

Šifrovanie, kódovanie, bit a byte, digitálne informácie

Šifry – šifrovanie sa používa všade tam, kde treba utajiť obsah komunikácie. Existuje veľmi veľa metód na tajné šifrovanie (a protimetódy na dešifrovanie). Šifry dosiahli neuveriteľnú úroveň a dôležitosť kvôli počítačom a komunikácii na Internete, súkromným informáciám (napr. rodné číslo, presná adresa bydliska, číslo účtu v banke atď.).

Kódy – cieľom kódovania je, aby sme mohli prenášať informáciu. Nie vždy však ide o utajenie. Často sa musíme prispôbiť **možnostiam technického zariadenia** (preto vznikla napr. Morseova abeceda ako jazyk pre telegraf), alebo **možnostiam ľudí** zapojených do komunikácie (preto vzniklo Breillovo písmo pre nevidiacich).

Kódovanie informácií je ľubovoľná vopred dohodnutá a všeobecne známa množina pravidiel, ktorá dovoľuje informáciu vyjadriť tak, aby sa dala uchovať, alebo šíriť.

Binárny kód. Bit

Ľudia medzi sebou používajú na komunikáciu reč. Ktorá pozostáva zo slov tvorených jednotlivými písmenami. Aby teda počítače porozumeli tomu, čo chceme aby vykonali, museli ľudia vymyslieť iný spôsob komunikácie. Počítače komunikujú – prenášajú informácie - v číslach. Informácie, ktoré im teda človek zadá, musia **prekódovať** do im zrozumiteľného jazyka.

Počítače používajú zvláštny spôsob kódovania informácií – **binárny kód**. Sú to postupnosti dvoch znakov – **0** a **1**. Morseova abeceda tiež používa iba dva znaky (ale na oddelenie slov používa tretí znak – medzeru).

Pamäť počítača si môžeme predstaviť ako milióny miniatúrnych prepínačov, z ktorých každý je buď ľavej polohe (pre znak 0) alebo v pravej polohe (pre znak 1). Dlhé postupnosti prepínačov predstavujú rôzne informácie.

Najmenšia jednotka binárneho kódu je **bit** (binary digit). Informácie zapísané v binárnom kóde sa nazývajú **digitálne informácie**.

Počítače spracovávajú obrovské množstvo informácií (znaky a čísla, farby, zvuk) a preto sa zapisujú do väčších jednotiek, ktoré sa označujú ako **byte** (pozostávajú z 8 bitov).

Kódovanie informácií v PC – binárna (dvojková) číselná sústava

Bežne v živote používame čísla vyjadrené v **desiatkovej pozičnej sústave**, ktoré :

- používajú cifry od nuly do deväť – teda **0, 1, 2, ..., 9**,
- využívajú pozičný spôsob zápisu. Skutočnú hodnotu každej cifry v čísle určuje to, či stojí na pozícii jednotiek alebo desiatok alebo stoviek atď. Tieto kľúčové čísla sa nazývajú **pozičné hodnoty**.

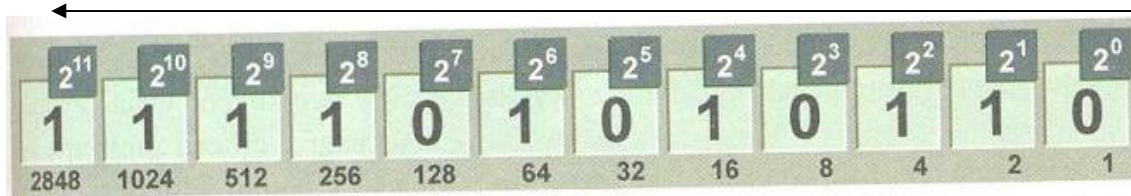


Napr. číslo **3 926** je súčtom **3000 + 900 + 20 + 6** teda 3-krát pozičná hodnota **1000** plus 9-krát pozičná hodnota **100** plus 2-krát pozičná hodnota **10** plus 6-krát pozičná hodnota **1**.

– binárny kód a dvojková sústava tvoria most medzi informáciou a elektronickými obvodmi počítača

Dvojková pozičná sústava :

- používa cifry od nula do jeden – teda iba 0 a 1,
- používa pozičný spôsob zápisu, ale pozičnými hodnotami sú mocniny čísla 2, teda sprava doľava



Prevod desiatkových čísel na dvojkové čísla

Každé desiatkové číslo je buď párne alebo nepárne. Napr. 30 je $15 \cdot 2$ so zvyškom 0 a 31 je $15 \cdot 2$ so zvyškom 1.

Pripísať za desiatkové číslo nulu, znamená vynásobiť ho desiatimi. Pripísať za dvojkové číslo nulu, znamená vynásobiť ho dvoma.

2. Prevody v rôznych číselných sústavách

1. Prevod z (10) do (2) ; prevody z (10) do iných číselných sústav (napr. 8,16)

Postup: postupne delíme číslo 2 (ak do inej sústavy tak 8,16...) a sprava doľava zapisujeme zvyšky, ktoré môžu byť:

1. dvojková sústava: 0,1

2. trojková sústava: 0,1,2

...

8. osmičková sústava: 0,1,.....,7

9. deviatková sústava: 0,1,.....,8

10. (z nej robíme prevod): 0,1,.....,9

11. jedenástková sústava: 0,1,.....,9,A

12. dvanástková sústava: 0,1,.....,9,A,B

...

16. šestnástková sústava: 0,1,.....,9,A,B,.....,F

Príklad 1:

$327 (10) \rightarrow ? (2)$

$327 : 2 = 163 : 2 = 81 : 2 = 40 : 2 = 20 : 2 = 10 : 2 = 5 : 2 = 2 : 2 = 1 : 2 = 0$

← 1 1 1 0 0 0 1 0 1

zápis čísla v dvojkovej sústave sprava doľava

Výsledok: $327 (10) \rightarrow 101000111 (2)$

Príklad 2:

$327 (10) \rightarrow ? (8)$

$327 : 8 = 40 : 8 = 5 : 8 = 0$

← 7 0 5

zápis čísla v osmičkovej sústave sprava doľava

Výsledok: $327 (10) \rightarrow 507 (8)$

3. Prevod z inej číselnej sústavy (2,8,16) do (10)

Postup je zhodný s prevodom čísla z dvojkovej do desiatkovej sústavy, mení sa iba číslo umocňované od 0 až po n (podľa sústavy, z ktorej prevod robíme) postupne, zprava doľava.

Pr. 1:

$$\begin{array}{ccccccc} & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & (2) & \longrightarrow & ? & (10) \\ & \swarrow & & \swarrow & \downarrow & \swarrow & \swarrow & \swarrow & \swarrow & & & & \\ 1.2^6 & + & 0.2^5 & + & 1.2^4 & + & 0.2^3 & + & 0.2^2 & + & 1.2^1 & + & 1.2^0 = 83 \end{array}$$

Výsledok: 1 0 1 0 0 1 1 (2) \longrightarrow 83 (10)

Pr. 2:

$$\begin{array}{ccc} & 3 & 2 & 7 & (8) & \longrightarrow & ? & (10) \\ & \swarrow & & \swarrow & & & & \\ 3.8^2 & + & 2.8^1 & + & 7.8^0 & = & 215 \end{array}$$

Výsledok: 3 2 7 (8) \longrightarrow 215 (10)

Pr. 3:

$$\begin{array}{ccc} & 3 & 2 & 7 & (16) & \longrightarrow & ? & (10) \\ & \swarrow & & \swarrow & & & & \\ 3.16^2 & + & 2.16^1 & + & 7.16^0 & = & 807 \end{array}$$

Výsledok: 3 2 7 (16) \longrightarrow 807 (10)

4. Prevod z inej číselnej sústavy (8,10, 16) do (2)

4a) Prevod z desiatkovej do dvojkovej sústavy už poznáme.

Príklad 1: 327 (10) \longrightarrow ? (2)

$$327 : 2 = 163 : 2 = 81 : 2 = 40 : 2 = 20 : 2 = 10 : 2 = 5 : 2 = 2 : 2 = 1 : 2 = 0$$

\longleftarrow 1 1 1 0 0 0 1 0 1
zápis čísla v dvojkovej sústave sprava doľava

Výsledok: 327 (10) \longrightarrow 101000111 (2)

4b) Prevody z iných číselných sústav do dvojkovej sústavy sa robia cez desiatkovú sústavu.

Pr. 1 : 327 (8) \longrightarrow ? (2)

Postup: 327 (8) → ? (10) → ? (2)

3. Sčítanie a odčítanie v dvojkovej sústave

Základné číselné operácie fungujú v dvojkovej sústave rovnako ako v desiatkovej, len nesmieme zabudnúť, že základným číslom nie je **10** ale **2**!

E	D	C	B	A
1	0	1	1	0
		1	1	1
	1	1		
?	?	1	0	1

Sčítanie

Rovnako ako v 10-tkovej sústave budeme sčítavať po stĺpcoch zprava doľava. Na každej pozícii oboch čísel môže stáť iba 0 alebo 1. Sčítujeme podľa pravidiel:
 $0 + 0 = 0$
 $1 + 0 = 1$
 $0 + 1 = 1$
 $1 + 1 = 0$ a **1** prenese ako zvyšok do ďalšieho stĺpca. V ďalšom stĺpci potrebujeme opäť sčítať $1 + 1$ miesto na zápis zvyšku je už obsadené z predchádzajúceho sčítania. Jednoducho ten zvyšok posunieme do ďalšieho stĺpca.

Odčítanie

Počítač nepozná záporné čísla. Teda, správne povedané záporné číslo chápe ako číslo kladné, ale inverzné. Uvedme si príklad:

V desiatkovej sústave odčítanie vyzerá takto: $3 - 5 = -2$

Číslo 5 v dvojkovej sústave sa zapíše ako 101.

Ale počítač nepozná záporné číslo a urobil by toto: $11 + 101 = 1000$, čo je číslo 8.

Jednou z možností ako vyjadriť „záporné“ číslo je použiť tzv. **doplňkový kód**.

Podme naspäť k nášmu príkladu : $3 - 5 = -2$

Počítaču to ale musíme „povedať“ takto: $3 + (-5) = (-2)$

Teda musíme si to číslo -5 „vyrobiť“.

1. Číslo 5 je v dvojkovej sústave 101. Zaberá teda 3 bity.
2. Na znamienko mínus použijeme jeden voľný bit, ktorý **doplníme** pred číslo.
3. Číslo 5 teda bude vyzeráť takto: 0101
4. 0 na prvej pozícii pred číslom bude označovať znamienko „+“
5. V ďalšom kroku prevedieme inverziu čísla – čo je nulou bude jednotkou a opačne.
6. Teda naše číslo 5 bude teraz vyzeráť takto: 1010
7. Teraz k nemu pripočítame číslo 1. (Tiež musí zaberáť 4 bity, takže zapíšeme: 0001)
8. Sčítame: $1010 + 0001 = 1011$
9. Toto číslo 1011 je naše hľadané číslo -5.

Výpočet bude teraz vyzeráť takto: $3 - 5 = -2$

Nezabudnime si číslo 3 (11) doplniť na 4 bity (0011)!

$$0011 + 1011 = 1110$$

Overíme si, či je číslo 1110 naozaj číslom -2.

1. číslo 2 je v dvojkovej sústave vyjadrené ako 10. Zaberá dva bity.

2. keďže číslo 5 zaberá tri bity a na vyjadrenie znamienka potrebovalo štvrtý bit, doplníme číslo -2 (10) o dva bity.
3. teda číslo 2 bude vyzeráť takto: 0010
4. teraz spravíme inverziu: 1101
5. pripočítame číslo 1: $1101 + 0001 = 1110$
6. Výsledok je teda správny. Číslo -2 je v doplnkovom kóde dvojkovej sústavy: 1110