**KPB**

**Ostrava 2022 Vojtěch Prokop**

**2. zápočtový úkol**

**KPB**

**Vedoucí práce: RNDr. Eliška Ochodková, Ph.D**

**Vypracoval: Vojtěch Prokop**

**Studijní obor: IVT**

Obsah

[ÚKOL Č. 1 5](#_Toc100159625)

[1.1 Zadání 5](#_Toc100159626)

[1.2 Použité instrumenty 5](#_Toc100159627)

[1.3 Řešení 5](#_Toc100159628)

[1.4 Dešifrovaný text 7](#_Toc100159629)

[1.5 Odpovědi 7](#_Toc100159630)

[ÚKOL Č. 2 8](#_Toc100159631)

[1.6 Zadání 8](#_Toc100159632)

[1.7 Použité instrumenty 8](#_Toc100159633)

[1.8 Řešení 8](#_Toc100159634)

[1.9 Šifrovaný text 9](#_Toc100159635)

[1.10 Dešifrovaný text 9](#_Toc100159636)

[1.11 Odpovědí 9](#_Toc100159637)

[ÚKOL Č. 3 10](#_Toc100159638)

[1.12 Zadání 10](#_Toc100159639)

[1.13 Použité instrumenty 10](#_Toc100159640)

[1.14 Řešení 10](#_Toc100159641)

[10](#_Toc100159642)

[11](#_Toc100159643)

[1.14.1 Dešifrovaný text 11](#_Toc100159644)

[1.14.2 Dešifrovaný text s mezerami 12](#_Toc100159645)

[1.15 Odpovědi 12](#_Toc100159646)

[ÚKOL Č. 4 13](#_Toc100159647)

[1.16 Zadání 13](#_Toc100159648)

[1.17 Použité instrumenty 13](#_Toc100159649)

[1.18 Řešení 13](#_Toc100159650)

[1.19 Odpověďi 14](#_Toc100159651)

[ÚKOL Č. 5 15](#_Toc100159652)

[1.20 Zadání 15](#_Toc100159653)

[1.21 Použité instrumenty 15](#_Toc100159654)

[1.22 Řešení 15](#_Toc100159655)

[1.23 Dešifrovaný text 16](#_Toc100159656)

[1.24 Odpovědi 16](#_Toc100159657)

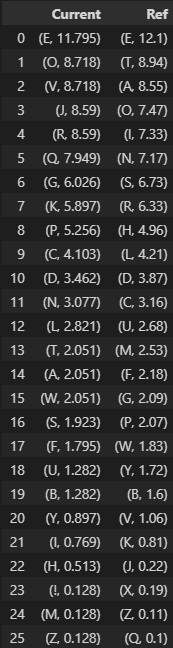
# ÚKOL Č. 1

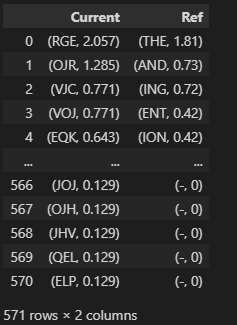
## Zadání

## Použité instrumenty

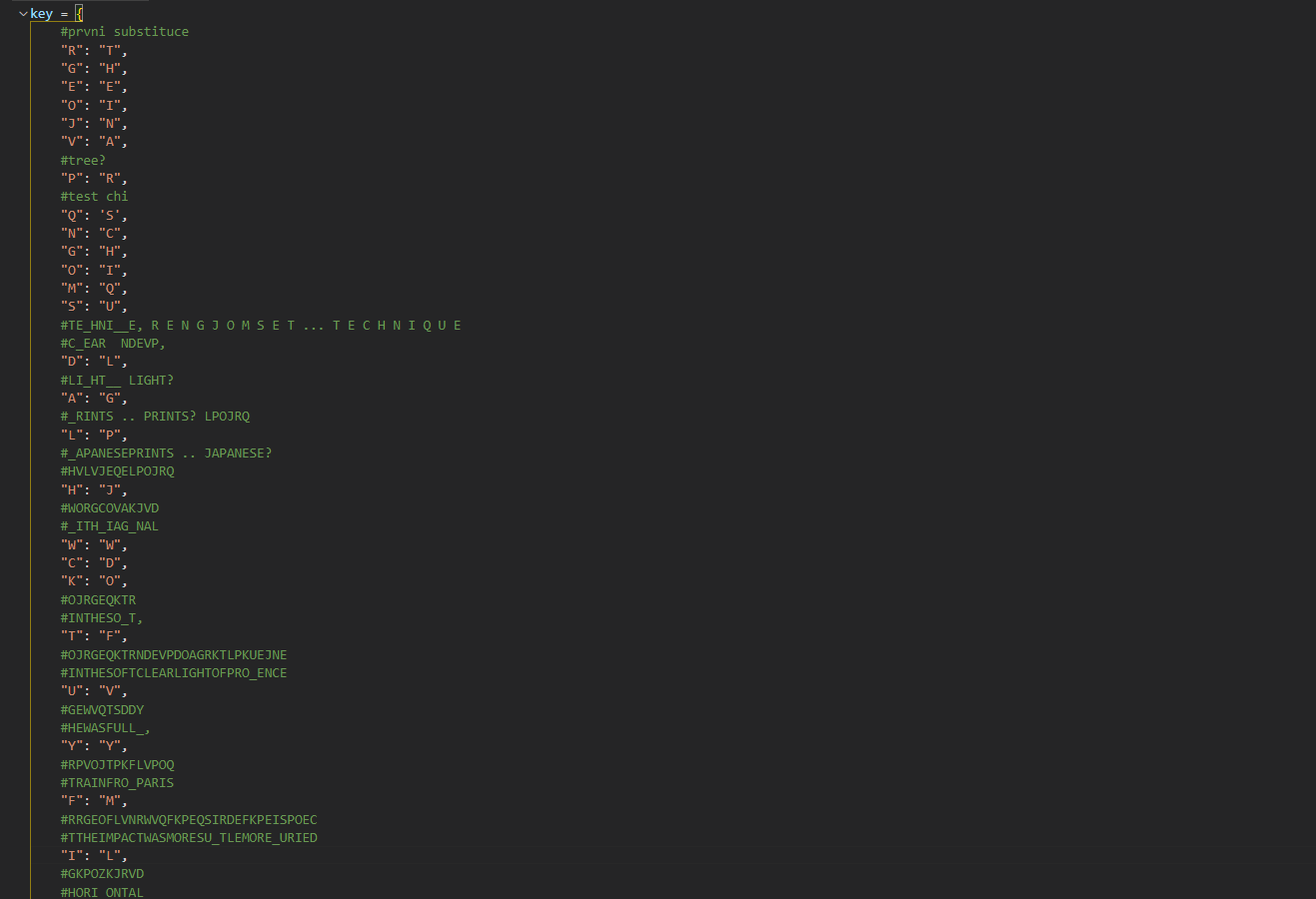
* Python
  + Frekvence n-gramu
  + Chi

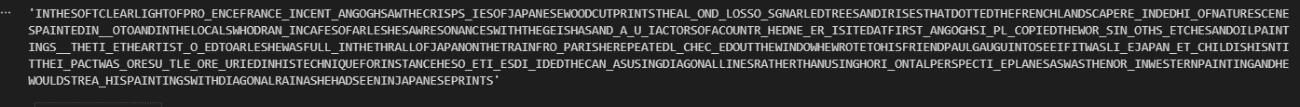
## Řešení

Implementoval jsem pomocné funkce na zobrazení statistik v textu a pomocí nich postupně tvořil klíč, reprezentující správnou substituci. Pomocné metody vypisovaly počet n-gramu.



Postupně jsem se pokoušel nahrazovat jednotlivé znaky, a tak jsem dospěl k dešifrování. Slovník, v kterém jsem udržoval překlady jsem postupně obohacoval o komentáře, které krátce popisují, jak jsem postupoval. V prvním kroku substituce jsem vycházel z frekvenční analýzy (trigramy). Nahrazení znaků z trigramu THE. Následně jsem podobné kroky aplikovat pro monogramy společně s statistickou metodou chí-kvadrát testu.



Po pár těchto pokusech jsem si napsal pomocnou metodu, která vypsala řetězec v podobě, kde neznámé byly nahrazeny znakem \_.

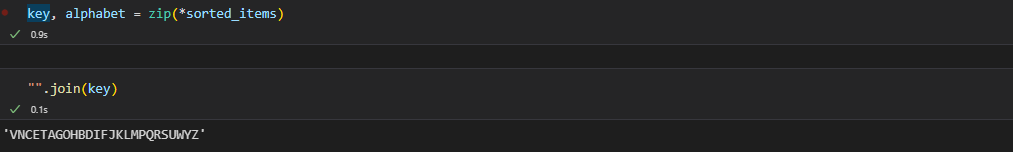
V takto zkonstruovaném řetězci jsem vždycky našel kus anglického slova, který mohl být doplněn. Z komentářů tyto slova lze pozorovat. Tree, Technique, Prints, With Diagonal, Provence, Fully, From, Horizontal..

## Dešifrovaný text

INTHESOFTCLEARLIGHTOFPROVENCEFRANCEVINCENTVANGOGHSAWTHECRISPSKIESOFJAPANESEWOODCUTPRINTSTHEALMONDLLOSSOMSGNARLEDTREESANDIRISESTHATDOTTEDTHEFRENCHLANDSCAPEREMINDEDHIMOFNATURESCENESPAINTEDINKYOTOANDINTHELOCALSWHODRANKINCAFESOFARLESHESAWRESONANCESWITHTHEGEISHASANDKALUKIACTORSOFACOUNTRYHEDNEVERVISITEDATFIRSTVANGOGHSIMPLYCOPIEDTHEWORKSINLOTHSKETCHESANDOILPAINTINGSLYTHETIMETHEARTISTMOVEDTOARLESHEWASFULLYINTHETHRALLOFJAPANONTHETRAINFROMPARISHEREPEATEDLYCHECKEDOUTTHEWINDOWHEWROTETOHISFRIENDPAULGAUGUINTOSEEIFITWASLIKEJAPANYET\_CHILDISHISNTITTHEIMPACTWASMORESULTLEMORELURIEDINHISTECHNIQUEFORINSTANCEHESOMETIMESDIVIDEDTHECANVASUSINGDIAGONALLINESRATHERTHANUSINGHORIZONTALPERSPECTIVEPLANESASWASTHENORMINWESTERNPAINTINGANDHEWOULDSTREAKHISPAINTINGSWITHDIAGONALRAINASHEHADSEENINJAPANESEPRINTS

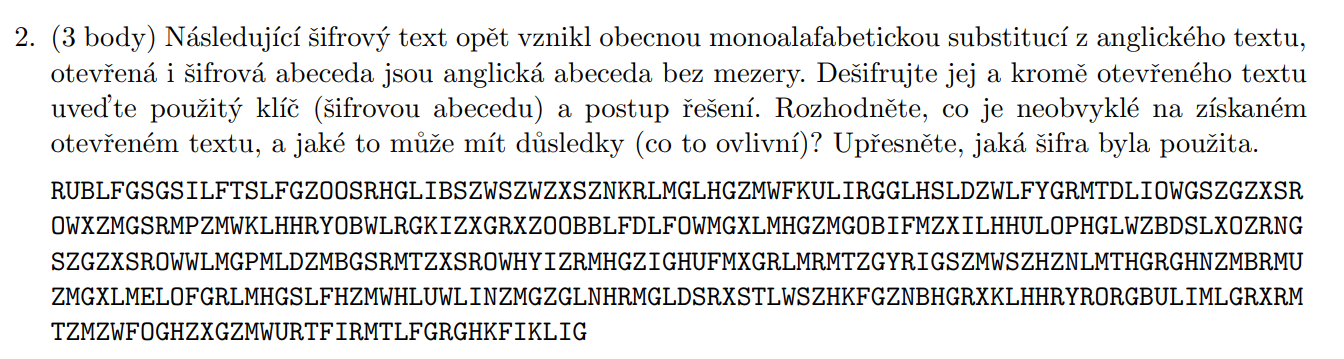
## Odpovědi

Klíč = **VINCETAGOHBDFJKLMPQRSUWYZ**



# ÚKOL Č. 2

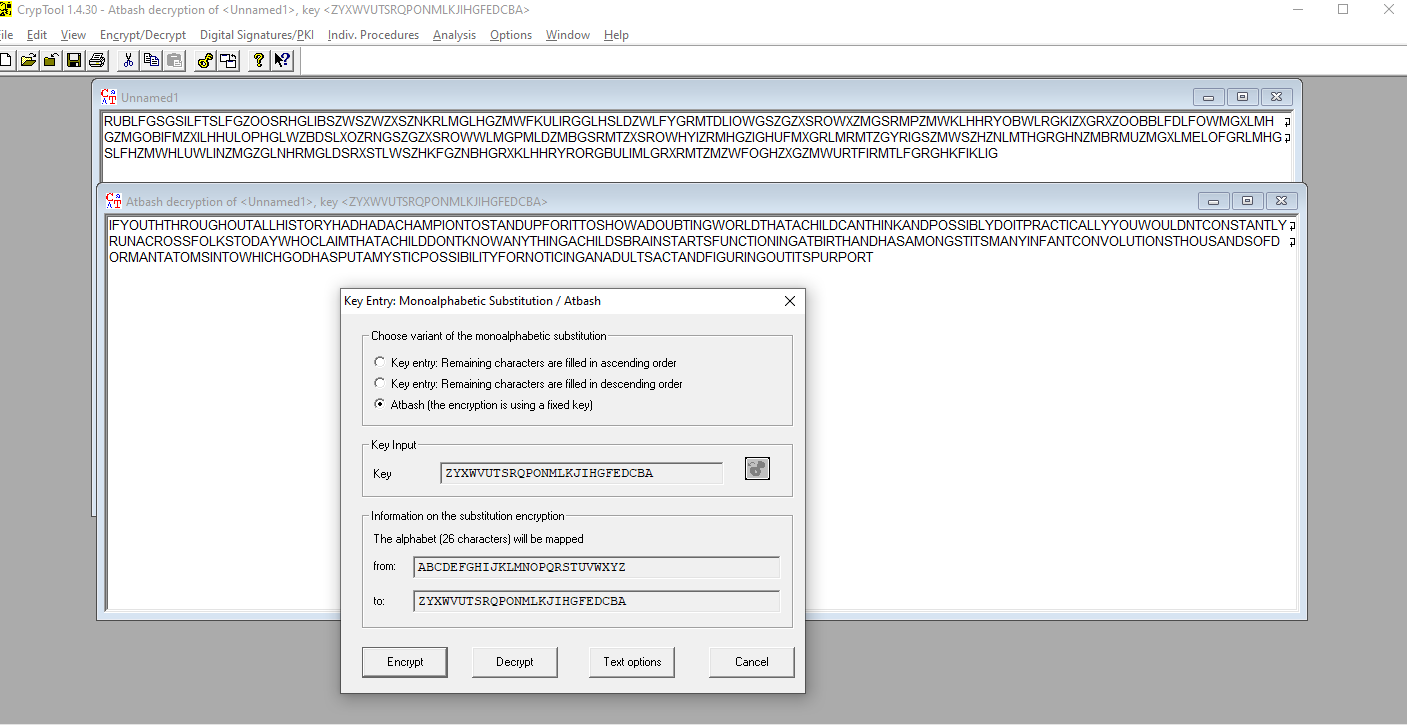
## Zadání



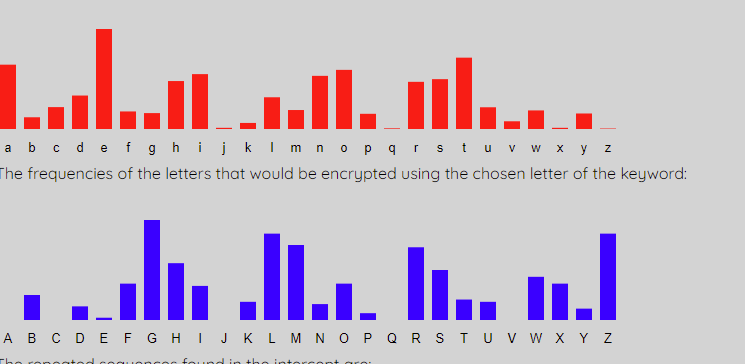
## Použité instrumenty

* Python
* CryptTool
* https://crypto.interactive-maths.com/kasiski-analysis-breaking-the-code.html

## Řešení



V druhém úkolu byl využit **CrypTool**, který po správném nastavení dešifroval text. Prvně byl pokus o stejný přístup jako v prvním příkladě, ale bohužel se nepovedlo moc dobře pokročit pomocí frekvenční analýzy.



## Šifrovaný text

RUBLFGSGSILFTSLFGZOOSRHGLIBSZWSZWZXSZNKRLMGLHGZMWFKULIRGGLHSLDZWLFYGRMTDLIOWGSZGZXSROWXZMGSRMPZMWKLHHRYOBWLRGKIZXGRXZOOBBLFDLFOWMGXLMHGZMGOBIFMZXILHHULOPHGLWZBDSLXOZRNGSZGZXSROWWLMGPMLDZMBGSRMTZXSROWHYIZRMHGZIGHUFMXGRLMRMTZGYRIGSZMWSZHZNLMTHGRGHNZMBRMUZMGXLMELOFGRLMHGSLFHZMWHLUWLINZMGZGLNHRMGLDSRXSTLWSZHKFGZNBHGRXKLHHRYRORGBULIMLGRXRMTZMZWFOGHZXGZMWURTFIRMTLFGRGHKFIKLIG

## Dešifrovaný text

IF YOUTH THROUGHOUT ALL HISTORY HAD HAD A CHAMPION TO STANDUP FOR IT TO SHOW A DOUBTING WORLD THAT A CHILD CAN THINK AND POSSIBLY DO IT PRACTICALLY YOU WOULDNT CONSTANTLY RUN ACROSS FOLKS TODAY WHO CLAIM THAT A CHILD DONT KNOW ANYTHING A CHILDS BRAIN STARTS FUNCTIONING AT BIRTH AND HAS AMONGST ITS MANY INFANT CONVOLUTIONS THOUSANDS OF DORMANT ATOMS INTO WHICH GOD HAS PUT A MYSTIC POSSIBILITY FOR NOTICING AN ADULTS ACT AND FIGURING OUT ITS PURPORT

## Odpovědí

* Nemá obvyklou distribuci znaků.
* Klič = **ZYXWVUTSRQPONMLKJIHGFEDCBA**

# ÚKOL Č. 3

## Zadání

## Použité instrumenty

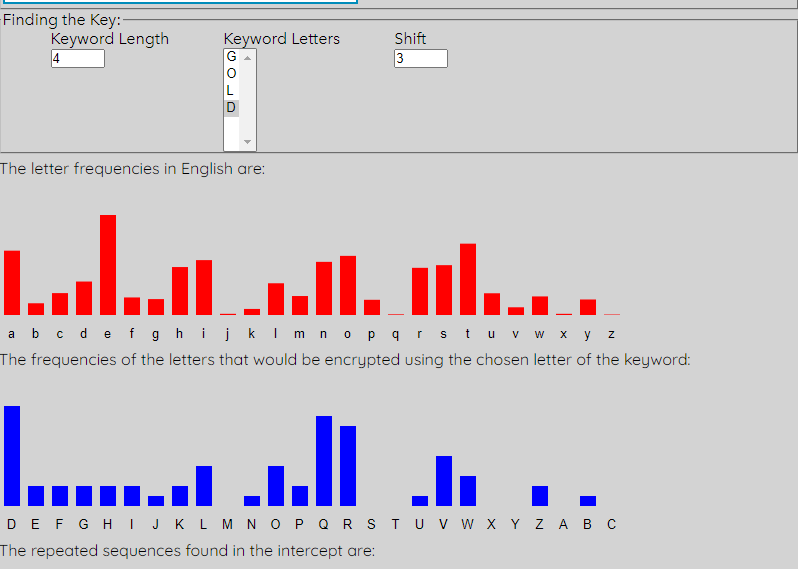
* <https://crypto.interactive-maths.com/kasiski-analysis-breaking-the-code.html>
* CryptoTool

## Řešení

V prvním kroku byl využit online nástroj, který pomocí Kasiského testu provedl analýzu a vizualizoval vzdálenost výskytu daného n-gramu společně s děliteli. Jelikož jsem věděl, že klíč na šifrování je velikost méně jak 6, pak jsme mohli odhadnout, že klíč bude 2 nebo 4.

## 

Po rozdělení celistvého textu na 4 sloupce jsem byl schopen provést frekvenční analýzu s mapováním na anglický text, díky kterého jsem odhadl klíč.



Po uhodnutém klíči na dešifrování jsem využil CryptoTool nástroj, dle kterého jsem si vygeneroval otevřený text. Tento text jsem obohatil o mezery.

### 

### Dešifrovaný text

BYWINNINGGOLDINBOTHSNOWBOARDANDALPINESKIINGLEDECKAHASCHALLENGEDTHECONVENTIONALWISDOMREGARDINGWHATISACHIEVABLEANDSHEHADAMESSAGEFORANYYOUNGSTERSWHOMIGHTWISHTOFOLLOWINHERFOOTSTEPSANDAIMFORSUCCESSONBOTHSKISANDSNOWBOARDDOWHATEVERYOUWANTSHESAIDIFYOUWANTTOCHOOSEJUSTONETHENCHOOSEJUSTONEIWANTEDTOCHOOSEBOTHANDALOTOFPEOPLETOLDMETHATITSNOTPOSSIBLETOGETTOTHETOPINBOTHOBVIOUSLYITSNOTEASYITSAGREATTHINGTHATICANBEHEREINBOTHSPORTSANDENJOYBOTHSPORTSHEREINTHEREPUBLICOFKOREAMYPLANISTOSTAYWITHMYHEARTSOFORNOWITHINKIWILLDOBOTHBECAUSEILOVEBOTHANDILOVETODOTHISSHEADDED

### Dešifrovaný text s mezerami

BY WINNING GOLD IN BOTH SNOWBOARD AND ALPINE SKIING LEDECKA HAS CHALLENGED THE CONVENTIONAL WISDOM REGARDING WHAT IS ACHIEVABLE AND SHE HAD A MESSAGE FOR ANY YOUNGSTERS WHO MIGHT WISH TO FOLLOW IN HER FOOTSTEPS AND AIM FOR SUCCESS ON BOTH SKIS AND SNOWBOARD DO WHATEVER YOU WANT SHE SAID IF YOU WANT TO CHOOSE JUST ONE THEN CHOOSE JUST ONE I WANTED TO CHOOSE BOTH AND A LOT OF PEOPLE TOLD ME THAT ITS NOT POSSIBLE TO GET TO THE TOP IN BOTH OBVIOUSLY ITS NOT EASY ITS A GREAT THING THAT I CAN BE HERE IN BOTH SPORTS AND ENJOY BOTH SPORTS HERE IN THE REPUBLIC OF KOREA MY PLAN IS TO STAY WITH MY HEART SO FOR NO WITH INKI WILL DO BOTH BECAUSE I LOVE BOTH AND I LOVE TO DO THIS SHEADDED

## Odpovědi

* Velikost klíče jsou 4 znaky.
* Klíč na šifrování a dešifrování je GOLD.

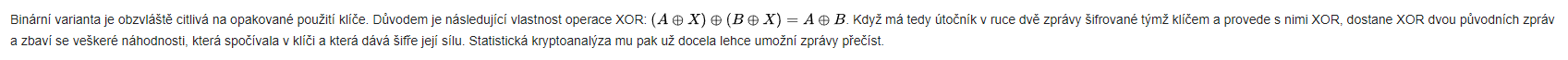
# ÚKOL Č. 4

## Zadání

## Použité instrumenty

* <https://isaaccomputerscience.org/concepts/data_encrypt_vernam?examBoard=all&stage=all>
* https://cs.wikipedia.org/wiki/Vernamova\_%C5%A1ifra

## Řešení



Předpokládáme, že pokud by byly klíče různé, pak bychom neměli možnost rozluštit šifrované zprávy. Respektive bychom mohli možná aplikovat přístup, kdy bychom zkoušeli různý klíč pro šifrovanou zprávu a pokud by bylo slovo ze slovníku, pak bychom si ho uložili. Přesto si ale myslím že nebudeme mít jistotu správného dešifrování. Jelikož tato operace nám bude moci vyprodukovat více správných slov z dodaného slovníku.

Předpokládejme tedy, že po provedení XOR mezi C1 a C2 dostaneme XOR mezi originálními zprávami. Na tomhle můžeme provést pokus o dešifrování.

* Provedení XOR mezi C1 a C2.
* Načtení slovníku.
* Vyfiltrování slovníku, 12 znaků dlouhé slova.
* Iterace přes všechny tyto slova, přičemž využijeme doplněk k získání znaku pro msg2\_j. Pokud nezůstáváme v povolené abecedě otevřeného textu přeskakujeme a zkoušíme další slovo.
* Pokud zůstaneme v abecedě pro všech 12 znaků, pak testujeme, zda slovo existuje v definovaném slovníku.
* Pokud ano máme řešení.
* Z výsledných dvou slov získáme klíč pomocí C1 ^ msg1 a analogicky pro C2.

## Odpověďi

* M1 = **Lichtenstein**
* M2 = **superimposes**
* Klíč = **plausibility**

# ÚKOL Č. 5

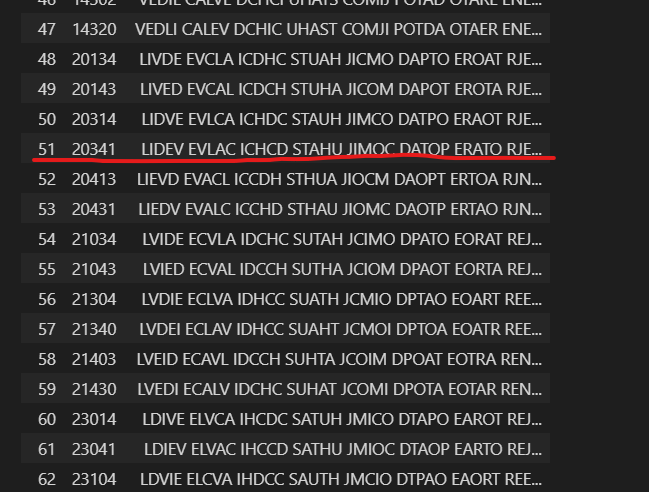
## Zadání

## Použité instrumenty

* https://tholman.com/other/transposition/

## Řešení

* Implementace metody, která vytvoří matici vzhledem k velikosti klíče.
  + Klíč definuje počet sloupců.
* Text je rozdělen na segmenty, tak aby šel vložit to matice o n sloupcích.
* Segmenty textu byly vloženy do matice.
* Sloupce byly přehazovány, tak aby bylo zajištěno bezpečnější šifrovací mechanismus.
* Implementoval jsem metodu, která vytvořila všechny možné permutace vzhledem k přehození sloupců, a tyto texty explicitně procházel a zkoušel najít text, který bude v mateřském jazyce.
* K tomuto otevřenému textu byl následně nalezena šifrovací permutace. Podobným způsobem jako u dešifrování ale převrácený postup. Uložil jsem si permutaci, která generovala text rovný s šifrovým textem.



## Dešifrovaný text

LIDE VE VLACICH CD STAHUJI MOC DAT OPERATOR JE NELZEVNI NAOPAK JE O MEZI ZAKAZNICI CESKYCH DRAH SE NA SOCIALNICH SITICH PODIVUJI NAD ZVAZOVANYM OMEZENIM DAT STAHOVANYCH PŘES WIFI VE VLACICH POPISUJI ZKUSENOSTI S POMALYM A NESTABILNIM PRIPOJENIM PARADOX NE TAK BYLA POPRENA ORIGINALNI EKONOMICKA TEORIE MINISTRYNE MARTY NOVAKOVE KDY VI CESTA ZENYCH DAT ZNAMENA JEJICH ZLEVNENI CO TAM KDO STAHUJE VZDYT SIGNAL FURT PADA A JE TO POMALE TO MAM RYCHLEJSI MOBILNI POPSAL JEDEN Z DISKUTUJICICH NA FACEBOOKU UMEALE SPONTAKRKA VŽDY NEFUNKCNI ZNIDALSIKOMENTARNAADRESU WIFICDO MEZITDATAVICUZ TO SNAD ANI NEJDE NEPTA SE RECNICKY DAL SI CESTUJICI **QQ**

## Odpovědi

* Šifrovací permutace - **14023**
* Dešifrovací permutace - **20341**