

Tugas 2 Kriptografi dan Keamanan Informasi

1. Kriptanalisis Caesar Cipher

Diberikan cipherteks dengan Caesar Cipher sebagai berikut (cipherteks dikelompokkan dalam blok-blok 5 huruf):

MXXFT QQHUX WMDYM QHQDO DQMFQ PNKYQ EUZOQ ARAXP AZMOO AGZFA
RYKNQ SUZZU ZSXQE ESDQQ PTMFD QPMZP USZAD MZOQN ADZAR YKOAZ
PGOFE BQQOT MZPFT AGSTF UZAIQ AZRQE EABQZ XKMZP RGXXX

Kriptanalisislah cipherteks tersebut untuk memperoleh pliantekstanya. Berapa nilai pergeseran hurufnya?

2. Kriptanalisis sembarang monoalphabetic cipher

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 kriptanalisis 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 mengenkripsi karakter abjad (a..z). Karakter lain (spasi, koma, titik, dan lain-lain) dibuang (tidak dienkripsi).

Anda sebagai penerima dokumen harus mampu mendekripsi chiperteks tersebut menjadi plaintekst semula meskipun anda tidak mengetahui kuncinya. Anda menggunakan kombinasi teknik analisis frekuensi dan metode terkaan untuk mendekripsi dokumen tersebut. Anda diperbolehkan menggunakan 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.

CZWKWFKWUFKXHLZCZWXKNWFLCXQZWKWCZWCWKEUNSNJPXKNPNJFCWYXJWVXXSLC
XCZWBWENJNJWGKWBNIUNSEWFJNJPNJVWCXKOFRQZNVWXCZWKLVFNECZWNLCXKN
AJXKQWPNFJLWCCVWEWJCBUNSWJNLQZWKWCZWFJEWYWKNUWLZJAWUNSNJPLQWKW
CZWXKNPNJFVYQWVWKLXBUNSWJFVCWKJFCNUWVRKWAXPJNLWYWCREXVXPNLCLLHA
ZFLFJFCXVRVNOWKEFJGXNJCCXCZWXVYJXKLWQXKYUNSEWFJNJPLWFENVWCZWLGF
AWVWBCOWCQWWJCQXKXQNJPOXFCLNJAXJUXRQZNVWXCZWKWKWBKWCXCZWCZAWJCHK
RFJVPVXLFIXJGXWEQNYLNCZQZNAZKWBWKLCLAFJYNJFUNFJGNKFCWLFLQANANJPLK
WPFKYVWLLPNUWJJCZWLAFJYNJFUNFJLYXENJFJAWXBCZWLWYHKNJPCZNLWFKVGRW
KNXYNCQFLJCVXJPHJCNVAXJCKFLCNJPJFEWLQWKWOWNJPXBBWKWYHGORUFKXHLX
CZWKAHVCHKWLFAXLLCZWGVFJWCCZWFKFOLLVFULFJYORDFJCNJWLXBKXWIFEGVWS
JWQXBCZWLWKFNYWKLFLKHLXKKZXLKWFVFCNJPXCXKXQNJQPZNVWCZWPWKEFJLVFOWV
VWYCZWEFLFLAXEFJNLFLEWJFVHYNJPCXCZWNKFLZQXXYOXFCLXCZWKJFCNXJLL
HAZFLCZWWJPVNLZFJYAWVCLLWCCVWYEWKVRXJYFJWLZWFCZWLXKGFJLQZNVL
CCZWNKNLZKWBWKKWYCXZWEFLYHOPFNVFJYBNJJPFNVFYKSFJYBFNBKXKWNPJWKL
XKTHNCWLHNCFOVRJXKCZEWJPNWJJCZWAXEEXJAHVCHKFVGGKFCNAWXBCXKEWJCNJ

PAXFLCFVLWCCVWEWJCLFJYEXJFLCWKNWLNLCQFLJCVXJPHJCNVCZWUNSNJPLBWFKL
XEWKWHGCFCNXJLGKWFYCXFVEXLFCVAVAXKJWKLXBWHKXGWFJYEWLXGXCFENFCZWKW
NLWUWJWUNYWJAWCZFCZCWUNSNJPLKWFVAZWYOFZFYFCZAWAJCKWXBCZWNLVFENAW
EGNKWFCCZWCNEWCZWUNSNJPPWF LAXEEXJVRKWBWKKWYCXVFLCWYBKXECZWWFKVR
LCXCZWJXKEFJAXJTHWLCXBWJPVFJYNJCZKXHPZXHCCZNLGWKNXYCZWUNSNJPLHLW
YCZWJXKCZWKJFYOFVCNALWFLCXWKKXKNLWJWNPZOXHKNJPSNJJPYXELWICWJYNJ
PCZWNKNJBVHWJAWCZKXHPZAXEFCFJYAHVCHKWHJCNVWUWJCHFVVRUNSNJPLAXHV
YJXVXJPKWOWEKKWVRYWLAKNOWYFLAXFLCFVKFNWKLAXJLNYWKCZWBFAFLCQXUNS
NJPSNJPLLQWRJBXKSOWFKYFJYAJHCCZWPWFQXHVYFLAWJYCZWWJPNLZCZKXJW
VWNBWKNLXJFJWFKVRNAWVFJYWKQXHVYLWCCVWLZXXCNUWYAXVXJNWLNJXKXCFE
WKNFLAFJYNJFUNFJLQXHVYUWJLWUWFLWKAJFKNWLXKXZWORDFJCNJWWEKN
KWNJLZXXKCCZWLWQWKWJXEWKGNKFCWLOHCCZWBXKWBFCZWKLXBFQCAZQXKSTHN
CAHVCHKWCZWEFCNUFCNXJLBXKLHAZWIGFJLNJFKWLHOMWACCXYWOFWCBXKEXYWK
JZNLXKXNFJLXCZHPZCZWKWFKWAVWFKNJAWJCNULWFLCXQZRCZWXGHVFCNXJXBLA
FJYNJFUNFENPZCFUWFACWYNJCZWFQFRCZFCZWRYNHYHKNJPCZNLRFKGNKXJYJ
WKWVFCNUWVRFGGFKWJCKWFLXJNLF LAFKANCRXBKWLXHKAWLCZHLBXXANJPCZWUN
NJPLCXVXXSBHKCZWKFBWVYUWJXKXOONJPFJYSNVVNJPAVFLWLBXGWXGVWVWLL
WYQNCZFEKWOXHJCNBHVZXEWVFJYFJXCZWKGXLLNOVWLCNEHVHLNLCZWKHVWXBZ
FKVWEFPJWFJYCZWKWVNPXHLGWKLWAHCNXXJCZFCQWJCZJYJNZFJYQNCZNCQNCZA
ZKNLCNFJNJBVHWJAWLWGNJPWUWKBHKCZWKJCYWJEFKSLQWYWFJYJXKQFRNCE
FSWLXVPAFVLWJLWCZFCZCWUNSNJPLQWKVXXSNJPCXGKXCWACCZWNKGFJOWVN
WBLRLCWEKWLNLCMHYWAXZKNLCNFJUFVHWLWJYUWJCFSWKWUWJPWBXKXZLWLWCC
VWEWJCLFVKWFYRVXLCCXFEJXCZWNLCNAYWUXCNXXJCZNLNLJXCLGWAHVFCNXJCZ
NJCKXYHACNXXJBAZKNLCNFJNCRQXHVYAXEWXUNUNYWJXKQFRBXXFVEXLCZVBFBA
WJCHKRAFHLNJPHJCVYOVXXYLZWYFJYAHVCHKFVCKFJLBXKEFCNXJNCLZXHVYFVL
XOWJXCWYCZFCYHKNJPCZWUNSNJPPWLAJYJNFUNFLAVXLWLCJWNPZOXHKLQWKWW
IGWKNWJANJPUFKRNJPVWUWVLXBNJJKCHKEXNVCZHLPKFJCNJPCZWUNSNJPLFJFY
UFJCFPWQZJWIGVXNCNJP CZWLWVFJYLBXKQWFVCLVFWLXKCKKNCXKRCZWLWFK
XHCWLHLWYORCZWUNSNJPLQWKWVEXLCWJCNKWVRBKWXXBXGGXLNLCNXJVWFUNJPCZ
WKFNYWKLHJNEGWYWFYFLCZWRCKFUWVWVYBKXEXJWYWLCNJCFCNXJXBGVHJYWKXCXZ
JWICCNLQKWF SYXQJNJCZFCZFYXJAWOWWJFGKXBNCFOWJWCQXKSXBCFYKXHCW
LBXKWHKXGWFJSNJPYXELAFJOWZWKVYVYOFASF LBFKFLCZWAXVVFGLWXBCZWKXEF
JWEGNKWNJCZWCZAWJCHKRFJYVFCWKXCXZWKFGNYCZAWJCHKRWIGFJLNXXJBNLVFE
NAGZNVXLXGZRCZWWJYXBCZWUNSNJPPWAFJOWGNJWYXQJCFJHEOWKXBBFACXK
LBNKLCXBFVVCZWBVFXHCCZFCXAAHKKWYBXVXQNJPCZWAZKNLCNFJNLFCNXJXBL
AFJYNJFUNFQXHVYZFUWHJCVYWBWACLXJCZWKWPNXJLYXEWLNAFJYBXKWNJGX
VNARORCZWCZAWJCHKRYWJEFKSJXKQFRFJYLQWYWJQWKWBBWACNUWVRAXJCKXVV
YORYNXAWLWLVWPCNENLWYORCZWAFCZVNAAZHKAZFJYZFYBNKEVRWLCFOVNLZWY
CZWEWLVUWLFLLWGFKFCWSNJPYXELCZNLWFJCFJWJXKEXHLAHVCHKFVLZNBCNJCZ
WGKNXKNCNWLXBLAFJYNJFUNFLVWFYWKLZNGNJCZFCFLWJLWCZUNSNJPLQWKWJXCY
WBWFCWYOHCFKPHFOVREFYWCXOWZFUWVJFEFJWKCZFCBNCCZWANUNVNCRXBCZWNK
THNASVRCKFJLBXKENJPZXEWFJYLBXKWI FEGVWCZWEWYNWUFAZHKAZEFYWNCBXX
ONYWJXCXCFSWBVVXQAZKNLCNFJLFLVFWLWPNWJPCZWBFAACCZFCVFWWCKFYJNP
QFLCZWJHEOWKXJWLXHKAWXBGKXBNCBXKCZUNSNJPLCZNLKWEXUWYFPKWFCYWFVX
BCZWWAXJXENANJAWJCNWUCXCKFUWVFJYKFNXUWKLWFLCZWJWQVWFYWKLZNGFVLX
AZXLWCXKBXAHLCZWNKENVNCFKRFCCWJCNXJBKXECZWSNJPYXELXBCZWQWLCFJYN
JLCWFYGFKCFSWNJLHAZAFEGFNPJLFLCZWOFVCNAQFKLFJYCZWFCCWEGCWYAXJTHW

LCXBMWKHLFVWEBKXEZWKWXJXHCNCLWWEWYCZWUNSNJPLQWKWJXVXJPWKFKWAXPJN
LWYBXXKAWNJCZWQXKVYCZXHPZCZWNKOKHCFVNCROKFUWKRFJYLCKWJPCZQXHVYVXJ
POWKWEWEOWKXYORCZXLWQZXZFYXJAWBWCCZWLZFKGWYPWXBCZWNKOFCCVWF IW

Alamat pengumpulan: https://docs.google.com/forms/d/e/1FAIpQLSdbQVcY-Fao2gvnJB5k6e5Pr2YlcnqLvD1XLsnvH9aKoa-bA/viewform?usp=sf_link