

Ukázka z kapitoly 3. Šifry, které nikdy skutečnými šiframi nebyly

Jednoduchá záměna č. 1 (knihy)

K laickému šifrování otevřeného textu pomocí jednoduché záměny je oblíbené použití některých převodových tabulek mezi šifrovou abecedou a znaky otevřeného textu, které byly publikovány v různých knihách. Typickým příkladem může být převodová tabulka z knihy Arthura Conana Doylea - *Návrat Sherlocka Holmese*, konkrétně z povídky *Příběh tančících figurín* (The Adventure of the Dancing Men) nebo znaková převodová tabulka z povídky E. A. Poea - *Zlatý brouk*. K šifrování se využívají buď přímo tabulky uvedené v textu nebo jejich mírně pozměněné podoby, a to často jen z důvodu, aby použité symboly šly lépe kreslit.

Šifrová abeceda v knize A. C. Doylea, se skládá ze stylizovaných postaviček v různých „tanečních“ pozicích a k zápisu otevřeného textu je potřeba použít mezinárodní abecedu.

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

Převodová tabulka z příběhu A. C. Doylea - *Příběh tančících figurín*

Otevřený text: Kdo jinému jámu kopá, sám do ní padá.

Zápis v mezinárodní abecedě: KDO JINEMU JAMU KOPA SAM DO NI PADA

Šifrový text:

V povídce *Zlatý brouk* E. A. Poea je šifrová abeceda tvořena čísly a různými znaky. Povídka je zajímavá i z hlediska teorie, neboť autor velmi detailně popsal, jak lze jednoduchou záměnu luštit na základě porovnání frekvence šifrových a otevřených znaků.

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
5	2	-	♦	8	1	3	4	6	!	7	0	9	*	↗	.	/	()	;	?	¶] <	:	>	

Převodová tabulka z příběhu E. A. Poea - *Zlatý brouk*

(šifrová abeceda je doplněna o znaky !/⟨⟩, neboť v povídce se v otevřeném textu šifrové znaky pro písmena J, K, Q, X, Z nevyskytují, a proto by nebylo možné původní tabulku úplně rekonstruovat)

Otevřený text: Kdo jinému jámu kopá, sám do ní padá.
Zápis v mezinárodní abecedě: KDO JINEMU JAMU KOPA SAM DO NI PADA
Šifrový text: 7♦x̂ !6*89? !59? 7x̂.5)59 ♦x̂ *6 .5♦5

Šifrový text z povídky E. A. Poea, který obsahuje návod k nalezení pokladu

53x̂x̂♦305))6* ;4826)4x̂.)4x̂) ;806* ;48♦8¶60))85 ;
)]8* :x̂*8 ♦83(88)5*♦ ;46(;88* 96*? ;8) *x̂(;485) ;5*♦2
*x̂(;4956*2(5-4)8¶8* ;4069285) ;)6♦8)4x̂x̂ ;1(x̂9 ;48
081 ;8 :8x̂1 ;48♦85 ;4)485♦528806*81(x̂9 ;48 ;(88
 ;4(x̂?34 ;48)4x̂ ;161 ;:188 ;x̂? ;