

Materiály k cvičení 1

Příklad 1

PDBSB RAFB KQMBU Y LRRS PYQKRS, HDR DYU Y XRA FYKKBU YKYUUQA, Y FYSBKBXX, QUKB WRN HDR HRIKU UR ARPDQAG WIP LKYN YKK UYN KRAG QA PDB XPSBBPX HQPD KQPPKB QUKB WRNX KQTB DQZXBKE. PDQX XR GSBMBU PDB EYPDBS PDYP DB UQBU; NBP, QA XLQPB RE DQX ZRPDBSX PBYSX YAU LSYNBSX, YKYUUQA UQU ARP ZBAU DQX HYNX. RAB UYN, HDBA DB HYX LKYNQAG QA PDB XPSBBPX YX IXIYK, Y XPSYAGBS YXTBU DQZ DQX YGB, YAU QE DBHBSB ARP PDB XRA RE ZIXPYLDY PDB PYQKRS. Q YZ, XQS, SBLKQBU YKYUUQA; WIP DBUQBU Y KRAG HDQKB YGR. RA PDQX PDB XPSYAGBS, HDR HYX Y EYZRIX YESQFYA ZYGQFYA, EBKK RA DQX ABFT YAU TQXXBU DQZ, XYNQAG: Q YZ NRIS IAFKB, YAU TABH NRI ESRZ NRIS KQTBABXX PR ZN WSRPDBS. GR PR NRIS ZRPDBS YAU PBKKDBS Q YZ FRZQAG. YKYUUQA SYA DRZB, YAU PRKU DQX ZRPDBS RE DQX ABHKN ERIAU IAFKB. QAUBBU, FDQKU, XDB XYQU, NRIS EYPDBS DYU Y WSRPDBS, WIP Q YKHYNX PDRIGDP DB HYX UBYU. DRHBMBS, XDB LSBLYSBU XILLBS, YAU WYUB YKYUUQA XBBT DQX IAFKB, HDR FYZB KYUBA HQPD HQAB YAU ESIQP. DB LSBXBAPKN EBKK URHA YAU TQXXBU PDB LKYFB HDBSB ZIXPYLDY IXBU PR XQP, WQUUQAG YKYUUQAX ZRPDBS ARP PR WB XISLSQXBU YP ARP DYMQAG XBBA DQZ WBERSB, YX DB DYU WBBA ERSN NBYSXRIP RE PDB FRIAPSN. DB PDBA PISABU PR YKYUUQA, YAU YXTBU DQZ DQX PSYUB, YP HDQFD PDB WRN DIAG DQX DBYU, HDQKB DQX ZRPDBS WISXP QAPR PBYSX. RA KBYSAQAG PDYP YKYUUQA HYX QUKB YAU HRIKU KBYSA AR PSYUB, DB REEBSBU PR PYTB Y XDRL ERS DQZ YAU XPRFT QP HQPD ZBSFDYAUQXB. ABCP UYN DB WRIGDP YKYUUQA YEQAB XIQP RE FKRPDBX, YAU PRRT DQZ YKK RMBS PDB FQPN, XDRHQAG DQZ PDB XQGDPX, YAU WSRIGDP DQZ DRZB YP AQGDPEYKK PR DQX ZRPDBS, HDR HYX RMBSJRNBU PR XBB DBS XRA XR EQAB.

Příklad 2 (ze slidů k cvičení)

YAQZOSXYGJEXMJXNHMEIESIKIZEIZUASYHDXYGMEIESXLISJESHMAYMAYJEHJEAOMIYZIYZWXSJMYYX GEJQEHEymeHEIZHYZHZEJHJIBHAWNIISOWMEHSAMHIYDXMMHZEJHGSAYUHWASHEXNMILXYGG SHIJDXYGWASIJEAOMIYZIYZAYHYXGEJMXEIFUHHYSHPAOYJXYGJALAOJEHWIUBHMAWRIMJIGHMIYZ JEHBHGHYZMAWIYPXHYJDXYGMNIXNIDHMAUABZIMJAPSIFHIWIFASAWLAOSNITHMJL

Příklad 3

QEJACKUJTTKCYTJLGUJSXKXJIQTKRJCQEWTTJWCWJTKUHEGCGHQJCTQEJICGWTWIVEWTTAJHQGHZJT EJACKIKYIHJLQEJTJGCJCYIWHZJQQJCTQEJBGCIJPGHQZBZWNJQEKTKUQEJXGIYTHCWAQKUTIKCCJQY CZZJTKIDYQSEGQKIJGCQEWTEJWCXJGIWIVCYIWHZJQQJCTGAAJGCWIVQKXBXWILQKDJGIVIRJIQWK IKUQEJZJGCIJLQKXBTQWUBQEWTAKKCSKZLWSGTIKQTKCCBQKTJXBYIHZJTYUUCWIVQEJAGIVTKUX BTQWUWHGQWKIGQZJGTQTKWQTJXJLQKXJMYLVWIVUCKXEWUWIVJCTSEWHESJCDJVVIIWIVQKS KCNSWQEJCCWDZJJIJCVBWQWTHJCQGWIZBKZLWHJZGILWHEJXYQQJCLDJQSJIIEWTQJQEGILACKU JTCKZWLJLIDCKHNXYTQEGRNISUKCEJSGTGHNIKSZJLVJLQKDJOWQJGAKZBVZKQIKQEGQJEJHKYZ LTAJGNUZYJIQZBWIQEJQSKQEKYTGILZGIVYGVJTGILQSZJRJQEKYTGILLWGZJHQJSEWHEGCJTAKNJIQI EJJGCQEDYQEJNIIJSGQZJGTQEWTEGCIKUQEJX

Užitečné weby

Frekvenční analyzátory

<http://www.mcl.d.co.uk/decipher/>

<http://practicalcryptography.com/cryptanalysis/text-characterisation/monogram-bigram-and-trigram-frequency-counts/>

<https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html>

http://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html

<http://jnicholl.org/Cryptanalysis/Tools/FrequencyAnalysis1.php>

Frekvenční tabulky pro angličtinu

<http://www.mcl.d.co.uk/decipher/longenglish.htm>

<http://www.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html>

<http://www3.nd.edu/~busiforc/handouts/cryptography/Letter%20Frequencies.html>

<http://www.richkni.co.uk/php/crypta/freq.php>

Nástroje pro úpravu textu

<http://skola-kly.cz/odstraneni-diakritiky-z-textu-online/>

<http://www.gorewrite.com/modify.html>

<http://www.miniwebtool.com/remove-spaces/>