

# Zóna 2

## Základné šifrovacie postupy

Vitajte v druhej zóne, ktorá vás naučí niekoľko základných spôsobov, ktoré sa bežne používajú pri lúštení šifier. Sú založené na reálne používaných spôsoboch komunikácie (nemusia sa nevyhnutne jednať o metódu šifrovania), z ktorých mnohé sú v špecifických prípadoch používané dodnes.

Prvým podstatným prvkom pri šifrovaní je samotná abeceda. Za štandardných okolností používame 26 písmenovú abecedu (písmená bez mäkčeňov, dĺžňov a podobných záležitostí), pričom „CH“, „DZ“, „DŽ“ a ďalšie príbuzné vecičky považujeme za sériu dvoch samostatných znakov. V špeciálnych prípadoch toto pravidlo nemusí platiť, ale štandard je takýto. A teraz už hor sa na dešifrovacie postupy!

Prvým veľmi často používaným šifrovacím (a dešifrovacím) postupom je vzájomné premieňanie čísiel na písmená a naopak. Princíp tohto premieňania je veľmi jednoduchý – jednotlivým písmenám bežnej 26 písmenovej abecedy priradíme čísla od 1 do 26. Ak potom pri lúštení šifry narazíme na sériu čísiel 22, 12, 1, 11, ľahko tieto čísla premeníme na heslo VLAK. Naopak, v špecifických prípadoch sa môže hodiť premieňať písmená na čísla a tieto čísla ďalej využiť. Z uvedeného tiež vyplýva, že čísla je možné pomerne jednoducho sčítavať a odčítavať ( $F + N = T$ ), rovnako je možné k celému heslu pričítať nejaké písmeno, čím sa pôvodne zrozumiteľné slovo zmení na blábol ( $VLAK + 1 = WMBL$ ). Aby ste sa s premenou písmen na čísla ľahšie vysporiadali, sú súčasťou tohto dokumentu aj malé šifrovacie pomôcky, ktoré môžete v prípade potreby využiť na rýchle priradenie čísiel k písmenám a naopak.

**Príklad: VLAK = 22, 12, 1, 11**

Ďalším často používaným kódovacím postupom je morzeovka. Tá využíva iba dva základné znaky – bodky a čiarky, kombináciou ktorých je možné vytvoriť všetky písmená. Zároveň platí, že jednotlivé písmená je potrebné nejakým spôsobom oddeliť (na to sa používa tretí znak). Ak sa vám teda pri lúštení stane, že narazíte na priestor obsadený tromi typmi objektov/znakov/písmen/niečoho, zbystrite rýchlo pozornosť a skontrolujte, či sa náhodou nejedná o morzeovku. Preklad jednotlivých písmen do morzeovky je tiež súčasťou priložených šifrovacích pomôcok.

**Príklad: VLAK = ...- / .-.. / .- /-.-**

Braillovo písmo sa bežne využíva na zapisovanie informácií pre nevidiacich. Každé písmeno je kódované šesticou bodiek, z ktorých každá môže byť vypuklá alebo nevypuklá a trénovaný čitateľ následne dokáže tento zápis čítať pomocou hmatu. V šifrách môžu byť dva stavy bodky vyjadrené rôznymi spôsobmi (napr. čierna/biela), ale pokiaľ pri lúštení narazíte na podozrivé šesticu objektov, zamyslite sa, či náhodou nebolo použité Braillovo písmo. Ako ste asi uhádli, Braillova abeceda je tiež uvedená v šifrovacích pomôckach.

**Príklad: VLAK =**



Semaforová abeceda vznikla pôvodne ako dorozumievací prostriedok v námorníctve, dnes je však už málo využívaná, snáď s výnimkou šifier. Podstatou tejto abecedy je, že s použitím dvoch vlajočiek (pozor, nemýliť si s vlajkovou abecedou) ukazujúcich do dvoch rôznych smerov, je možné vytvoriť rôzne kombinácie, z ktorých každá reprezentuje jedno písmeno abecedy. Zjednodušenú verziu semaforovej abecedy nájdete, samozrejme, v šifrovacích pomôckach.



Dobre známou alternatívou ku klasickým arabským čísliciam, ktoré bežne používame, sú tzv. Rímske čísla. Tieto čísla využívajú menej znakov (I = 1, V = 5, X = 10, L = 50, C = 100, D = 500, M = 1000), ktoré sú navyše zameniteľné s niektorými písmenami abecedy. Vďaka tejto vlastnosti sa s nimi dá pracovať aj iným spôsobom ako so štandardnými číslicami (napr. môžu byť ukryté v texte). Nebojte sa, v šifrovacích pomôckach sme nezabudli ani na ne.















































































**Príklad: VLAK = XXII, XII, I, XI**

Posledným základným šifrovacím postupom je tzv. vlajková abeceda, ktorá bola (podobne ako v prípade semaforovej abecedy) pôvodne používaná na komunikáciu medzi plavidlami, dnes sa s ňou však stretnete len vzácné. Abecedu tvoria rôzne typy vlajočiek, ktoré zodpovedajú jednotlivým písmenám abecedy. Ak si ich chete pozrieť, mrknite sa do šifrovacích pomôcok.



Tu sú šifrovacie pomôcky:

(môžete si ich vytlačiť, zalaminovať a zaradiť do šifrovačkovej výstroje)

1	A	--				I
2	B	---•				II
3	C	---•				III
4	D	--••				IV
5	E	•				V
6	F	••••				VI
7	G	---•				VII
8	H	••••				VIII
9	I	••				IX
10	J	•---				X
11	K	---•				XI
12	L	••••				XII
13	M	--				XIII
14	N	--•				XIV
15	O	---				XV
16	P	••••				XVI
17	Q	••••				XVII
18	R	•••				XVIII
19	S	•••				XIX
20	T	-				XX
21	U	••-				XXI
22	V	•••-				XXII
23	W	••-				XXIII
24	X	•••-				XXIV
25	Y	••••				XXV
26	Z	••••				XXVI

# Zóna 2

## Šifra 1 – Návšteva

Keď som naposledy išiel na návštevu k tete, práve v ten deň som prišiel vlakom do Bratislavy. Na Hlavnej stanici som nasadol na električku číslo 2 a smelo sa pustil vpred. V centre mesta som si spomenul, že by som ešte mohol rýchlo zaskočiť do Petržalky, kde ma na pošte čakal balík. Prestúpil som teda na jednotku a previezol sa zrekonštruovaným električkovým mostom. Balík som vyzdvihol a po ceste naspäť som nastúpil na trojku, ktorá ma odviezla až do Rače, kde býva teta. Návšteva bola príjemná, poklebetili sme, no nemohol som sa príliš zdržiavať. Ešte sa ani nezotmelo, keď som sedel v deviatke smerom do Karlovej Vsi. Dúfal som, že stihnem skočiť do obchodu a kúpiť si niečo na večeru, no električka sa pokazila na polceste. Celý mrzutý som vystúpil a počkal na dvanástku, ktorá ma konečne odviezla domov.

# Zóna 2

## Šifra 2 – Rodokmene

Denisa ○ Emil



Ivana



?

Andrej ○ Filoména



Gregor

Gabriela ○ Cyprián



Jozef



?

Barbora

Filip ○ Irena



?

Karolína ○ Boris



Milada



?

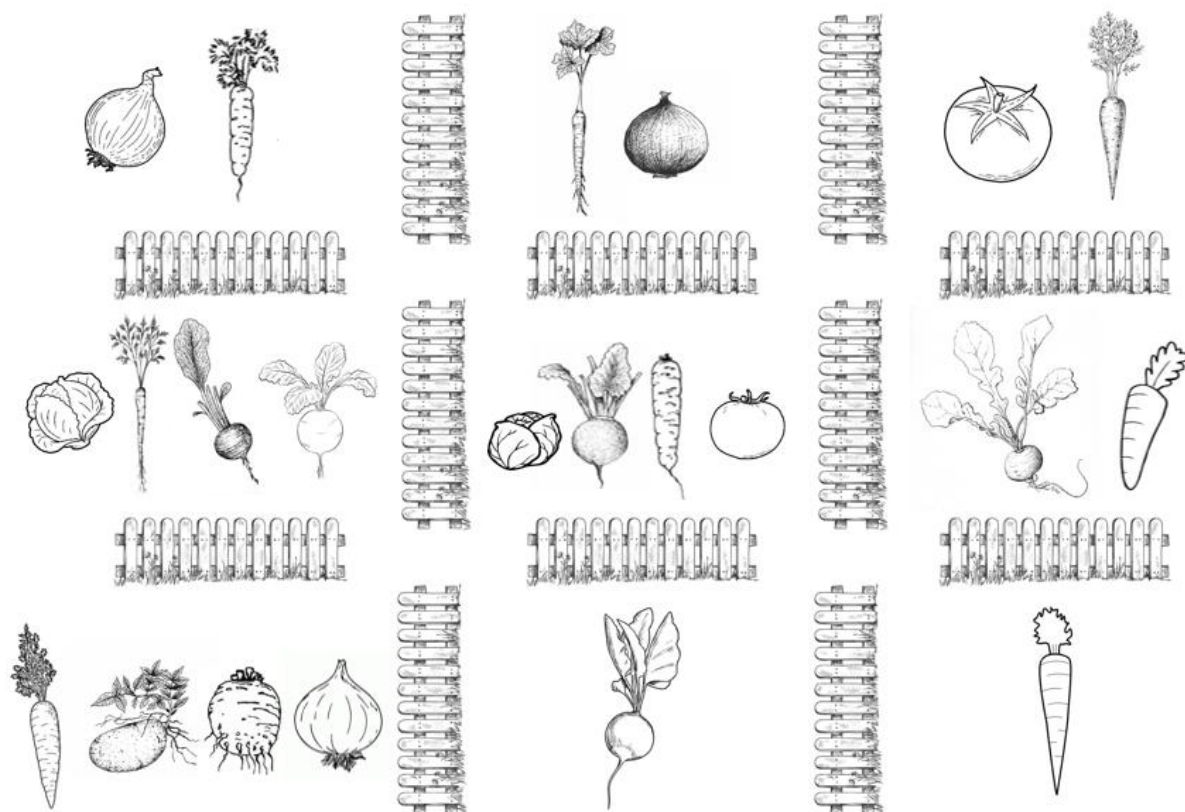
Drahomír ○ Cecília



Gustáv

# Zóna 2

## Šifra 3 – Záhradky



# Zóna 2

## Šifra 4 – Rovnice a nerovnice

$$2 \square 7 = 19 - 5$$

$$3 \square 3 = 7 + 2$$

$$2 \square 5 = 10$$

$$5 \square 5 = 25$$

$$3 \square 7 = 21$$

$$7 \square 3 = 2 \times 2$$

$$5 + 2 \square 8$$

$$3 + 1 \square 4$$

$$2 = 8 \square 6$$

$$12 \square 4 \times 3$$

$$7 \square 5 = 2$$

$$6 \square 1 = 5$$

$$8 \square 4 + 5$$

# Zóna 2

## Šifra 5 – Harmonogram

- 6:00 Vstanem, umyjem sa a vypijem štyri kávy.
- 7:30 Dva razy prestúpim a priveziem sa do práce.
- 2:55 Mojich päť detí príde zo školy a všetci spolu pôjdeme von.
- 3:00 Než zamierime na ihrisko, dáme si každý tri kopčeky zmrzliny.
- 4:30 Jeden z nás bude musieť ísť do obchodu, ostatní pôjdu oddychovať domov.



# Zóna 2

## Šifra 6 – Zložitý výlet

Veľmi som chcel ísť na výlet na Ukrajinu, no keď som tam konečne prišiel, bol som nútený zmeniť kurz o 90 stupňov doprava a odhodiť vrchnú časť batožiny. Celý nešťastný som odišiel do San Marína, kde som si dal odstrániť znak, ktorý som mal vytetovaný uprostred čela. Keď už som tam bol, otočil som sa vľavo a zahodil modré trojuholníkové pravítko, ktoré ma po celý čas štuchalo do pravého boku. V takom malom štáte však človek dlho nevydrží, preto som po pár dňoch odcestoval do Škótska. V škótsku bolo všetko ideálne a dokonca som trochu schudol z bokov. Napokon sa však ukázalo, že potrebujem ísť do Lichtenštajnska, kde mi amputovali pravú časť tela a musel som za to zaplatiť svojou kráľovskou korunou. Určite si viete predstaviť, že po tom všetkom sa mi už nechcelo cestovať nikam inam, len do Bavorska. Videl som z neho len kúsok, ale to mi nevadilo, lebo Bavorsko je vlastne všade rovnaké.

# Zóna 2

## Šifra 7 – Lekcie biliardu

Ako skúsený hráč biliardu by som sa s vami rád podelil o môj pohľad na taktiku a najmä správne zvládnutie koncovky v profesionálnom zápase. Tu sú moje lekcie:

Lekcia 1: Ak začínate, postavte sa za kratšiu hranu stola a hneď ako sa dostanete na ťah, trafte prvú guľu do diery vo vzdialenom rohu po vašej ľavici. Tým získate príležitosť potopiť ďalšiu guľu. Presuňte sa do stredu dlhšej hrany stola po vašej ľavici a mali by ste mať voľný výhľad na diery priamo oproti vám. Trafte do nej ďalšiu z vašich guľí. Tretiu guľu najlepšie trafíte tak, že prejdete na opačnú stranu stola a budete mieriť do ľavého rohu na náprotivnej stene. Ak trafíte, máte partiu perfektne rozbehnutú a ďalšie gule nebudú predstavovať problém.

Lekcia 2: Ak je partia dlho nerozhodná, postavte sa za kratšiu hranu stola a namierte prvú guľu do strednej diery po vašej ľavici. Nie je to jednoduchý šťuch, ale ak sa vám podarí, môžete sa presunúť k dlhšej hrane po vašej pravej ruke a trafiť druhú guľu do protiahlého pravého rohu. Týmto spôsobom získate v partii okamžitú prevahu.

Lekcia 3: Ak je váš súper skúsený, môže sa stať, že rýchlo potopí viacero guľí a vy ho budete potrebovať čo najskôr dobehnúť. V takom prípade sa opäť postavte za kratšiu hranu stola, trafte prvú guľu do diery hneď po vašej ľavej ruke, potom sa presuňte k protiahlejšej hrane a potopte ďalšiu guľu do diery po vašej pravej ruke. Keď sa následne presuniete k dlhšej hrane stola po vašej ľavici, môžete bez problémov mieriť do prostrednej diery priamo oproti vám. Týmto spôsobom poľahky zmažete súperov náskok zo začiatku hry.

Lekcia 4: Ak je pre správny postup partie potrebné rýchlo potopiť jednu guľu, postavte sa za kratšiu hranu stola a trafte ju do náprotivného rohu na ľavej strane. Viac vás nebude zdržovať.

Lekcia 5: Správne zvládnutý záver partie je pre úspech absolútne kľúčový. Ak vám zostávajú posledné dve gule, postavte sa za kratšiu hranu stola a rýchlo trafte prvú z nich do diery po vašej ľavej ruke. Následne prejdite k dlhšej hrane stola po vašej pravici a poslednú guľu namierte do náprotivného pravého rohu. Ak to zvládnete, víťazstvo je vaše.