Frekvenční analýza a substituční šifra pro začátečníky

Před nějakou dobou jsem luštil jednu obzvláště vypečenou mystery keš z okolí Plzně. Když jsem vyčerpal všechny dobré nápady, došlo na frekvenční analýzu (FA). Prohledal jsem internet a nalezl několik slušných stránek o tom, jak frekvenční analýza funguje a dokonce stáhnul i pár šifrovacích programů, které FA umějí. Žádný z programů, ale nedokázal uživatelsky přívětivě proměnit výsledek analýzy v rozšifrovaný text. To mě přimělo vytvořit vlastní jednoduchý program, díky kterému se mi podařilo šifru rozluštit. V tomto krátkém článku bych se rád podělil o program samotný a o zkušenosti s jeho použitím.

1) **Co je frekvenční analýza?** Stručně řečeno, je to analýza frekvence, tedy četnosti výskytu jednotlivých znaků v textu. Pokud máme například text o 100 písmenech a písmenko „A“ se v něm vyskytuje 10x, „B“ 5x a „C“ 1x, znamená to, že průměrná četnost písmena „A“ v daném textu je 10%, „B“ 5% a „C“ 1%... Tímto způsobem zjistíme četnost výskytu všech v textu obsažených znaků. Důležité je zmínit, že v každém jazyce jsou výskyty písmen různé. Tedy četnost výskytu písmene „a“ v Češtině se bude lišit od četnosti výskytu písmene „a“ v Angličtině. Na internetu se dají najít frekvence znaků pro většinu řečí, Češtinu nevyjímaje. Další důležité upozornění je, že záleží na velikosti referenčního vzorku (čím více textu, tím přesnější čísla) a na druhu textu, který analyzujete.
   Například kapitola o chovu okounů bude mít jinou četnost výskytu písmene „O“, než například text písničky Královské Rege, kde zase bude výrazně vyšší četnost písmene „R“.

   K čemu to mohu využít? Frekvenční analýzu je možné použít na luštění různých plyalfabetických substitučních šifer – jednoduše – když jsou v textu nahrazena písmena jinými písmeny. Například: nezašifrovaný text: „Harry Potter „ Zašifrovaný text: „jsttx úpzzrt“. Případně, když jsou písmena nahrazena znaky, nebo obrázky.

2) **Jak to využít v praxi?** Uvádím příklad.
   K rozluštění mám následující text:
   „ΑΒΧΕΔΦΓ ΗΙϑΑϑ ΚΑΛ ΓΥΙΒΜΗΑ ΝΑ ΟΚΦΚΕΓΗΑΗΦ Α ΟΕΛΕΠΙΗΥΝΓΦ ΧΝΙΚ ΨϑΦ ΛΕΧΝΕΚ ΓΔΑΒΜ ΟΚΕΟΔΙΝΑ ΥΤΓ ΝΙϑΟΙΚΑϑΙΗΝΗΦ ΚΙΒΦ ςΖΗΑΓΑϑ ΖΙ Η Α ΝΕϑ ΗΑΖΕΚΗΙϑ ΟΚΦΧΔΑΛς Υ ΧΑΓΑΚΗΕς ΒΔΕΓΙΧΙϑ Α ϑΦΥΕς ΧΕΠΔΦΜ ΗΙ ΒΕ ΣΙ ΔΖΙ ΗΑ ΗΙϑ ΑΥΟΕΗ ΟΚΦΠΔΦΖΗΙ ςΧΑΖΑΝ ΣΑΧΨϑ ΒΔΕΓΙΧΙϑ ΣΙ ΥΑΝς ΚΗΦΗ ΛΕΧΝΕΚ ΓΔΑΒΜ ΥΦ ΝΕΝΦΖ ΚΕΖΛΙΔΦΔ ΔΦΛΦ ΟΕΛΔΙ ΝΕΜΕ ΣΑΧ ΥΙ ΒΜΕΓΑΣΦ Γ ΟΕΔΕΟΚΑΖΛΗΙ ΧΑΓΑΚΗΙ ϑΑΣΦΔΦ ΟΚΙΛ ΥΙΠΕς ϑΦΥς ΧΕΠΔΦΜ ΟΚΙΛΥΝΑΓΝΙ ΥΦ ΔςΞςΥΗΦ ΧΑΓΑΚΗς ΖΑ ΗΙΛΙΔΗΦΜΕ ΕΛΟΕΔΙΛΗΙ ΓΙΗΧς ΣΙ Χ ΚΑΥΗΨ ΛΙΗ Α ΜΕΥΝς Γ ΧΑΓΑΚΗΙ ΣΙ ϑΑΔΕ ςΖ ΣΥΝΙ ΥΙ ΗΑΥΗΦΛΑΔΦ ΟΚΙΒΙ ΝΔΦ ΣΥΝΙ ΓΥΙΒΜΗΨ ΗΕΓΦΗΨ Α ΝΙΛ ΣΥΝΙ ΥΙ ΟΕΜΕΛΔΗΙ ΕΟΚΙΔΦ Γ ϑΙΧΧΙϑ ΠΕΞς Α ΖΑϑΨΥΔΙΗΙ ΥΙ ΛΦΓΑΝΙ ΗΑ ϑΦΥς ΧΕΠΔΦΜ ΗςΛΑ ΥΙ ΟΕϑΑΔς ΚΕΖΔΙ ΖΑ ΛΕ ΓΥΙΒΜ ΧΕςΝς ΧΑΓΑΚΗΨ Α Νς ΥΙ ΝΙΛΨ ϑΑ ςΧΑΖΑΝ ΛΕ ΧΝΙΚΙ ΥΧςΟ ΦΗΨ ΔΦΛΦ ΟΕΛΔΙ ΝΙΕΚΦΙ ΛΕΧΝΕΚΑ ΓΔΑΒΜΑ ΟΑΝΚΦΝΙ ΣΥΝΙΔΦ ΟΚΨ ΒΔΕ ΓΙΧΙϑ ΠΙΖ ΘΑΗΝΑΖΦΙ ΠΙΖ ΝΕςΜΨ ΟΕ ΛΨΗΑϑΦΒΙ Α ΠΙΖ ΥϑΨΥΔς ΟΚΕ ΜςϑΕ Κ ΠςΛΙΝΙ ΥΙ ΗΑ ΝΨ ΧΕΠΔΦΜΨ ΛΦΓΑΝ ΝςΟΙ Α ΠΙΖϑΨΥΔΙΗΧΕΓΦΝΙ ΝΚΙΠΑ ΑΖ ΛΕ ΟΕΔΙΛΗΙ Α ΟΑΧ ΥΙ ΖΓΙΛΗΙΝΙ Α ΟςΣΛΙΝΙ Χ ΕΠΙΛς ϑΑϑ ΛςΓΕΛΗΙ ΟΕΛΙ ΖΚΙΗΦ ΖΙ ΛΕ ΝΙΝΕ ΟΚΓΙ ΥΧςΟΦΗΨ ΖΑΚΑΖςΣΙ ΛΕΧΝΕΚ ΓΔΑΒΜ ΝΑΧΙ ϑΗΙ ϑ ΨΥΔΦϑ ΖΙ ΗΙΗΦ Γ ΟΚΑΓς Ε ΜςϑΕΚς Α Ε ΝΙ ΛΨΗΑϑΦΒΙ ΗΙΠςΛΙϑΙ ϑΔςΓΦΝ ΑΔΙ ΝΕ ΖΙ ϑΦ ςΟΦΚΑ ΘΑΗΝΑΖΦΦ ΧΛΨΖ ΓΦ ΖΙ ΥΙ ϑΦ ΟΕΓΛΔΕ ΥΟΚΑΓΗΙ„

   a) Jako první krok přiřadíme každému symbolu jedno písmeno z naší abecedy, abychom mohli zanalyzovat. Nejsnazší postup je začít u A, a pokračovat přes B…. až do Z. Výsledkem bude:

„ABCEDFG HIJAJ KAL GUIBMHA NA OKFKEGHAHF A OELEPIHUNGF CNIKYJF LECNEK GDABM OKEODINA UGI NIJOIKAJIHNHF KIBF VZHAGAJ ZI HA NEJ HAZEKHIJ OKFCDALV U CAGAKHEV BDEGICIJ A JFUEV CEPDFM HIBE SI DZI HA HIJ AUOEH OKFPDFZHI VCAZAN SACYJ BDEGICIJ SI UANVKHFH LECNEK GDABM UF NENFZ KEZLIDFD DFLF OELDI NEME SAC UI BMEGASF G OEDEOKAZLHI CAGAKHI JASFDF OKIL UIPEV JFUV CEPDFM OKILUNAGNI UF DVXVUHF CAGAKHV ZA HILIDHFME ELOEDILHI GIHCV SI CKAUHY LIH A MEUNV G CAGAKHI SI JADE VZ SUNI UI HAUHFLADF OKIBINDF SUNI GUIBMHY HEGFHY A NIL SUNI UI OEMELDHI EOKIDF G JICCIJ PEXV A ZAJYUDIHI UI LFGANI HA JFUV CEPDFM HVLA UI OEJADV KEZDIZA LE GUIBM CEVNV CAGAKHY A NV UI NILY JA VCAZAN LE CNIKI UCVOFHY DFLF OELDI NIEKFI LECNEKA GDABMA OANKFNI SUNIDF OKY BDEGICIJ PIZ QAHNAZFI PIZ NEVMY OE LYHAJFBI A PIZ UJYUDV OKE MVJEK PVLINI UI HA NY CEPDFMY LFGAN NVOI A PIZJYUDIHCEGFNI NKIPA AZ LE OEDILHI A OAC UI ZGILHINI A OVSLINI C EPILV JAJ LVGELHI OELIZKIHF ZI LE NINE OKGI UCVOFHY ZAKAZVSI LECNEK GDABM NACI JHI JYUDFJ ZI HIHF G OKAGV E MVJEKV A E NI LYHAJFBI HIPVLIJI JDVGFN ADI NE ZI JF VOFKA QAHNAZFF CLYZ GF ZI UI JF OEGILDE UOKAGHI „

b) Nyní přijde na řadu frekvenční analýza. Doporučuji otevřít excelovský soubor:Frekvenční analýza a prohlédnout si ho. (http://pankun.webzdarma.cz/data/fa.xls)

Do políčka F6 – s popisem Zkoumaný text nakopírujeme text, který jsme získali převodem znaků na písmena. (Bude to vypadat asi takto)

TEXT	Absolutní četnost	Relativní četnost	Vzorová četnost	Substituce
A			9,6	
B			1,8	
C			2,9	
D			3,8	
E			10,9	
F			0,2	
G			0,2	
H			2,5	
I			6,7	
J			2,3	
K			3,5	
L			5,7	
M			3,6	
N			5,9	
O			8,1	
P			3,1	
Q			0,0	
R			4,4	
S			5,6	
T			5,4	
U			3,6	
V			3,9	
W			0,1	
X			0,0	
Y			2,9	
Z			3,3	

FREKVENČNÍ ANALÝZA

Zkoumaný text:

ABCEDFG HIJAJ KAL GUIBMHA NA OKFKEGHAHF A OELEPIHUNGF CNIKYJF LECNEK GDABM OKEODINA UGI NIJOIKAJIHNHF KIBF VZHAGAJ ZI HA NEJ HAZEKHIJ OKFCDALV U CAGAKHEV BDEGICIJ A JFUEV CEPDFM HIBE SI DZI HA HIJ AUOEH OKFPDFZHI VCAZAN SACYJ BDEGICIJ SI UANVKHFH LECNEK GDABM UF NENFZ KEZLIDFD DFLF OELDI NEME SAC UI BMEGASF G OEDEOKAZLHI CAGAKHI JASFDF OKIL UIPEV JFUV CEPDFM OKILUNAGNI UF DVXVUHF CAGAKHV ZA HILIDHFME ELOEDILHI GIHCV SI CKAUHY LIH A MEUNV G CAGAKHI SI JADE VZ SUNI UI HAUHFLADF OKIBINDF SUNI GUIBMHY HEGFHY A NIL SUNI UI OEMELDHI EOKIDF G JICCIJ PEXV A ZAJYUDIHI UI LFGANI HA JFUV CEPDFM HVLA UI OEJADV KEZDIZA LE GUIBM CEVNV CAGAKHY A NV UI NILY JA VCAZAN LE CNIKI UCVOFHY DFLF OELDI NIEKFI LECNEKA GDABMA OANKFNI SUNIDF OKY BDEGICIJ

Upravený text

Substituce

Vlevo ve sloupci D jsou uvedeny vzorové četnosti výskytů znaků v Českém jazyce.
A zmáčkněte tlačítko „Analyzuj!“

TEXT	Absolutní četnost	Relativní četnost	Vzorová četnost	Substituce
A	85	5,0	**9,6**	
B	17	1,0	**1,8**	
C	36	2,1	**2,9**	
D	43	2,5	**3,8**	
E	70	4,1	**10,9**	
F	57	3,4	**0,2**	
G	39	2,3	**0,2**	
H	57	3,4	**2,5**	
I	115	6,8	**6,7**	
J	38	2,2	**2,3**	
K	42	2,5	**3,5**	
L	43	2,5	**5,7**	
M	19	1,1	**3,6**	
N	51	3,0	**5,9**	
O	35	2,1	**8,1**	
P	16	0,9	**3,1**	
Q	2	0,1	**0,0**	
R	0	-	**4,4**	
S	14	0,8	**5,6**	
T	0	-	**5,4**	
U	40	2,4	**3,6**	
V	39	2,3	**3,9**	
W	0	-	**0,1**	
X	2	0,1	**0,0**	
Y	20	1,2	**2,9**	
Z	31	1,8	**3,3**	

FREKVENČNÍ ANALÝZA

Zkoumaný text:

ABCEDFG HIJAJ KAL GUIBMHA NA OKFKEGHAHF A OELEPIHUNGF CNIKYJF LECNEK GDABM OKEODINA UGI NIJOIKAJIHNHF KIBF VZHAGAJ ZI HA NEJ HAZEKHIJ OKFCDALV U CAGAKHEV BDEGICIJ A JFUEV CEPDFM HIBE SI DZI HA HIJ AUOEH OKFPDFZHI VCAZAN SACYJ BDEGICIJ SI UANVKHFH LECNEK GDABM UF NENFZ KEZLIDFD DFLF OELDI NEME SAC UI BMEGASF G OEDEOKAZLHI CAGAKHI JASFDF OKIL UIPEV JFUV CEPDFM OKILUNAGNI UF DVXVUHF CAGAKHV ZA HILIDHFME ELOEDILHI GIHCV SI CKAUHY LIH A MEUNV G CAGAKHI SI JADE VZ SUNI UI HAUHFLADF OKIBINDF SUNI GUIBMHY HEGFHY A NIL SUNI UI OEMELDHI EOKIDF G JICCIJ PEXV A ZAJYUDIHI UI LFGANI HA JFUV CEPDFM HVLA UI OEJADV KEZDIZA LE GUIBM CEVNV CAGAKHY A NV UI NILY JA VCAZAN LE CNIKI UCVOFHY DFLF OELDI NIEKFI LECNEKA GDABMA OANKFNI SUNIDF OKY BDEGICIJ PIZ GAHNAZFI PIZ NEVMV OE IVHAIFBI A PIZ UIVUDV OKE MVIEK PVLINI UI HA NV

Upravený text

abcedfg hijaj kal guibmha na okfkeghahf a oelepihungf cnikyjf lecnek gdabm okeodina ugi nijoikajihnhf kibf vzhagaj zi ha nej hazekhij okfcdalv u cagakhev bdegicij a jfuev cepdfm hibe si dzi ha hij auoeh okfpdfzhi vcazan sacyj bdegicij si uanvkhfh lecnek gdabm uf nenfz kezlidfd dflf oeldi neme sac ui bmegasf g oedeokazlhi cagakhi jasfdf okil uipev jfuv cepdfm okilunagni uf dvxvuhf cagakhv za hilidhfme eloedilhi gihcv si ckauhy lih a meunv g cagakhi si jade vz suni ui hauhfladf okibindf suni guibmhy hegfhy a nil suni ui oemeldhi eokidf g jiccij pexv a zajyudihi ui lfgani ha jfuv cepdfm hvla ui oejadv kezdiza le guibm cevnv cagakhy a nv ui nily ja vcazan le cniki ucvofhy dflf oeldi niekfi lecneka gdabma oankfni sunidf oky bdegicij piz gahnazfi piz nevmv oe ivhaifbi a piz uivudv oke mviek pvlini ui ha nv

Substituce

V políčku Upravený text se nám zpráva automaticky převede na malá písmena, odstraní se diakritika a další znaky, které nechceme.

Nyní přišel čas prozkoumat výsledky Frekvenční analýzy:

TEXT	Absolutní četnost	Relativní četnost	Vzorová četnost	Substituce
A	85	5,0	**9,6**	
B	17	1,0	**1,8**	
C	36	2,1	**2,9**	
D	43	2,5	**3,8**	
E	70	4,1	**10,9**	
F	57	3,4	**0,2**	
G	39	2,3	**0,2**	
H	57	3,4	**2,5**	
I	115	6,8	**6,7**	
J	38	2,2	**2,3**	
K	42	2,5	**3,5**	
L	43	2,5	**5,7**	
M	19	1,1	**3,6**	
N	51	3,0	**5,9**	
O	35	2,1	**8,1**	
P	16	0,9	**3,1**	
Q	2	0,1	**0,0**	
R	0	-	**4,4**	
S	14	0,8	**5,6**	
T	0	-	**5,4**	
U	40	2,4	**3,6**	
V	39	2,3	**3,9**	
W	0	-	**0,1**	
X	2	0,1	**0,0**	
Y	20	1,2	**2,9**	
Z	31	1,8	**3,3**	
Počet znaků:			**1695**	

Na první pohled jsou vidět rozdíly mezi četnostmi znaků v analyzovaném textu a vzorové četnosti. (např. znak „O“ je v textu obsažen 2%, kdežto v běžné řeči až 8,1%....)
Je načase všechny hodnoty srovnat podle četnosti. (v excelu nakopírujeme na další list a srovnáme) Výsledek bude vypadat takto:

TEXT	Relativní četnost	Vzorová abeceda	Vzorová četnost
I	6,8	**E**	**10,9**
A	5,0	**A**	**9,6**
E	4,1	**O**	**8,1**
F	3,4	**I**	**6,7**
H	3,4	**N**	**5,9**
N	3,0	**L**	**5,7**
D	2,5	**S**	**5,6**
K	2,5	**T**	**5,4**
L	2,5	**R**	**4,4**
U	2,4	**V**	**3,9**
G	2,3	**D**	**3,8**
V	2,3	**M**	**3,6**
J	2,2	**U**	**3,6**
C	2,1	**K**	**3,5**
O	2,1	**Z**	**3,3**
Z	1,8	**P**	**3,1**
Y	1,2	**C**	**2,9**
M	1,1	**Y**	**2,9**
B	1,0	**H**	**2,5**
P	0,9	**J**	**2,3**
S	0,8	**B**	**1,8**
Q	0,1	**F**	**0,2**
X	0,1	**G**	**0,2**
R	-	**W**	**0,1**
T	-	**X**	**0,0**
W	-	**Q**	**0,0**

Co nám to říká? Analýza říká, že znak „I“ v zašifrovaném textu odpovídá znaku „E“ v rozšifrované podobě, A odpovídá A, E odpovídá O ……..
Nyní je třeba vyzkoušet, zda to funguje i v praxi.
Do sloupečku E (Substituce) je třeba ručně přiřadit písmena podle výsledů analýzy. Je dobré začít několika nejpoužívanějšími znaky. (Pro ukázku doplním 6 nejčastějších.) Doplněná tabulka bude vypadat následovně:

TEXT	Absolutní četnost	Relativní četnost	Vzorová četnost	Substituce
A	85	5,0	9,6	A
B	17	1,0	1,8	
C	36	2,1	2,9	
D	43	2,5	3,8	
E	70	4,1	10,9	O
F	57	3,4	0,2	I
G	39	2,3	0,2	
H	57	3,4	2,5	N
I	115	6,8	6,7	E
J	38	2,2	2,3	
K	42	2,5	3,5	
L	43	2,5	5,7	
M	19	1,1	3,6	
N	51	3,0	5,9	
O	35	2,1	8,1	
P	16	0,9	3,1	
Q	2	0,1	0,0	
R	0	-	4,4	
S	14	0,8	5,6	
T	0	-	5,4	
U	40	2,4	3,6	
V	39	2,3	3,9	
W	0	-	0,1	
X	2	0,1	0,0	
Y	20	1,2	2,9	
Z	31	1,8	3,3	
Počet znaků:			1695	

Nyní je čas zmáčknout tlačítko „Substituce !“
Další dvě políčka se nám zaplnila textem. Výsledkem je následující zpráva:

Substituce
AbcOdIg NEjAj kAl guEbmNA nA oklkOgNANl A oOlOpENungl cnEkyjl lOcnOk gdAbm okOodEnA ugE nEjoEkAjENnNl kEbl vzNAgAj zE NA nOj NAzOkNEj oklcdAlv u cAgAkNOv bdOgEcEj A jluOv cOpdIm NEbO sE dzE NA NEj AuoON oklpdIzNE vcAzAn sAcyj bdOgEcEj sE uAnvkNIN lOcnOk gdAbm ul nOnIz kOzlEdId dlll oOldE nOmO sAc uE bmOgAsI g oOdOokAzlNE cAgAkNE jAsIdl okEl uEpOv jluv cOpdIm okElunAgnE ul dvxvuNl cAgAkNv zA NElEdNImO OloOdElNE gENcv sE ckAuNy lEN A mOunv g cAgAkNE sE jAdO vz sunE uE NAuNllAdI okEbEndl sunE guEbmNy NOgINy A nEl sunE uE oOmOldNE OokEdl g jEccEj pOxv A zAjyudENE uE llgAnE NA jluv cOpdIm NvlA uE oOjAdv kOzdEzA lO guEbm cOvnv cAgAkNy A nv uE nEly jA vcAzAn lO cnEkE ucvolNy dlll oOldE nEOklE lOcnOkA gdAbmA oAnklnE sunEdl oky bdOgEcEj pEz qANnAzlE pEz nOvmy oO lyNAjlbE A pEz ujyudv

Substituce ***
A**O*I* NE*A* *A* **E**NA *A **I*O*NANl A *O*O*EN***I **E***I *O**O* **A** **O**E*A **E *E**E*A*EN*Nl *E*I **NA*A* *E NA *O* NA*O*NE* **I**A** * *A*A*NO* **O*E*E* A *I*O* *O**I* NE*O *E **E NA NE* A**ON **I**I*NE **A*A* *A*** **O*E*E* *E *A***NIN *O**O* **A** *I *O*I* *O**E*I* *I*I *O**E *O*O *A* *E **O*A*I * *O*O**A**NE *A*A*NE *A*I*I **E* *E*O* *I** *O**I* **E***A**E *I *****Nl *A*A*N* *A NE*E*Nl*O O**O*E*NE *EN** *E **A*N* *EN A *O*** * *A*A*NE *E *A*O ** ***E *E NA*Nl*A*I **E*E**I ***E **E**N* NO*IN* A *E* ***E *E *O*O**NE O**E*I * *E**E* *O** A *A****ENE *E *I*A*E NA *I** *O**I* N**A *E *O*A** *O**E*A *O **E** *O*** *A*A*N* A ** *E *E** *A **A*A* *O **E*E ****IN* *I*I *O**E *EO*IE *O**O*A **A**A *A**I*E ***E*I *** **O*E*E* *E* *AN*A*IE *E* *O*** *O **NA*I*E A *E* ****** **O ***O* ***E*E

Pokud se analýza nespletla, máme dobrý základ pro odhadnutí dalších znaků. Pokud se

analýza spletla, je dobré mezi sebou prohodit několik nejfrekventovanějších znaků, než dostaneme výsledek, který se nám bude zdát smysluplný. Horní buňka „Substituce“ kombinuje rozšifrovaná písmena (psaná Velkými písmeny) s původním textem. Druhá buňka ukazuje rozšifrovaný text + nahrazuje původní text znakem hvězdičky.
Myslím, že nyní můžeme uhodnout několik dalších znaků a slov. (druhé slovo NEjAj by mohlo být slovem NEMAM = J v zašifrované podobě odpovídá M) Slovo nEMoEkAMENnNI by mohlo být TEMPERAMENTNI = n – T, o – P, k – R,)
! Po každé změně v tabulce Substituce, je třeba znovu zmáčknout tlačítko „Substituce !“

Nyní výsledky vypadají takto:

Substituce ***
A**O*I* NEMAM RA* **E**NA TA PRIRO*NANI A PO*O*EN*T*I *TER*MI *O*TOR
A PROP*ETA **E TEMPERAMENTNI RE*I **NA*AM *E NA TOM NA*ORNEM
PRI**A** * *A*ARNO* **O*E*EM A MI*O* *O**I* NE*O *E **E NA NEM
A*PON PRI**I*NE **A*AT *A**M **O*E*EM *E *AT*RNIN *O*TOR **A** *I TOTI*
RO**E*I* *I*I PO**E TO*O *A* *E **O*A*I * PO*OPRA**NE *A*ARNE MA*I*I
PRE* *E*O* MI** *O**I* PRE**TA*TE *I *****NI *A*ARN* *A NE*E*NI*O
O*PO*E*NE *EN** *E *RA*N* *EN A *O*T* * *A*ARNE *E MA*O ** **TE *E
NA*NI*A*I PRE*ET*I **TE **E**N* NO*IN* A TE* **TE *E PO*O**NE OPRE*I *
ME**EM *O** A *AM***ENE *E *I*ATE NA MI** *O**I* N**A *E POMA**
RO**E*A *O **E** *O*T* *A*ARN* A T* *E TE** MA **A*AT *O *TERE
***PIN* *I*I PO**E TEORIE *O*TORA **A**A PATRITE **TE*I PR* **O*E*EM

Stejným způsobem pokračujeme dál, dokud nedoplníme matrici. Finální podoba substituce znaků bude následující:

TEXT	Absolutní četnost	Relativní četnost	Vzorová četnost	Substitu uce
A	85	5,0	9,6	a
B	17	1,0	1,8	c
C	36	2,1	2,9	k
D	43	2,5	3,8	l
E	70	4,1	10,9	o
F	57	3,4	0,2	i
G	39	2,3	0,2	v
H	57	3,4	2,5	n
I	115	6,8	6,7	e
J	38	2,2	2,3	m
K	42	2,5	3,5	r
L	43	2,5	5,7	d
M	19	1,1	3,6	h
N	51	3,0	5,9	t
O	35	2,1	8,1	p
P	16	0,9	3,1	b
Q	2	0,1	0,0	f
R	0	-	4,4	g
S	14	0,8	5,6	j
T	0	-	5,4	q
U	40	2,4	3,6	s
V	39	2,3	3,9	u
W	0	-	0,1	w
X	2	0,1	0,0	x
Y	20	1,2	2,9	y
Z	31	1,8	3,3	z
Počet znaků:			1695	

a výsledný text:

Substituce
ACKOLIV NEMAM RAD VSECHNA TA PRIROVNANI A PODOBENSTVI KTERYMI DOKTOR VLACH PROPLETA SVE TEMPERAMENTNI RECI UZNAVAM ZE NA TOM NAZORNEM PRIKLADU S KAVARNOU CLOVEKEM A MISOU KOBLIH NECO JE LZE NA NEM ASPON PRIBLIZNE UKAZAT JAKYM CLOVEKEM JE SATURNIN DOKTOR VLACH SI TOTIZ ROZDELIL LIDI PODLE TOHO JAK SE CHOVAJI V POLOPRAZDNE KAVARNE MAJILI PRED SEBOU MISU KOBLIH PREDSTAVTE SI LUXUSNI KAVARNU ZA NEDELNIHO ODPOLEDNE VENKU JE KRASNY DEN A HOSTU V KAVARNE JE MALO UZ JSTE SE NASNIDALI PRECETLI JSTE VSECHNY NOVINY A TED JSTE SE POHODLNE OPRELI V MEKKEM BOXU A ZAMYSLENE SE DIVATE NA MISU KOBLIH NUDA SE POMALU ROZLEZA DO VSECH KOUTU KAVARNY A TU SE TEDY MA UKAZAT DO KTERE SKUPINY LIDI PODLE TEORIE DOKTORA VLACHA PATRITE ISTELI PRY CLOVEKEM BEZ FANTAZIE BEZ

Snadné, že? ☺

c) Tipy a triky.
- Na adrese http://www.mojepixwords.cz/napoveda/ funguje vyhledávání slov podle písmen. Prázdné znaky jsou nahrazovány hvězdičkami. Stačí tedy slovo nakopírovat z buňky obsahující písmena proložená hvězdičkami. (T6)

d) Jak to celé funguje? Soubor je ve formátu Excel a používá funkce VBA. (je třeba povolit) Soubor dávám k dispozici pro další úpravy a testování.

Přeji hodně zdaru s luštěním. V případě dotazů mě kontaktujte na emailu:
pankun@centrum.cz