

Prolamování substitučních šifer

Z předchozí kapitoly už víte, co to jsou substituční šifry. Pro zopakování to jsou šifry, kde se jedno písmeno nahrazuje druhým. Toto přeházení písmen se dá definovat dvojí abecedou:

- Abeceda původního textu: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Abeceda zašifrovaného textu: ZYXWVUTSRQPONMLKJIHGFEDCBA

Z čehož je jasné definované, které písmeno je kterým nahrazeno.

Takže četnost písmen je stále stejná v plaintextu i ciphertextu, ale v ciphertextu jsou reprezentovány jinými písmeny. Právě toho se využívá při frekvenční analýze textu.

V principu se díváte na to, kolik procent nebo úkazů je standardní pro daný jazyk a kolik procent/úkazů je v daném zašifrovaném textu. Toto však funguje pouze u delších textů. U krátkých textů, je až moc malý objem dat na spolehlivou frekvenční analýzu.

Dneska si vyzkoušíte, jak obtížné je prolomit substituční šifru pomocí frekvenční analýzy. Jedná se o jednu z nejzákladnějších metod prolamování v kryptografii.

Zadání

Na <https://gist.github.com/mikison9/d5923764273dff078467fd392aac020c> je uložen soubor se šifrovaným textem, pokuste se ho dešifrovat.

Online nástroj pro frekvenční analýzu

Tipy:

- Text je v angličtině
- Text začíná slovem "the"
- Podívejte se na šifrovaný text, neopakují se v něm určité řetězce znaků?
- Písmena, která musíme prohodit, bývají často u sebe
- Tipování anglických slov: <https://www.crosswordsolver.org/>

Task 01

Kterým slovem končí báseň?

Vlajku zapište ve formátu `haxagon{poslednislavo}`.