ŠIFROVACÍ KROUŽEK - 2. hodina

Stereogram ... je optická iluze trojrozměrného zobrazení na dvourozměrném obrázku. Stereogram může být zábavná forma jak schovat nějakou zprávu nebo obrázek.

Příklady: http://www.hidden-3d.com

Další transpoziční šifry:

1. Sloupcová transpozice s klíčem. Nejprve si napíšeme text do tabulky:

   SIFR
   OVAC
   IKRO
   UZEK

   Zvolíme si „klíč" – nějaké slovo o stejném počtu písmen, kolik je sloupců v naší šifře. Pro zjednodušení bude klíč zrovna slovo KLIC. Seřadíme si písmena klíče podle abecedy, tedy: K-3, L-4, I-2, C-1. Tento číselný klíč si napíšeme nad naší tabulku:

   3421
   SIFR
   OVAC
   IKRO
   UZEK

   Nyní šifrujeme po sloupcích a pořadí sloupců je podle klíče: Výsledná šifra je tedy:

   Výsledek: **RCOK FARE SOIU IVKZ**

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

2. Dvojitá sloupcová transpozice. Je totéž jako předchozí jednoduchá sloupcová transpozice, ale je aplikovaná 2x. Můžeme použít stejný anebo jiný klíč.

   Napíšeme si předchozí výsledek do stejné tabulky:

   ```
   3421
   RCOK
   FARE
   SOIU
   IVKZ
   ```

   Stejným způsobem jako minule pak dojdeme k následujícímu výsledku:

   Výsledek: **KEUZ ORIK RFSI CAOV**

3. Myszkowskiho transpozice – tuto vymyslel Émile Victor Théodore Myszkowski roku 1902. Principem je zvolit si klíč, který má opakující se písmeno. V našem případě zvolíme klíč např. BFAB … naše pořadí znaků klíče tedy bude 2 3 1 2

   ```
   2312
   SIFR
   OVAC
   IKRO
   UZEK
   ```

   Nyní sloupce s neopakujícími se čísly (1 a 3) prezentujeme stejně jako v jednoduché sloupcové transpozici, tedy od shora dolů, zatímco sloupce s opakujícím se číslem (2) zapisujeme postupně zleva-doprava ... tedy:

   Výsledek: **FARE SROC IOUK IVKZ**

4. Šifrovací mřížka: První známá mřížka je od matematika, filosofa, astronoma a astrologa jménem: Hieronymus Cardanus (nebo Gerolamo Cardano), který žil v letech 1501 – 1576.

   Šifrovací mřížku zpopularizoval Jules Verne ve svém románu Matyáš Sandorf. Ještě za první světové války se používala tzv. Fleissnerova mřížka.

   Princip mřížky je jednoduchý, do vytvořené mřížky se zapíše text, poté se mřížka otočí o 90° napíše se pokračování, znovu a znovu. Tak je popsán text celého čtverce a mřížka jej umožňuje číst.

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

Nástroje k luštění šifer: Frekvenční analýza

Principem frekvenční analýzy, je zjistit četnost jednotlivých znaků a porovnat s průměrnou četností písmen v určitém jazyce.

Např. zde:
http://rumkin.com/tools/cipher/frequency.php

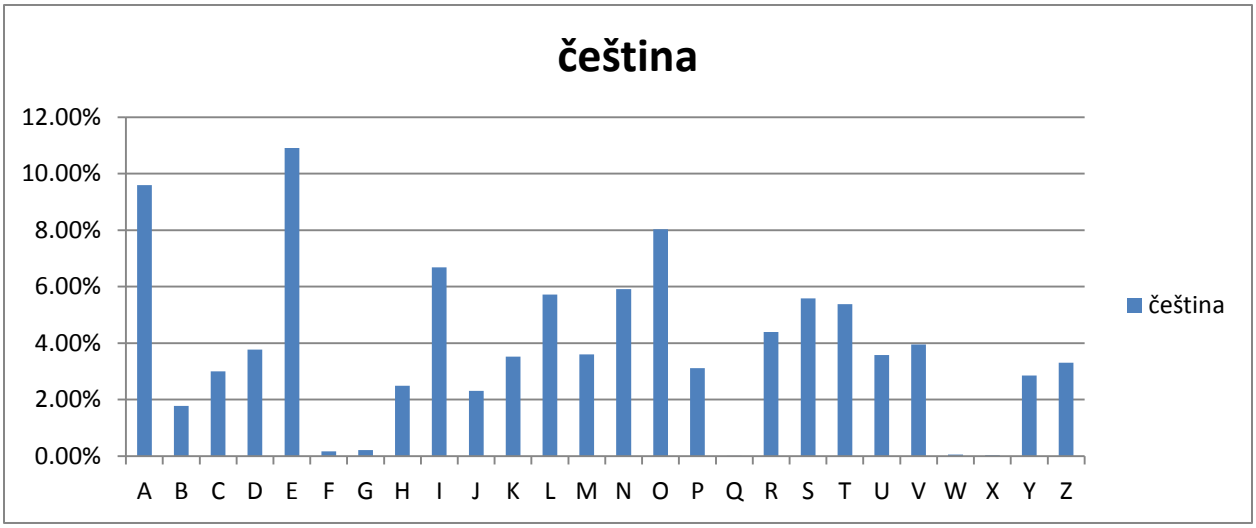
nebo zde:
http://www.musilek.eu/michal/sifry-frekvence.html?menu=cc&item=t&lang=cz

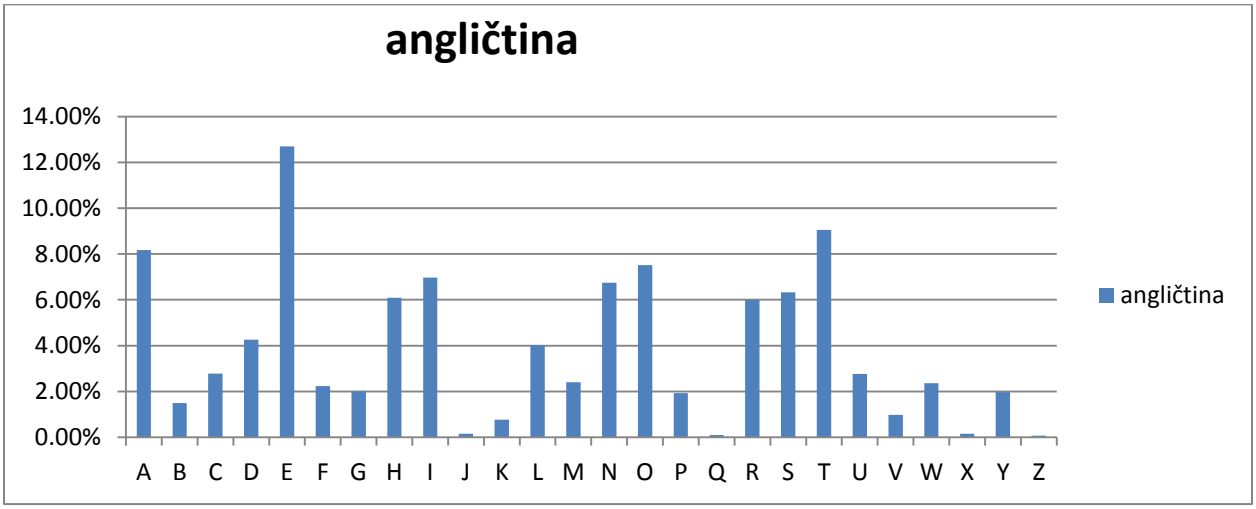
Průměrná četnost znaků v češtině a angličtině

Písmeno	čeština	angličtina
A	9.59%	8.17%
B	1.78%	1.49%
C	3.00%	2.78%
D	3.77%	4.25%
E	10.90%	12.70%
F	0.18%	2.23%
G	0.22%	2.02%
H	2.50%	6.09%
I	6.69%	6.97%
J	2.31%	0.15%
K	3.53%	0.77%
L	5.72%	4.03%
M	3.61%	2.41%
N	5.92%	6.75%
O	8.03%	7.51%
P	3.11%	1.93%
Q	0.01%	0.10%
R	4.40%	5.99%
S	5.59%	6.33%
T	5.39%	9.06%
U	3.58%	2.76%
V	3.95%	0.98%
W	0.05%	2.36%
X	0.04%	0.15%
Y	2.86%	1.97%
Z	3.30%	0.07%

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.QUEST
Pořádá RADIOKLUB OK1KPI Písek





Ostatní jazyky: http://en.wikipedia.org/wiki/Letter_frequency

Frekvenční analýza funguje tím lépe, čím delší text máme k dispozici. Při krátkých úsecích textu nemusí být přesná.

Frekvenční analýza nám pomůže určit, zda se jedná o češtinu a pokud ano, pak zároveň víme, zda písmenka sobě odpovídají, tedy že se jedná o nějaký tip transpoziční šifry.

Frekvenční analýzu použil ve své povídce Zlatý brouk např. Edgar Allan Poe: http://cs.wikipedia.org/wiki/Zlat%C3%BD_brouk

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

Cvičení:

1. **Rozluštěte sloupcovou šifru s klíčem: CMELAK**

   JZLPLVR NEUVVUU NRTJICI SLSROOU IOIISOF YMSONPS

2. **Rozluštěte Myszkowskiho transpozici s klíčem: CERCANY**

   ELSKSDI TLNSIJI ARJDULT OETFOOU JOITMVL HJERUSS EZSEEYI

3. **Zašifrujte libovolný text pomocí mřížky a dejte přečíst postupně ostatním.**

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.QuEst
Pořádá RADIOKLUB OK1KPI Písek

Úkol: Chodíte rádi na procházky? V okolí Čerčan je schované poselství, dokážete ho do příští hodiny najít a rozluštit? Cestu k posleství najdete, když postupně rozluštíte následující šifry. Když rozluštíte první, dovíte se jak rozluštit druhou, atd.

1.

KIBKDIFE TPTELASR NERRTILI JIMIEICS OEKVJTJK DLPOAMIE RSOOBLEO PEKUMEEN

2.

ORTIZINIJVCLYDNTC NIZRKEKDINEVNIEOZ RDETONCSUEIATOAUC
PAJSRTILRZNDCMCLA ANIIYSLAFASZEKRZN TAUCCKASEVEERCPEE

3.

YOAMZAEOOAAZHUSZ ZUEIEVAHADZADTOC AELZCEZRCAIETEEI UUEPORVOETEHRSAU
VPNRINCVTTRIUEOE ITSHREVRZEATESMK TEMOCDLBLVKKJIUO RZCEAMSKVVVOLVTN

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.Quest
Pořádá RADIOKLUB OK1KPI Písek