



How to šifry - Základný prehľad

Šifry z videa

1. Šifra

WRWR MH FHCDURYD VLIUD

Postup riešenia: Ide o posun v abecede o tri písmená. Každému písmenku zodpovedá písmenko, ktoré je o tri miesta skôr v abecede. Takýto posun vidíme v nasledujúcej tabuľke:

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
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

Riešením je **TOTO JE CÉZAROVA ŠIFRA**.

2. Šifra

Hurá, ideme, výborne.

Máš prvé písmeno?

Mám.

Ďalšie písmeno vieš?

Stále hľadám.

Fajne.

Ej, chýba mi niečo.

Gratulujem.

Mám asi celé hesielko.

Postup riešenia: Dĺžne a bodky nad písmenami dávajú po riadkoch morseovku. Dostávame:

- - -

- - -

-

- - -

- -

-

- - - .

-

- - - -

Riešením je **KOTRMELEC**.



Zadania šifier

1. Posun

GXTHTCXT BPBT PCIXADEP

2. Pokémoni



3. Neposun

KMTOTAMI ETBES OMQKL BT BNUGNK



Všeobecné rady pri riešení šifier

- Žiaden nápad nie je zlý. Na vyriešenie šifry vyskúšaj **všetko čo ti napadne**.
- Všímaj si **detaAILY**. Všímaj si, čo je spoločné a čo je naopak špecifické pre jednotlivé časti šifry. Skús sa zamyslieť či ti šifra niečo nepripomína.
- Občas na vyriešenie využívame špeciálne kódovania zo šifrovacích pomôcok – Morseovku, Braillovu abecedu, semafór, vlajky a iné. Najčastejšie používané šifrovacie pomôcky nájdeš tu: <https://chlyftym.cz/pomucky/>.
- Ak je niečoho 26, tak to asi nebude náhoda. V šifrách bežne využívame anglickú **abecedu s 26 písmenami**. Vďaka tomu vieme potom jednoducho prepísať čísla na písmená a to tak, že A=1, B=2, C=3, D=4, ...
- Neboj sa **skúsiť tú istú myšlienku aj viackrát**, respektíve overiť či si sa niekde nepomýlil. Vďaka malej chybke ti môže celá šifra vychádzať zle, preto je potrebné sa im vyvarovať.
- Ak ti ako riešenie vychádza CKWGO, tak to nie je správne.
- Bežne platí, že ak nie je pri šifre uvedené inak, riešenie je **podstatné meno v nominatíve singuláru**. V tomto prípade to platí.



Nápovedy k šifrám

1. Posun

Zisti, ktoré písmenko tam je najčastejšie a skús ho nahradíť častým písmenkom v normálnych slovách.

2. Pokémoni

Niekterí pokémoni sú guľatí, niektorí sú podlhovastí a niektorí nie sú ani takí ani takí.

3. Neposun

Každé písmeno je nahradené iným písmenkom. Skús ich zopár objaviť. Možno tam nájdeš skrytú morseovku, to ti však teoreticky ani netreba.



Riešenia šifier

1. Posun

Najdeme najčastejšie písmená. Písmeno **T** tam je 4-krát a písmeno **X** 3-krát. Skúsime ho nahradíť nejakým častým písmenkom – niektorou samohláskou. Prípadne môžeme skúsiť nahradíť dvojice za sebou idúcich písmen. Odskúšame a zistíme, že nasledovný posun je správny:

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
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

Dostávame **RIEŠENIE MÁME ANTILOPA**.

2. Pokémoni

Po poriadnom zadívaní sa na pokémonov ich vieme rozdeliť do troch skupín – guľatí, podlhovastí a takí, ktorí nie sú ani guľatí ani podlhovastí. Tiež si môžeme všimnúť, že sú najviac 4 pokémoni z prvých dvoch skupín za sebou. To indikuje morseovku, v ktorej tretia skupina pokémonov sú oddelovače.

Prirodzene skúsime najprv to, aby guľatí pokémoni boli bodky a podlhovastí pokémoni boli čiarky. Po prepísaní do morseovky máme: **- · - / - - - / · · / · - - / - - / - - / - - -**, kde / značí oddelovač písmen. Riešením je **POSLANEC**.

3. Neposun

Aj názov šifry hovorí, že v tejto šifre nejde o posun abecedy. V zadaní sú však natoľko divoké písmená, že nadobudneme dojem, že ich treba transponovať. Transpozícia je nahradenie každého písmenka z pravidla iným písmenkom. Môžeme skúsiť odhadnúť najkratšie slovo. Najkratšie slovo je BT a pomerne časté dvojpísmenové slová v bežnom jazyku sú na, ty a je. Vyskúšame ich a následne si skúsime domyslieť ďalšie písmená v ostatných slovách. Je možné, že sa nám týmto postupom podarí vyriešiť celá šifra.

Každopádne slovo BT je JE. Potom môžeme ísť na druhé slovo šifry, pretože už poznáme 2 písmená z piatich. Už určené písmená budeme značiť tučným písmom. Máme teda **EEJES** a chceme nahradíť E a S. Pri hľadaní slova, ktoré obsahuje **EJ** asi pomerne rýchlo najdeme slovo **TEJTO**. Má aj dve T a to na miestach E. Takže už sme našli prevod medzi písmenami B → J, T → E, E → T a S → O.

Takýmto postupom môžeme všetky slová odšifrovať, ale vieme si to istým pozorovaním výrazne uľahčiť. Môžeme si všimnúť, že E sa mení na T a T sa mení na E. S poznaním ďalších písmen môžeme overiť, že dvojice písmen sa navzájom na seba transponujú.

Ten, kto veľmi dobre pozná morseovku tiež vie, že E je · a T je -. Tiež možno vie, že S je ··· a O je - - -. To naznačuje, že keď písmená zo zadania šifry prepíšeme do morseovky a následne vymeníme bodky s čiarkami, tak dostaneme riešenie. Prepíšeme zadanie do morseovky, pričom / budeme značiť oddelovače písmen a každé slovo bude v novom riadku.

- · - / - - / - / - - - / - / · - / - - / · ·
· / - / - · · / · / · ·
- - - / - - / - - - / - - - / · - -
- · · / -
- · · / - - / · - - / - - - / - - - / - - -

Po zámene bodiek a čiarok dostávame:

- - · / · · / · / · · / · / - · / · · / - -
- / · / - - - - / - / - - -
· · · / · · / · - - - / - - - / - - -
- - - - / ·
- - - - / - - - / - - - / · - - / · - -

Po prevedení dostávame **RIEŠENÍM TEJTO ŠIFRY JE JAGUÁR**.