

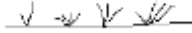
Základní šifry

• Morseova abeceda – včetně pomocných slov

.-	A	akát	-.	N	nástup
-...	B	blýskavice	---	O	ó náš pán
-..	C	cílovníci	.--.	P	papírníci
-..	D	dálava	--.-	Q	kvílí orkán
.	E	erb	.-.	R	rarášek
.-.	F	Filipíny	...	S	sobota
--.	G	Grónská zem	-	T	trám
....	H	hrachovina	..-	U	uličník
----	CH	chvátá k nám sám	...-	V	vyučení
..	I	ibis	.-.	W	vagón klád
.---	J	jasmín bílý	-..-	X	Xénokratés
-.-	K	krákorá	-.--	Y	Ýgar mává
.-..	L	lupíneček	--..	Z	známá žena
--	M	mává			

Šifrování pomocí morseovky může mít řadu podob:

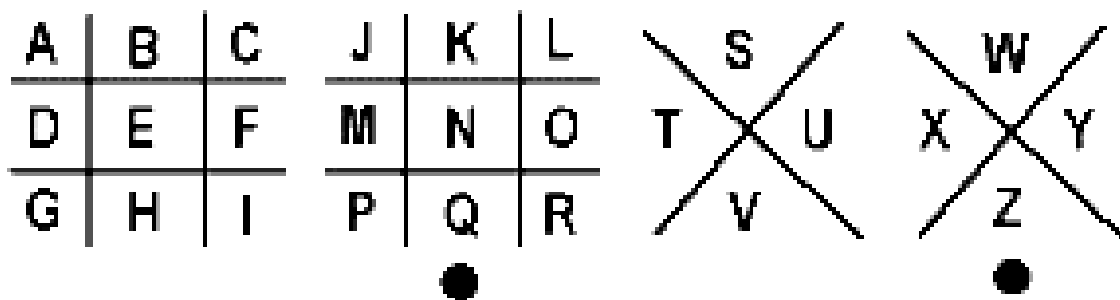
- normální morseovka
- obrácená morseovka (čárky jsou nahrazeny tečkami a opačně)
- číselná morseovka (sudé číslice – čárka, liché číslice – tečka)
- grafická morseovka

▪ „tráva“ 

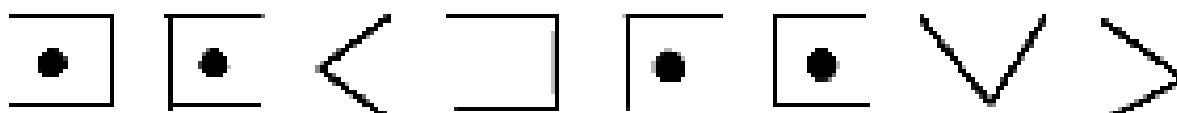
▪ „pila“ 

▪ „stromy“  - a to zatím stačí

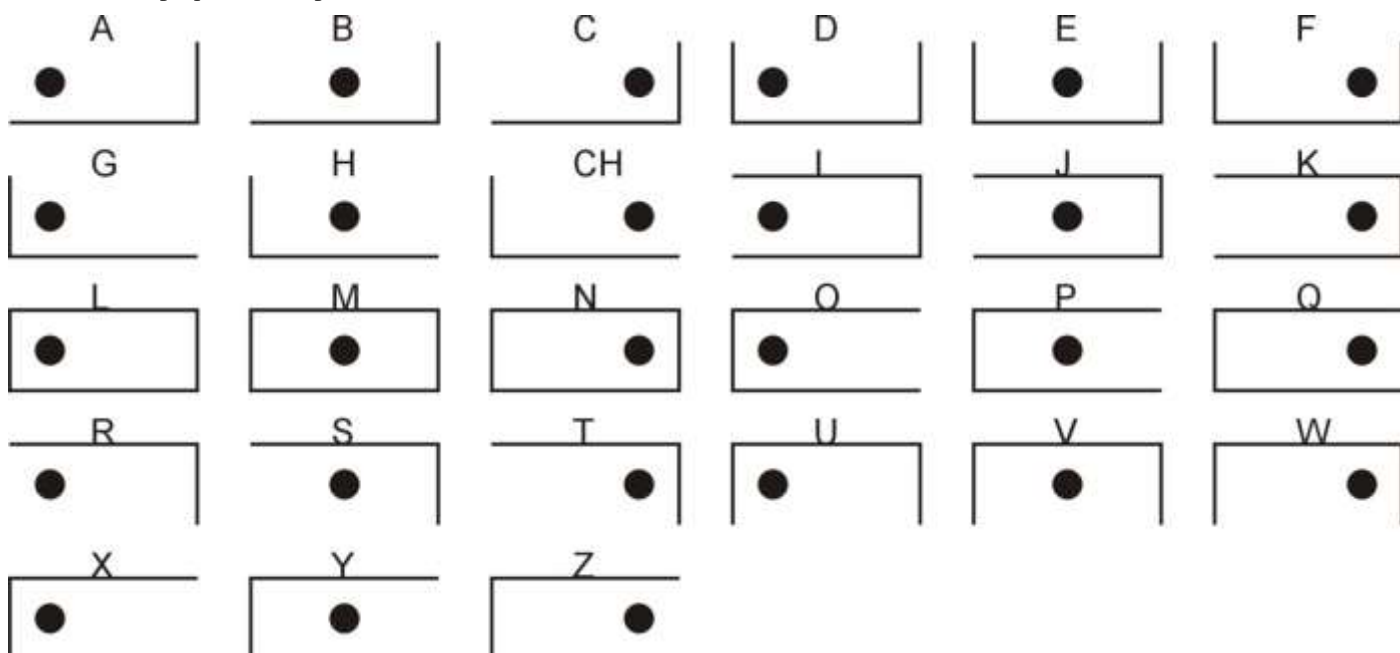
• Malý polský kříž



Takhle vypadá třeba slovo „moudrost“



• Velký polský kříž



Tohle je slovo „cyklista“



• Další jednoduché šifry

○ Mezi písmeny slovo

Mezi každá dvě písmena zprávy napíšeme nějaké krátké slovo:

ADUBHDUBODUBJDUBVDUBODUBDDUBNDUBIDUBKDUBU

○ Po určitém písmeni

V textu jsou písmena ze zprávy jen po určitém písmeni. Například po písmenu X:

BNXAMNBXHGZIXOKXJNMMNXVXOGHGXDMXNWEXIXKMNXU

○ První zepředu, druhé zezadu:

Písmena se čtou střídavě z obou konců zprávy. První písmeno je první, druhé je poslední, třetí je druhé, čtvrté předposlední a tak až doprostřed:

AOVDOUAZJSEIKJKNOJH

○ Velká písmena

Ve zprávě platí jen velká písmena:

Dvě Oči Při ceStě = DOPIS

• Šifry se záměnou nebo posouváním písmen, číselná abeceda

Pro všechny tyto šifry se většinou používá abeceda s 26 písmeny (bez háček, čárek a kroužku a bez písmene CH).

○ Šifry se záměnou písmen

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
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

Do první řádky se napíše celá abeceda a do druhé se napíše abeceda posunutá. Pod písmeno A se napíše to písmeno, o které je abeceda posunuta (např. A=F znamená, že A v šifře se rovná F ve skutečnosti). Při šifrování se hledá ve spodní řádce a do šifry se píše to z horní řádky a při luštění se v horní řádce hledá písmeno v šifře a v dolní je písmeno ze zprávy.

Tak třeba pro A=F zašifrované slovo VCJE je AHOJ.

○ **Šifry s posouváním písmen**

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Číslo před šipkou určuje, o kolik míst jsou písmena v abecedě posunuta směrem doprava. Šifruje se proti směru šipky, abychom zprávu mohli ve směru šipky luštit.

Třeba pro 7→ zašifrované slovo **GTSWTK** je NAZDAR.

○ **Číselná abeceda – místo písmen čísla**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

Jedna z nejjednodušších šifer. Místo písmen se do zprávy napíše čísla A=1 B=2... Jednotlivá čísla se oddělují středníkem nebo vodorovnou čárkou. Jiná možnost je čísla psát římskými čísly.

AHOJ VODNÍKU = 1;8;15;10 22;15;4;14;9;11;21