## Bonusový úkol A

Vaším úkolem je provést kryptoanalýzu a dešifrovat text ze souboru: **`monoalphabetic_cipher_2023.txt`**

Zdrojový text je v angličtině a obsahuje 6075 slov. Víte, že byla pro šifrování použita monoalfabetická substituce. Je nemyslitelné procházet všech *26!* možných řešení metodou hrubé síly. Použijte proto frekvenční analýzu (vezměte v úvahu jednotlivé znaky nebo dvojice/trojice znaků – tzv. bigramy a trigramy, obecně n-gramy).

Zaměřte se rovněž i na slova, protože úlohu máte zjednodušenou tak, že mezery byly ze šifrování vyjmuty (tzn. mezera je na stejném místě v šifrovaném i původním textu). Text obsahuje pouze znaky malé abecedy, tzn. žádná interpunkční znaménka (tečky, čárky) ani čísla. Abeceda, se kterou se pracuje, je pouze **[a-z] + mezera.** Znaky konce řádků byly nahrazeny rovněž mezerou.

Váš program musí automaticky rozhodnout o tom, že byla šifra prolomena, tzn. výsledný text je smysluplný. Použijte např. anglický slovník a testujte kolik korektních slov jste odhalili. Čím budete blíže ke správnému řešení, tím bude růst počet smysluplných slov, až se postupně dostanete na maximum.

Vytvořte také soubor `readme.txt`, ve kterém popíšete svoje řešení.

Váš program společně se souborem `readme.txt` a všemi soubory z archivu se zadáním zabalte do ZIP souboru a pojmenujte ho podle svého osobního čísla.

**Nápověda**: Frekvenční analýza, genetické a evoluční algoritmy

Za úspěšné vyřešení obdržíte 6 bodů.

## Bonusový úkol B

Mějme následujících 11 krátkých zpráv v češtině zašifrovaných pomocí **`Vernamovy šifry`**.

**de6315a7c29a4b922ba26eb44439669e76864e639eea96175aea71d5b312ce8be4404984f0b028c7d501e4e37a724e4a7f5321**

**d36716f5ca914b912eec6af6567862822fc4477d94a193184bf56cd5**

**db621caf8780198e2af06ebc586d77d138814d6e81a5881c55e4679cfd039c9afb405688bbb223**

**da6301bbc29a4b9523e92fb75f6061d1349d5b2f82be840a4ffe7b9cfd079c8fec191a9eb5a26acdd240f5ee782b4f0f6545267fe458b45e**

**c56200b9c6844b9727e12fbd497c60947697522f93a58f1056f522d6f642cc9cf80e53cdbba325d5864aa6ef6522474c6755**

**da6345b9c280188862f060ac4e6f7b853f90176d88bec5135efe22d1f20ed39bae134c84b3ba3f9ec844fcba66204d446349263eea1ca15fba**

**de6345a3d49908892ceb2fbd497c609876865b6084ae8c5951e36dc9b318c89cef035f83b9**

**ca6745bec68a0f8e37a264a45c6a7c9e23c4416a92a3c5135eb06cd9f903d797ae044898b8f128d1ca44f5ee7f**

**de6716b9c2941e8b62f179b31d6a7c88768517759caf8b5948e677d6b318d598e114**

**da6316a1cb994b8f23e86bb34e3964d12c8d416085afc51a5ee376c9b300d994ae104888bbb030dbcd01f3e8753b564a2f4e2134ff51f55caa8bc69085**

**db621caf879e0e972bf12fbd5c7432813a915d6a82ea9f185ffe7b9ce50bc89cae0e5f83b9f13accf5be8f3602b**

Víte, že všechny zprávy byly zašifrovány stejným klíčem (náhodně vygenerované číslo o délce 1024 bitů), což není považováno za bezpečné. Vaším úkolem je získat text z 11. zprávy. Předpokládejte, že znaky původní zprávy obsahují pouze malá písmena a mezery (tzn. žádná čísla ani interpunkční znaménka ani háčky a čárky – pracuje se s ASCII znaky).
Váš program nemusí 100% odhalit každý znak zprávy. Z vašeho útoku může vyplynout např. následující kus textu:
`??yz ti v??i hor?? nem?t?j se v ?uchy?i`

V takovém případě zkuste provést analýzu pravděpodobných znaků, případně hrubou silou naleznětě zbývající znaky a zprávu přečtětě. Vytvořte rovněž soubor `readme.txt`, ve kterém popíšete svoje řešení.

Váš program společně se souborem `readme.txt` a všemi soubory z archivu se zadáním zabalte do ZIP souboru a pojmenujte ho podle svého osobního čísla.

**Nápověda:** uvědomte si, jaké vlastnosti má XOR operace a také co se stane pokud uděláte XOR na dva šifrované texty. Co se stane pokud je znak mezera je XORován se znakem [a-zA-Z], One-time-pad

Za úspěšné vyřešení obdržíte 4 bodů.