Uživatelská příručka

Prolomení polyalfabetické šifry

V Brně 29. května Vojtěch Matulík

Skript napsaný v jazyce Python s názvem *projekt.py*, který lze nalézt v příloze, slouží k zašifrování anglicky psaného textu pomocí polyalfabetické šifry (konkrétně vigenerovy šifry) a dále i k odšifrování anglicky psaného textu zašifrovaného vigenerovou šifrou bez znalosti klíče.

Ke spuštění skriptu je potřeba nainstalovat si všechny knihovny, které skript používá. Skript byl naprogramován za použití interpreteru verze 3.11.9 64-bit (Microsoft Store). Je potřeba mít všechny přílohy .zip souboru (soubor, který byl vložen do odevzdávárny) ve stejné složce po rozbalení .zip souboru a spuštění skriptu.

Po spuštění se v terminálu skript zeptá na 3 anebo 4 otázky. První otázkou je „Encrypt or decrypt:“. Zde se skript ptá, zda-li chceme text šifrovat či dešifrovat. Odpovídáme pouze vstupem „encrypt“ či „decrypt“.

Dále se skript ptá, zda chceme text načíst ze souboru *vigenere.txt* v případě, že zvolíme volbu „encrypt“*.* (V souboru *vigenere.txt* se po stažení .zip souboru z odevzdávárny nachází text z knihy „The Old Man and The Sea“ od Ernsta Hamingwaye o velikosti 132 kB.) V případě, že zvolíme volbu „decrypt“ se skript ptá, zda chceme text načíst ze souboru *vigenere\_encrypted.txt*. (V souboru *vigenere.txt* se po stažení .zip souboru z odevzdávárny nachází zašifrovaný text z knihy „The Old Man and The Sea“ od Ernsta Hamingwaye o velikosti 132 kB.)

Odpovídáme v terminálu vstupem „yes“ či „no“.

**V případě volby možnosti „ecrypt“:**

Odpovíme-li „yes“, následuje výzva k zadání klíče „Enter the key“. Klíč musí být delší než 1 znak a musí obsahovat pouze znaky anglické abecedy. Nakonec se objeví zpráva, že zašifrovaný text byl uložen do *vigenere\_result.txt*.

Odpovíme-li „no“, vložíme text do terminálu ručně. Vkládat ručně se však nedoporučuje, protože po několika pozorování bylo zjištěno, že délka vkládaného textu by měla být alespoň 10 kB. Dále následuje výzva k zadání klíče, pro který platí stejná pravidla uvedená v odstavci výše. Nakonec se zašifrovaný text vypíše do terminálu. Tento text je možné zkopírovat pro následnou dešifraci.

**V případě volby možnosti „decrypt“:**

Odpovíme-li „yes“, skript vypíše délku klíče, kterým šifra byla zašifrována, následně klíč samotný a informaci o tom, že rozšifrovaný text byl uložen do souboru *vigenere\_decrypted.txt*.

Odpovíme-li „no“, skript po nás bude chtít vložit zašifrovaný text do terminálu a dále vypíše délku klíče, kterým šifra byla zašifrována, následně klíč samotný a nakonec rozšifrovaný text.

**Shrnutí:**

* Vkládejte text k šifrování dostatečně dlouhý (10 kB a více) … Krátký text může při dešifraci buďto vyhodit chybovou hlášku či skript nesprávně odhalí klíč
* Vkládejte text k šifrování pouze anglicky psaný (či česky a bez interpunkce)
* Vkládejte klíč dostatečně dlouhý (2 a více) … Pro některé klíče se může stát, že při dešifraci se odhalí špatná délka klíče (například pro klíč *heslojakokreslo*)
* Vkládejte klíč sestavený pouze ze znaků anglické abecedy (či česky a bez interpunkce)
* Preferuje se používat *vigenere.txt* soubor k vkládání šifrovacího textu před vkládáním terminálem
* Skript nezaručuje správné rozšifrování každého textu s jakýmkoliv klíčem (vizte body výše)
* Při zadávání do terminálu se vyvarujte překlepům, skript přijme pouze správně zadaný vstup