQHRDZHILKBZHGAFTLUPWPCBLHZLESKQC
FTMUSHUPDIUWVLBQPMSHZCBUMWKBBLHZAZFBOPRBALGRMBMUSHZHZAUGVCN
KPEUQKFCHLABLCHPWPUFTODKPCHDQWOBLGRHQUMZHIVDASHKMEDACMILRAM
HZUQXYZDLRAHPWPCCHWCALUGMEGIDQCVFVDKFTUQAMABFTWQBFDWSAGRHPR
OQPZHWQCDFTDMPCMEGIBLCSDIUWVLTFUGORIVHALUSHQPHPQUWCOEPOUSRU
FTILAHIGURXPRMHAEMCHBLFHPKHMWUAHMALEBMSHHABLKBZHGAEHEHDNGDC
HFTOWSKBFLUSHOWPUZDFBBLFZLELOCLACTENIKLBUSHMDOUPOFTMEGIUQXD
XDIVDAPONZWCXKPQKBGVCQUPUFKSPWPUDGRVAMHZUQXYZDLRHSCLUQOBMQD
KDPTFUGHARVBLCSDIUWVLUGMCPZZSKSHAEMCHTRBLKTIDZGCLZSKSRUBLAK
PORHBGKBLEPKBLFTBLKSPDMPRGRGRVUMPCAEEAAUFTLUSHHGTIEAIVDIWUB
QFBZHHAPZQZWCMKTKDQUQENACRUZQKLLUSHXDKFCHUWVLFNWCKTCHQUAEPU
UQVCUGZSCZFBALVCZNRUCQNURBLAAHXGUVEMLMOPMBAZFBGRDYSHBUSHZHZ
AUGVCNKOELVHSPOCZSHBUSHZQCVQBWUZDLRAHXGFQEMGKHCCLROQUBLFHUP
RBLUSHVFUMUFHZBOSKAUCHBLHZBAQOMUSHTKUGBLFZDMPCCHFTGCWCUGBLK
SPDMPBFODPOEZKCUKAHZGCLBLFZALFARGUMRUZDFBQBWUZDLRAKLVABSDKB
ZHGAFTLUMDLUSHOVLEBLCLLEXRSKBFLUSHBUSHZXKTBFILKBQUKAOPBKUME
HROQUSHNITCUIFTLUPWPQFBBLCHPWPUUMUQQUABSHONKZFBLADSSAZCBUGR
KNQUUMANSHHDEMMEUGMEGIDMPCGRIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVD
VDSGRBLHPMLUGHPBLAEKLBKMBQCLMMASHRGALBQZCBKLCZEAEPUCSGSBCFB
BLWCKTNAKLBKMBQCLMDGZHHERUMWKBBLHSGDHMZDKBABSHZHZAUGVCNKOHZ
CIVHMUQXYZDLRKHPZMBGDMLDGZAFTOUAHMLUGUQBFHPMPECPKEMZSCZSHBQ
SHSHKTLUSHHDEMPZMQACARDBPZZSABBKSTHALCUGZSPWPCXDBLTKHFQBWUZ
DLRHZLEIVDIHKZSAKKPCHAZFBGKLRDWMBMOASVGGKABSHBKROQUZSCZFBRL
BUMCONLRHZAKBKAMQUAHXNPWPOZDKBFBPWQUKZAZKBKCSAFTLUSHBKZSASC
LACZANXQPHPQUWCMEXRMICSRUPHHCLRDMPCCHXKABNVZDLRCZLRLEBKODSH
AFMPBLLAAZKBWQBFZDPMCVLRDMFQCHCQKPUTRUZDSCZATKBAKMHKKAQCLRO
TMBOBBKGVIGCZSHBUSHKMMICZEMBKCLZQSHMKGRBAILKBECKAFTIWIUHZZH

ILKBZHGAROEMCKWCBUNXUWVLTFUGMPZSCZFBUMZANUSHZHZATQWCBUKLBQU
MBLHZAZFBOUKTEQZSAFUQKFCHLABLCHPWPUQBWUZDLRKSRUSHBIACOWRUQC
BLCZGROWVCUGMEGIDKFTUQAMABFTWQBFGRBLHZAZFBOUKTEQLEZACQNTGIH
CTQKHRLMEIVMASHMESAUMSAFTOZKBCHBLCZPOFTHPLEIVHMPWQUHFUNGIQC
QVKMMIHZBLKBKHXDIVDHLXFZWCQUFBPMKLHOUQXYZDLRKHLCBKUQRVALFAF
TVNLGFQKTFZWCCETKGIQCQPHPQUMEGIBLCSDIUWVLTGPWPCDXGDDARUBLAC
XRMIKHBUUWXPAKHZWQBCLABLKBCHEDKZAFFTIGXDIVHALABLCZLGBABLACX
RMICZEMMPDCRYRGFQGVVLHCBLLAQUGVBLKBCHEDKZAFVCMQPDMPBFHOUQXY
ZDLRAHQUHFGCPUBLAEGRACXRMIACUGZDFBZSHZCVBLLABLCZPOFTLAKSKTU
MKGBMSHDWTDIUHZHPUBMDQUHFTKUGMBBKUASHOWRUSHBIFTLCUGUMPCBLKS
PDMPUQBOLEGATRBLKTIDZGCLZSACRHUMKGRLBGKBOPRULBLEBQSHEAIVDIW
UUGACLUSHBUSHONKZFBDMPCCHLASHUXLRLEIUACGCTDDMPCFTIDCTHLCHLM
WCLCUGMEGIZDLRACPZQBWUBKLCZEDMWOTHCKFCZHUSFNUWWOBLHPRLSABLC
HVCNKOEFTUQUVCFFZWCROFLKLTFUGZDFBZSACPECHQCBLAHPWPCGRIYHDEM
MEBLPOAHPWPCGRIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPMLUGH
PBLAEKLBKMBQCLMDGALBQZCBKLCAMEMUMGSBCFBGRBLHPMLUGBLWCKTNAKL
BKMBQCLMMASHBGKBFBXLWCZSACNULEIUHZBMQCKTEMFTFBXLWCZSACNUKCB
GLTKBHZRVBLCHVCNKOZSHBUSHWFLVHSPOKHBUSHAZFBGRQGWCUGQBWUZDLR
AHXGFQROQUBLFHUPRBHOSHTNACBLCHUQDMFQKBFTOUEMHCCLBLFZDGANCHS
HNRMIPWPCCHUMZHCZSHBLKBBLFZDWTDGCGRLCFNBLGRIQPDMPUQBORBMLKA
ILKBDWSTCHSHBIKLUXEMSHILKBXDBLVCBATKUGXDBFTRRLUVEMLMDMGFWCZ
HBLKSPWPUEDGDOUEMHCCLFTIUASKLBFIWHCCLBLFZMLGISHNRQPTFRHKBFT
LCIVHMAZFBQCBLASMEUNWCUGLRFTOUKSNAPUSHTKUGZCMRBLBKCHFVMHQUL
NSHBUSHZXKBFHPDFQUMTRNXSHNTRUZSHZRLIVIVDMPCCHEMGKZSCZKBAHLX
GRLFUGMBGDDLCLSHKXBKRVNVBKODSHAFMBSHZQKLOUAKWCDIUQUTRNZGKBG
RBLCHKTFIUPRBLCUGBLFZLELCUNFTMQKTFBUAQCKGUQGQMLPZMOCLHZMULE
BMSHDWTDHUHZKZFBKNPOLMHMGIHZFTLUSHVGKLILKBGRLRFTOUUPBASHNBL
VCBQPRGRLFQMDHCTGABBABPFTLULEBMSHVCMEIPFQOHCTHLBANUSHBUSHXQ
RUBLAKQCKGUQRUROQUBLASWCBUKLTFUGQUCSANSHVLDVFVPZMBFVCHNZLRF
TOULAEDCHLRFTHUPKHOKCSAUMMCUGZCMRCQBPUQXYZDLRAEPKMBFTWUMASH
TFTKZATFUGMLMBCLMWACUGUQZOUQXYZDLRAHFVLMQUHDQULNLPKHBUSHDWK
YKGTFUGZSCHGIUQUALEFQHERUDMPCCHEMGKZSCZKBACMHKZKSCQBPSHVCME
OZLGBAEMQBWUEMBKLCZEDMWOFTILKBLEPKVCMEZEMLKFEMHEQUXGBLKMSKB
FILWUAZKBBLLACFGRHQMPUFLVKHBUMUSHCQBKMBFTOUFBRVUMBLCHVCNKZS
WCZHUMMQFBLUSHRGHLBLHZCVBLAKQCKGUQBUSHOPRBALGRFTLUSHEHCTRLC
NHMUQXYZDLRCZLRLGRGALUGBKCLZDLAVCOZKPRVBABRQPRGRLFQMDHCTGAB
BABPBLFBSHMEGIUMBLCHVCNKMHABSALEZABLAKQCKGRGXDIVDHLXFZWCZDL
AAZKBWQCUFTNAPULRTRRVBLCHVCNKMEBQZCBKOUCZGDGTMUMKNUXDBLLRCQ
TKIVMASHDQDIGRBLCZPUDIBLFBSHMEGIHAAVHSLTKHALMEHGANCQKPKCRYU
QAMLXCZLRDSRUZHKHFQQBWUZDLRKHXDIVDLQUWCTKUGXKHXHSKBEMQVHCKT
HZRMPMZHPZPHQUEMSHMQPCKHBULGOZFVBLFHPWWOOUKTEQUMPCXPNVROQUL
GVLUGLFZALGVASHDWKYKGTFUGUQVUSHIPFQPZMPBGCLLRKCKRKPCHCVFVNZ
LGPZZHTXFTBMQUBLKHBPDSTDHCBPFTIGBLKMSKBFLULERVBLFZMBTOTHCHM
WKBLABKHZUROQFTOULRLBSHZSWDARSHQPHPQUWCMQHKKAQCKMMICZLGEDQB
WUZDLRHSCLRHRVBAUQKYEKLVCSRUQCSHNUIBMCALUGEHCQBKDMFQZSCSSKB
FILKBFZHZDGANCHROBLAHGIQCBLAKQCKGBQLAROFTOUEMQUKAOPBKLMLXCS
IZSHLTFBOZSHBKLVHPSHKUHKLUSHIPFQPZMPFGTDDMKGQWMEGIWQTCBKXDB

```
LSAFTLUMDILKBZDLALEILKMSKBFLCUGMEGIGDMWFZWCOPBKBLFTAZKBVNLG
FQGRBLCZPUDIDWSAXDBLSAUMQVECBLKBMQLMCKFZWCZSLMHTASZXGKACUGQ
BWUZDLRCZEMXDIVDGFQFTOUFBUVLRIZLGVLUGBLKHUXCHIGFQVCZSAHOULR
LHBKLAZSWUFTHOMIFBOWRNTRBMUQXYZDLRHZXDKFCHMBKSOPBLKBVCMEHMS
UGIHCBUMUSHEAEMUVSHBQSHLELCKRTKZFILKBZHGAGREHCTRLCNDADMBLHZ
ZSCZFBUTAEPUABSHDMPCGRIYHDEMMEUGMEGIDMPCGRIYHDEMMHPWPCGRIYH
DEMMPBUSHVCIVDVDSGRBLHPMLUGHPBLAEKLBKMBQCLMMASHHDEMMEBQZCBK
OWGSBCFBQCLMDLKBABSHECPKHZALNUBLWCTRRVBLFZWCFQONKZFBHPECPKK
BNZECTKPHUNWUBLFBBLCZDKFAOUPOFTRUBABKLCDCBPACUGVCPZMPXUABED
CHMPRUBATIZXBKUASHLULEBMSHFRCZUQUVLERVUMOWLAKGBPBMSHUWTDGUM
UDQUMBLCZCHIGFQLALMHTRUZSHSCLUQSKCKACUGOTMBDQUMZHABSHWQRBQY
BCFBFTOUSHBQSHZCBUGRZSAFBFZOUQXYZDLRACUGZSHZUMWOMBGDDVLRIBF
LACUGEAKTFTODWCDIUQBMRLNTRUPKQUMHPXSKBPLELCITACGWEHFBORURQP
BUSHKGBKFTLUSHZXKBHEUPNDLBGRXDBLUMFQMEUGZHUTAEPUHSKBBLFBZSC
ZEMCQUKCHUMORUMBUSHBKILMUZSSCMEUGLCUFCBBUGDZSCHUPXRSKIWOWYU
HCCLNZINLPPLCKSUFTOUGDSHMV
```

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

Setelah menemukan kuncinya, gunakan program *Playfair cipher* yang anda buat pada Bagian A untuk mendekripsi cipherteks tersebut.

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

Pada bulan Desember, wartawan Tintin dan teman yaitu Profesor Calculus pergi jalan-jalan ke Jakarta, Indonesia. Di Kemayoran Tintin menulis surat kepada Kapten Haddock, menceritakan sebuah berita tentang negara Selandia Baru. Surat Tintin kepada Kapten Haddock selalalu dimulai dengan kata 'Hello Captain Haddock' dan diakhir dengan "Tintin". Bantulah Kapten Haddock untuk memecahkan ciphertext tersebut dengan *known-plaintext attack*. Surat tersebut dienkripsi dengan Hill cipher, 3 karakter setiap kali enkripsi.
Cipherteks di bawah ini denkripsi dengan program online: https://www.dcode.fr/hill-cipher


```
TFJOXUPOUXYTTRDSXQMONIYPEUFJDQUBGIMOCJQTNBEHCZEKROVBNTWLMVX
MOWZLUCHOXYGSKBQGUAOBQZKIXYJIETSWVXHVKCUAOTOFYIZAKJGXKAWGQT
RVFDZAJNQDUIWZCMYWNFIUPYMCZXIAKYUCQIAZPIQMGAMGUAKKKHMWKDUXQ
DUAAKYOWEHLJPWYFKXSARBLLHGAJKTQNTRTPWSCIZASCGSLKVDHTUZSWBNB
TJGYYUPQMFSYZAUTOQCDNGQMFSRLRTUWEMKADIVYLTJKFHLKJUWTSSHMHJF
GTRIBYIDAHQEPMPIQCROWDYRYZNSPNOJHQVKKTOCBPNFAJNLYJZNVBAYJWR
GMCHJPWBDHHTPOXSIJVQWDMSIGMTRVEVXDILKVAYTNUNJXEZLAPGYETRVZN
VHSVWLGICDXQFOALDVPASUSYXPFHUWTILUQHTJQVGWFSPAEKBRBNIINYKHN
TNUKJVDHVLXQKUZNVQXUOZZOJZYNPIVYSVFVTZMMUUPWTGHRIOWCBKZYAGU
MRCKHIQZSIGISPGBXPYXMOAWGAGHQVUWTEIGPBMOMBWIOPQEVKMRQATNBMI
LHHLVUXGMOUWTZCLBKGWIJHFRNGOSCMUHDWHBB
```

Setelah ditemukan kuncinya, dekripsilah cipherteks dengan program Hill Cipher yang telah anda buat.

PENGUMPULAN TUGAS

Laporan tugas dikumpulkan paling lambat Jumat 3 Februari 2023 pukul 23.59 WIB. Tugas sebaiknya dibuat berpasangan (2 orang), namun diperkenankan per orang. Laporan yang dikumpulkan adalah file format PDF yang berisi:

BAGIAN A

1. *Source program* Javascrpt/Python/Ruby/Golang/PHP, dll
2. Tampilan antarmuka program (*print screen*).
3. Contoh plainteks dan cipherteks (text, gambar, file database, audio, video)
4. Link ke *github* atau *google drive* yang berisi kode program

BAGIAN B

1. Berkas cipherteks
2. Langkah-langkah yang anda lakukan dalam melakukan dekripsi

3. Plainteks hasil dekripsi

File PDF diunggah ke alamat berikut:
https://drive.google.com/drive/folders/1a2qJx4XMWX_zwkGvpNL9_peQ6zQ0RW_9?usp=share_link

Jika program/kriptanalisis tidak selesai/tidak bisa run/masih ada yang salah, maka tuliskan di dalam laporan. Tugas akan diperiksa dan dinilaioleh tim asisten (Michael Hans IF2018/S2 IF 2022 dan Hokki Suwanda IF 2019)

Program harus dibuat sendiri, DILARANG KERAS mengambil kode program dari tempat lain atau dari orang lain.

Lengkapi tabel berikut di dalam laporan dengan mencentang kolom):

BAGIAN A

No	Spek	Berhasil (√)	Kurang berhasil (√)	Keterangan
1	Vigenere standard			
2	Auto-Key Vigenere Cipher			
3	Extended Vigenere Cipher			
4	Affine Cipher			
5	Playfair cipher			
6	Hill Cipher			
7	Bonus: Enigma cipher			

Keterangan:
1) Berhasil artinya program sesuai spek, benar, bisa melakukan enkripsi dan dekripsi dengan benar (baik pesan diketik maupun file)
2) Kurang berhasil artinya i) program tidak selesai, atau ii) program masih ada kesalahan, atau iii) program hanya bisa melakukan enkripsi tetapi dekripsi salah, atau iv) hanya bisa enkripsi file text tidak bisa file sembarang, atau v) hanya bisa enkripsi pesan diketik langsung tidak bisa untuk file, vi) dll. Tuliskan pada bagian keterangan aspek apa yang kurang berhasil

Nilai bagian A: 70 + bonus 10

BAGIAN B

No	Kriptanalisis	Berhasil (√)	Kurang berhasil (√)	Keterangan
1	Kriptanalisis Cipher Abjad-			

	Tunggal			
2	Metode Kasiski			
3	Kriptanalisis Playfair Cipher			
4	Kriptanalisis Hill Cipher			

Nilai Bagian B: 40

Total nilai: 70 + 40 = 110 atau 120 (tambah bonus 10)