INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Doplňující materiály ke kryptologii – obrázky

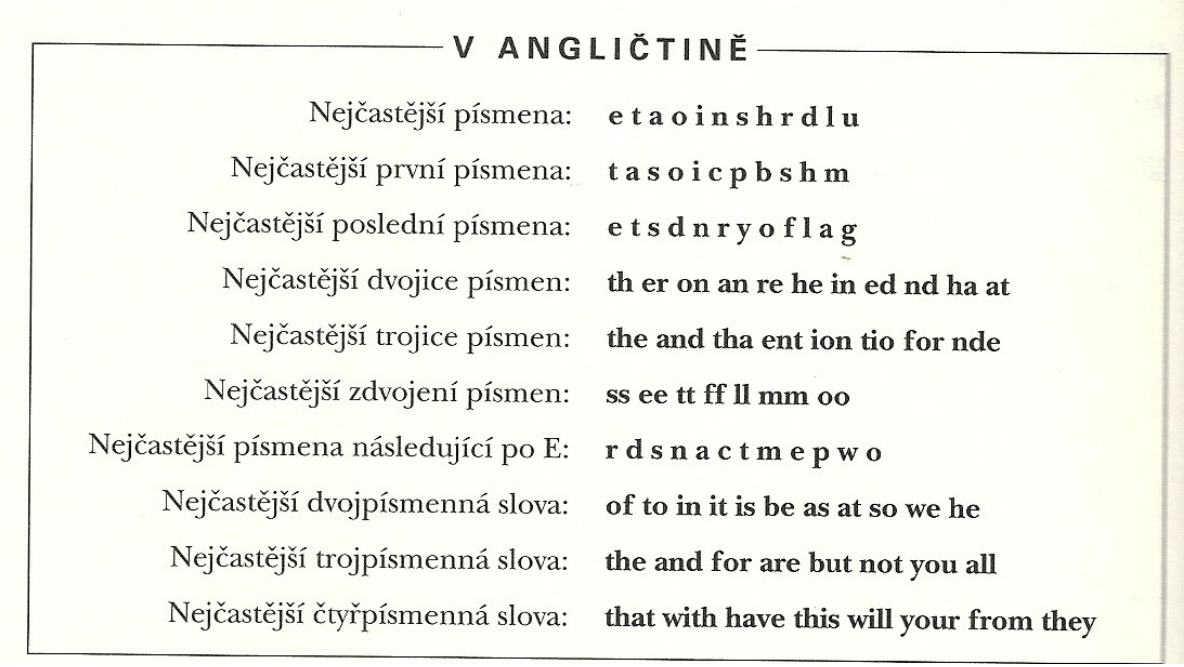
Césarova šifra[1]

Otevřený text	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
Šifrovaný text	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

Tabulka 2.1: Césarova šifra

[1] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. 190 s. ISBN 8025101061. s. 35

Základy frekvenční analýzy[2]

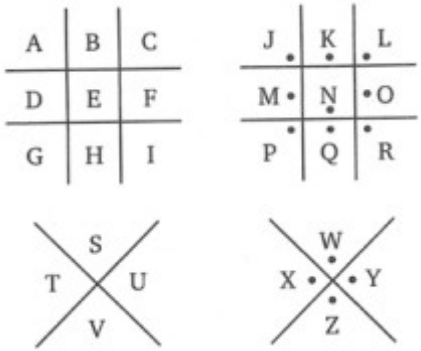


V ANGLIČTINĚ

Nejčastější písmena:	**e t a o i n s h r d l u**
Nejčastější první písmena:	**t a s o i c p b s h m**
Nejčastější poslední písmena:	**e t s d n r y o f l a g**
Nejčastější dvojice písmen:	**th er on an re he in ed nd ha at**
Nejčastější trojice písmen:	**the and tha ent ion tio for nde**
Nejčastější zdvojení písmen:	**ss ee tt ff ll mm oo**
Nejčastější písmena následující po E:	**r d s n a c t m e p w o**
Nejčastější dvojpísmenná slova:	**of to in it is be as at so we he**
Nejčastější trojpísmenná slova:	**the and for are but not you all**
Nejčastější čtyřpísmenná slova:	**that with have this will your from they**

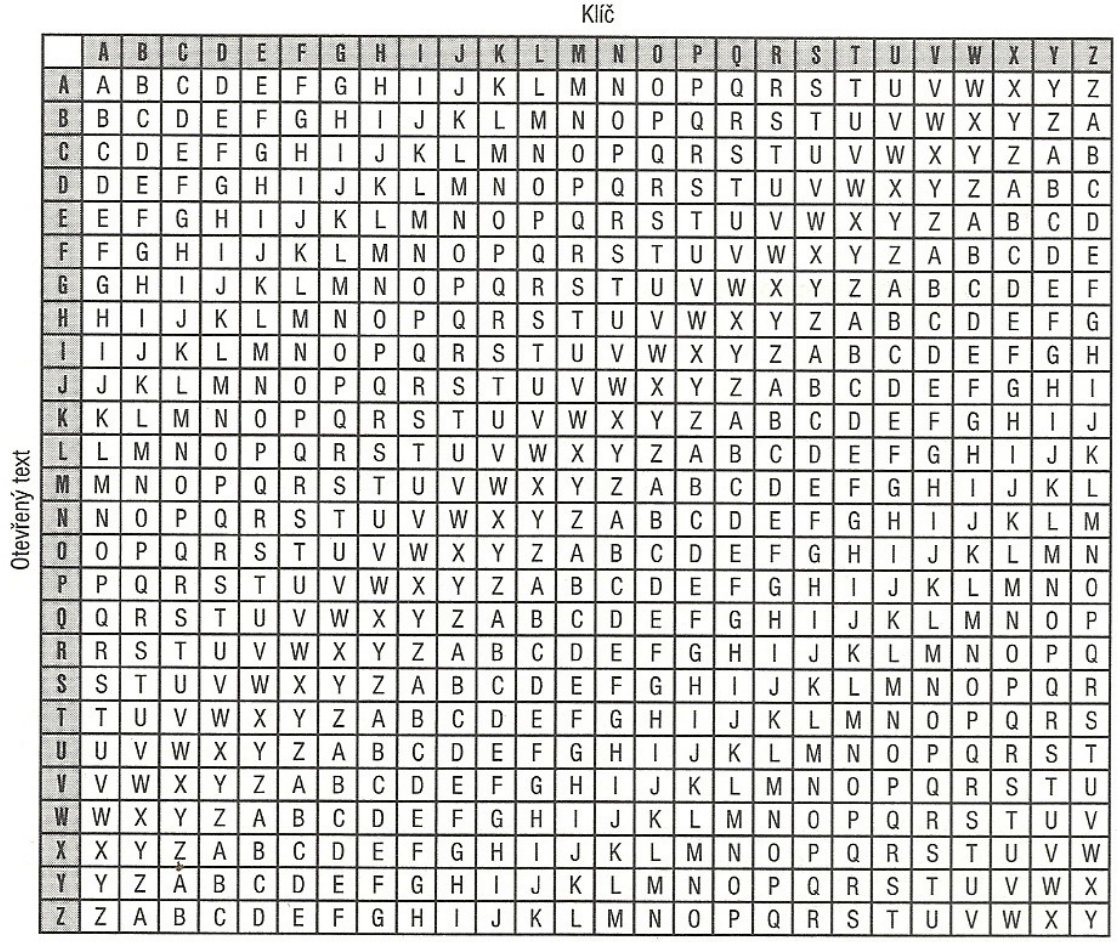
[2] BERLOQUIN, Pierre. *Skryté kódy a velkolepé projekty: Tajné jazyky od starověku po současnost*. Vydání první. Praha: Universum, 2011. 375 s. ISBN 978-80-242-2847-1. s. 158

Šifra prasečích chlívků[3]



[3] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii.* Simon Singh; přeložili Petr Koubský a Dita Eckhardtová. 1. vyd. V českém jazyce. Praha: Dokořán, 2003. 382 s, il., portréty, faksim. (Aliter ; sv. 9) ISBN 8086569187 (Dokořán). ISBN 8072034995 (Argo). s. 350

Vigenèrova šifra[4]



Otevřený text \ Klíč	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

Tabulka 2.2: Vigenerova šifra

[4] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. 190 s. ISBN 8025101061. s. 37

Albertiho kotouč (ulehčení Vigenèrovy šifry)[5]

[5] *Security-Portal.cz* [online]. 2 Prosinec, 2004 [cit. 2011-04-28]. Praktické základy Kryptologie a Steganografie. Dostupné z: http://www.security-portal.cz/clanky/praktick%C3%A9-z%C3%A1klady-kryptologie-steganografie