ŠIFROVACÍ KROUŽEK - 6. hodina

Vigenerova šifra: Je rozšířením Albertiho šifry. Používá 26 abeced, čímž činí případné dešifrování opravdu náročným.

Jak zašifrujeme text. Zvolíme si klíč, např. opět slovo HESLO (ačkoli čím delší tím lepší) a šifrujeme v řádcích postupně podle klíče s využitím tabulky níže:

```
SIFROVACIKROUZEK
HESLOHESLOHESLOH
```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Výsledek: **ZMXC CCEU TYYS MKS R**

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

Vernamova šifra: Tuto šifru si nechal patentovat v roce 1917 Gilbert Vernam a tato šifra je nerozluštitelná.

Princip spočívá v tom, že klíč je stejně dlouhý jako text, který chceme šifrovat. Každé písmeno v je v abecedě posunuté o tolik, kolik nám řekne klíč. Jako klíč je ideální vygenerovat řadu náhodných čísel.

Např: 5,24,21,23,11,5,25,16,25,23,19,16,17,3,6,25

K nim přidělíme písmena abecedy: EXUWKEYPYWSPQCFY

Postupovat pak můžeme stejně jako u Vigenerovy sifry:

Výsledek pak bude: **WFZN YZYR GGJD KBJI**

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.

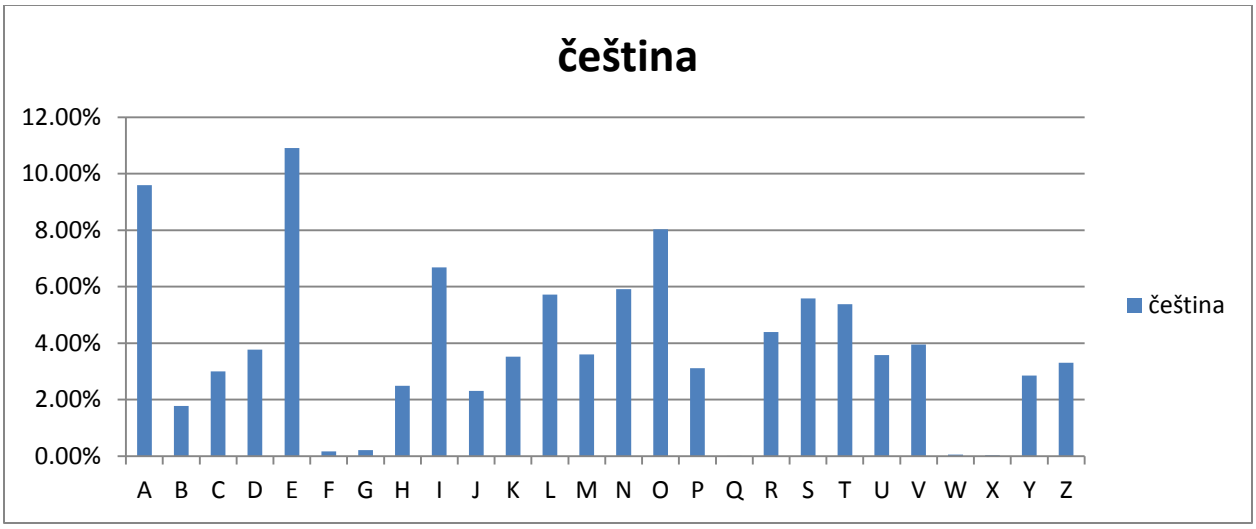
Např. zde:
http://rumkin.com/tools/cipher/frequency.php

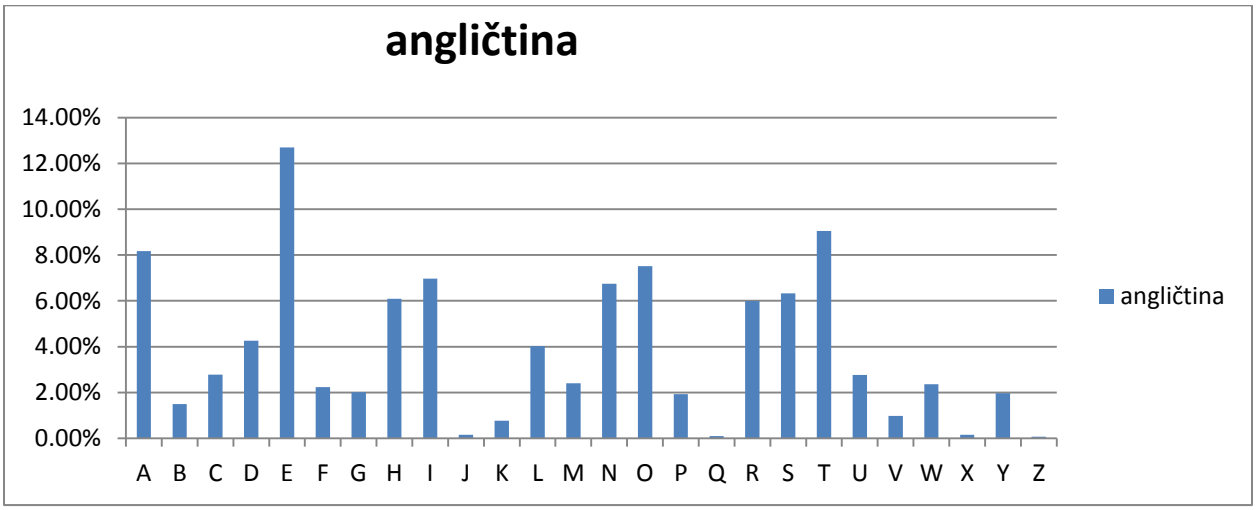
nebo zde:
http://www.musilek.eu/michal/sifry-frekvence.html?menu=cc&item=t&lang=cz

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!





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