

# Šifry, šifrování

Šifrované zprávy používají lidé už od té doby, co se naučili psát. Vždy se totiž našel někdo, kdo chtěl sdělit něco tajného tak, aby tomu nikdo nepovolný nerozuměl. Tajné špionážní organizace by bez šifrovaných zpráv snad ani nemohly existovat. To ony vymyslely mraky šifer a některé z nich používáme i my v oddílech. (Pokud chceš naučit šifry skupinku neposedných kluků, možná i holek, připrav si nějakou zajímavou historku o tom, jak se za války posílaly šifrované zprávy a uvidíš, že je bude zajímat zase o trošku víc než předtím.)

Šifry můžeme rozdělit do skupin podle různých kritérií, toto je jen jedno z mnoha:

## 1. Všechna písmenka patří do zašifrované zprávy:

a) se špatnými mezerami: VEN KUSVÍ TÍSLU NÍČKO

b) po zpátku: OKČÍNULSÍTÍVSUKNEV

c) po řádcích v různých směrech:

V	E	N	K	→	V	E	N	K	→
U	S	V	Í	→	Í	V	S	U	→
T	Í	S	L	→	T	Í	S	L	→
U	N	Í	Č	→	Č	Í	N	U	→
K	O	!	!	→	K	O	!	!	→



d) po sloupcích v různých směrech:

V	S	S	Č	↓	V	Í	S	!	↓
E	V	L	K	↓	E	T	L	!	↓
N	Í	U	O	↓	N	Í	U	O	↓
K	T	N	!	↓	K	V	N	K	↓
U	Í	Í	!	↓	U	S	Í	Č	↓

e) šneci:

K	Č	Í	N	U
O	U	K	N	L
!	S	V	E	S
!	V	Í	T	Í



V	U	T	U	E	1.	5.	9.	13.	2.
L	Í	!	Č	S	12.	15.	19.	16.	6.
Í	O	!	K	Í	8.	18.	20.	17.	10.
K	N	S	V	N	4.	14.	11.	7.	3.

## 2. Ne všechna písmenka patří do zašifrované zprávy:

a) každé druhé (třetí, čtvrté,...) písmenko:

VŠENUKLBSVNÍZTSÍASPLOVNLÍMČIKYO

b) pouze 1. písmenko (poslední) slova:

sen, luk, ucho, nůž, Írán, čočka, kůň, oko

c) první a poslední písmenko z každého slova:

sůl, uran, íč, kolo

d) 1. písmenko prvního slova, 2. písmenko druhého slova,... :

slon, ploutev, moucha, pláň, psaníčko, travič, klubíčko, přáníčko

e) čteme každý druhý sloupec:

P	S	P	N	L	K	↓
O	L	E	Í	E	O	↓
T	U	S	Č	N	!	↓

f) vybíráme písmenko jednoho druhu: SLonice Uši Nůš v ČoKOLádě!

### 3. Písmena v zašifrované zprávě jsou nahrazena jinými písmeny nebo čísly:

Abeceda:

A-1(24), B-2(23), C-3(22), D-4(21), E-5(20), F-6(19), G-7(18), H-8(17), I-9(16),  
J-10(15), K-11(14), L-12(13), M-13(12), N-14(11), O-15(10), P-16(9), R-17(8),  
S-18(7), T-19(6), U-20(5), V-21(4), X-22(3), Y-23(2), Z-24(1)

a) písmenka jsou nahrazena číslicemi (od začátku nebo od konce abecedy):  
18+12-20/14+9-3+11-15?

b) písmenka jsou nahrazeny jinými písmenky podle klíče: AZ, BY, CX,... ...ZA  
Gmekpxnj

c) „posun“ se říká šifře, ve které posouváme v abecedě písmenka o určitý počet nahoru či dolů. Počet můžeme pak zobrazit například v datumu.

6.7.1415

ZTVSJHRX (Sluníčko)

d) písmenka jsou nahrazena zlomky podle libovolné tabulky:

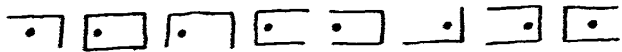
	T	Ř	I	N	E	C
1	A	B	C	D	E	F
5	G	H	I	J	K	L
6	M	N	O	P	R	S
0	T	U	V	X	Y	Z

C/6; C/5; Ř/0; Ř/6; I/5; E/5; I/6

### 4. Písmenka v zašifrované zprávě jsou nahrazena znaky:

a) šifrovací kříže

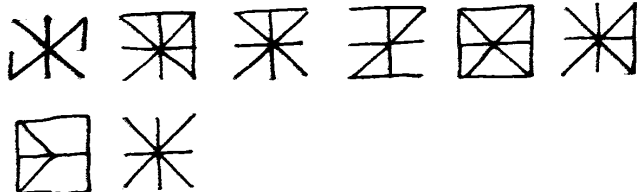
ABC	DE	FGH
IJK	LM	NOP
RST	UV	XYZ



b) hvězdice

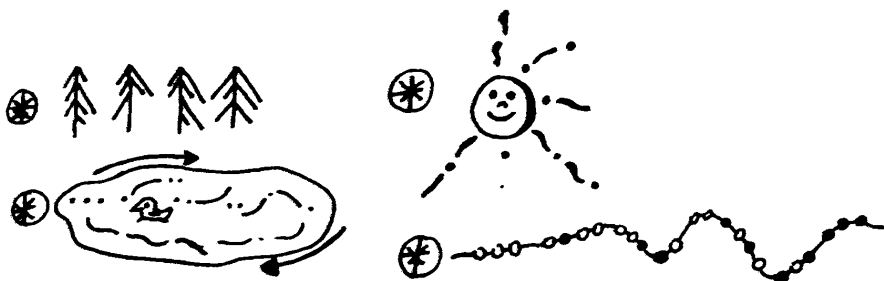


Základní tvar



## c) MORSEOVA ABECEDA

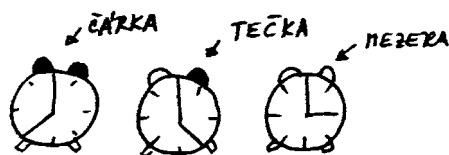
Morseovu abecedu určitě všichni znáte. Její použití je různé, můžete jí písat, vysílat baterkou, rukama nebo jednoduše napsat. S trochou fantazie se čárky a tečky mohou stát vlnkami či stromečky. Zprávu můžeme zašifrovat taky do korálků navlečených do nití, uzlíků nebo hřebíčku.



## d) SEMAFOR

Už samotné použití semaforu je dosti obtížné a tak vymýšlet na něj finty je ještě obtížnější. Přece jen jich ale několik existuje:

„Budíky“ – semafor zapisujeme do hodin pomocí hodinových ručiček. (Dost dobrý je zašifrovat semaforem klamnou zprávu a tu správnou zašifrovat morseovkou do „čudlíků“ - viz obrázek.)



„Hvězdice“ aneb tajemná šifra ze Skautskou stezkou – písmena semaforu odhalíme odčítáním písmenek - viz obrázek.



---

Tyto šifry jsou náhodně vybrané, existuje mnoho jiných a mnohé ještě čekají na to než je někdo vymyslí.

## **Jak na šifry?**

*Pokud chcete své svěřence naučit šifrovat nezbyvá vám, než jim pořád dokolečka dávat luštit šifry, aby si to zažili. Záleží ale jen na vás, jak jim to zpestříte, jestli je necháte nejdříve šifru někde venku najít, nebo jim jí nejdřív rozstříháte, nebo si budou šifry vymýšlet navzájem, závodit kdo vyluští víc šifer, nebo jim je budete dávat jako bodovačky...*

## **Jak na morseovku a semafor?**

*Obecně platí to samé co u šifer, dokud si znaky nezažijí (což u některých trvá i větší než velké množství času), rozhodně nemáte vyhráno. U morseovky a u semaforu je ta výhoda, že jsou to samostatné znaky. Můžete z nich vyrobit pexeso, domino či jen kartičky se znaky, které rozházíte po stole, klubovně, lese,... a úkolem vašich svěřenců je je najít a poskládat z nich co nejvíce slov, co nejdelší slovo,... Zatím co kluci budou asi raději běhat po lese a hledat kartičky, holky zas může bavit vymýšlet různé originální obrázkové variace na morseovku (tečky a čárky jako vlnky v rybníce, paprsky od slunička, stromečky, kytičky... fantazii se meze nekladou).*