Atividade 1 – Decifrar o texto cifrado sem conhecer a chave

Com a ajuda de ferramentas de análise de frequência caracteres e a tabela de frequência de caracteres na língua inglesa faça a cripoanálise do texto cifrado abaixo. Para um resultado mais preciso analise a frequência de pelo menos digramas (dois caracteres) e trigramas (três caracteres) também.

Uma ferramenta de análise de frequência útil pode ser encontrada em http://www.richkni.co.uk/php/crypta/freq.php.

Tabelas de frequência de caracteres na lingua inglesa podem ser facilmente encontradas na internet.

tipgkfxirgyp zj kyv girtkztv reu jklup fw kvtyezhlvj wfi jvtliv tfddleztrkzfe ze kyv givjvetv fw kyziu grikzvj (trccvu rumvijrizvj). dfiv xvevirccp, zk zj rsflk tfejkiltkzex reu rercpqzex gifkftfcj kyrk fmvitfdv kyv zewclvetv fw rumvijrizvj reu nyzty riv ivcrkvu kf mrizflj rjgvtkj ze zewfidrkzfe jvtlizkp jlty rj urkr tfewzuvekzrczkp, urkr zekvxizkp, rlkyvekztrkzfe, reu efe-ivgluzrkzfe. dfuvie tipgkfxirgyp zekvijvtkj kyv uzjtzgczevj fw drkyvdrkztj, tfdglkvi jtzvetv, reu vcvtkiztrc vexzevvizex. rggcztrkzfej fw tipgkfxirgyp zetcluv rkd triuj, tfdglkvi grjjnfiuj, reu vcvtkifezt tfddvitv.

tipgkfxirgyp gizfi kf kyv dfuvie rxv nrj vwwvtkzmvcp jpefepdflj nzky vetipgkzfe, kyv tfemvijzfe fw zewfidrkzfe wifd r ivrurscv jkrkv kf rggrivek efejvejv. kyv fizxzerkfi fw re vetipgkvu dvjjrxv jyrivu kyv uvtfuzex kvtyezhlv evvuvu kf ivtfmvi kyv fizxzerc zewfidrkzfe fecp nzky zekveuvu ivtzgzvekj, kyvivsp givtcluzex lenrekvu gvijfej kf uf kyv jrdv. jzetv nficu nri z reu kyv rumvek fw kyv tfdglkvi, kyv dvkyfuj ljvu kf triip flk tipgkfcfxp yrmv svtfdv zetivrjzexcp tfdgcvo reu zkj rggcztrkzfe dfiv nzuvjgivru.

dfuvie tipgkfxirgyp zj yvrmzcp srjvu fe drkyvdrkztrc kyvfip reu tfdglkvi jtzvetv girtkztv; tipgkfxirgyzt rcxfizkydj riv uvjzxevu rifleu tfdglkrkzferc yriuevjj rjjldgkzfej, drbzex jlty rcxfizkydj yriu kf sivrb ze girtkztv sp rep rumvijrip. zk zj kyvfivkztrccp gfjjzscv kf sivrb jlty r jpjkvd slk zk zj zewvrjzscv kf uf jf sp rep befne girtkztrc dvrej. kyvjv jtyvdvj riv kyvivwfiv kvidvu tfdglkrkzferccp jvtliv; kyvfivkztrc rumretvj, v.x., zdgifmvdvekj ze zekvxvi wrtkfizqrkzfe rcxfizkydj, reu wrjkvi tfdglkzex kvtyefcfxp ivhlziv kyvjv jfclkzfej kf sv tfekzelrccp rurgkvu. kyviv vozjk zewfidrkzfe-kyvfivkztrccp jvtliv jtyvdvj kyrk gifmrscp treefk sv sifbve vmve nzky leczdzkvu tfdglkzex gfnviΩre vordgcv zj kyv fev-kzdv gruΩslk kyvjv jtyvdvj riv dfiv uzwwztlck kf zdgcvdvek kyre kyv svjk kyvfivkztrccp sivrbrscv slk tfdglkrkzferccp jvtliv dvtyrezjdj.

tipgkfcfxp-ivcrkvu kvtyefcfxp yrj irzjvu r eldsvi fw cvxrc zjjlvj. ze kyv lezkvu bzexufd, ruuzkzfej kf kyv ivxlcrkzfe fw zemvjkzxrkfip gfnvij rtk 2000 ivhlziv r jljgvtkvu tizdzerc kf yreu fmvi yzj fi yvi uvtipgkzfe bvp zw rjbvu sp crn vewfitvdvek. fkyvinzjv kyv ljvi nzcc wrtv r tizdzerc tyrixv. kyv vcvtkifezt wifekzvi wfleurkzfe (vww) nrj zemfcmvu ze r trjv ze kyv lezkvu jkrkvj nyzty hlvjkzfevu nyvkyvi ivhlzizex jljgvtkvu tizdzercj kf gifmzuv kyvzi uvtipgkzfe bvpj kf crn vewfitvdvek zj letfejkzklkzferc. kyv vww rixlvu kyrk kyzj zj r mzfcrkzfe fw kyv izxyk fw efk svzex wfitvu kf zetizdzerkv fevjvcw, rj xzmve ze kyv wzwky rdveudvek.