

Základné pojmy informatiky

Údaj a informácia

Údaj (správa) – všetko, čo vidíme, počujeme alebo dokážeme zachytiť zmyslami (čuch, chuť, hmat) nezávisle od toho, či má pre nás nejaký informačný obsah.

Údaj – základný prvok (stavebná jednotka) informácie. Údaj je nedeliteľný. Údajmi môžu byť *písmená, čísla, znaky*, prípadne ich kombinácie. Údaje sa stávajú informáciami, ak sa použijú na riešenie nejakého problému. Ak nám daný údaj nepovie nič nového, hovoríme, že jeho *informačný obsah je nulový*.

Podľa *stanoveného cieľa* môžeme údaje zoskupovať týmito spôsobmi:

- na *vstupné* a *výstupné*
- na *numerické* a *alfanumerické*
- *aktívne* a *pasívne*.

Informácia

Informácie človek od nepamäti zbiera, spracúval, zaznamenával a šíril. Na zaznamenávanie využíval najprv iba pamäť, potom steny jaskýň, hlinené doštičky, papyrusy, neskôr papier a dnes na to používa aj počítače. Slovo informácia pochádza z latinského slova *informare*, čiže dať niečomu formu, oboznámiť, poučiť. Od IV. st. sa používalo vo význame vybaviť niekoho vedomosťou o čomsi.

Obdobiu, keď naši predkovia udržiavali vlastné skúsenosti a zážitky iba v svojej pamäti a nešírili ich inak než ústne, hovoríme *predhistória informácie*. Písmo a kníhtlač umožnili, aby sa vedomosti a pamäť ľudstva uchovávali aj inak než len v mysli človeka. Informácia sa stala voľne šíriteľnou. Objav písma a kníhtlače (okolo roku 1450) označujeme ako *prvú informačnú revolúciu ľudstva*. Potom nasledoval objav fotografie, telegrafu a telefónu. Dnes sa ľudstvo nachádza na prahu *druhej informačnej revolúcie*. Jej symbolom je počítač, výroba veľkého počtu osobných počítačov a ich intenzívne používanie.

Informácia – tá časť údajov, ktorá je pre prijímateľa zrozumiteľná a pochopiteľná. Znižuje nevedomosť prijímateľa, jeho neurčitost' a neistotu pri rozhodovaní. Informácia musí obsahovať *fakty*, ktorým prijímateľ rozumie.

Informácia robí z chaosu *poriadok* (alebo aspoň chaos znižuje), z neurčitosti *určitost'*, z náhodnosti *zákonitost'*.

Informácie musíme pred ich využitím najprv overiť. Nie vždy musia byť pravdivé. Informácie môžu byť tiež *užitočné* alebo *neužitočné*.

Informácie sú fakty, skúsenosti a vedomosti, ktoré ľudstvo **zbiera, zaznamenáva, spracúva a odovzdáva** ďalej. Pri slove *informácia* máme vždy na mysli odovzdávanie správ, ktoré svojho adresáta o niečom poučia, s niečím ho oboznámi.

Vzťah medzi informáciou a údajom je nasledovný: **Každá informácia musí byť údajom, ale nie každý údaj musí byť pre nás informáciou.**

Po uložení informácií (faktov) do počítača sa stávajú údajmi, ktoré sú v počítači zapísané pre nás nič nehovoriacimi reťazcami núl a jednotiek. V takomto tvare však s nimi výborne pracujú počítače, spracúvajú ich, vymieňajú si ich, ... Pre nás sa stávajú zrozumiteľnými až vtedy, keď ich zobrazí na obrazovke niektorý program.

Príklady:

Zápis $2^2 = 4$. Tento text je informáciou len pre žiaka, ktorý už čosi o mocninách počul. Prváčikovi, ktorý ledva dokáže prečítať prvých desať čísel, hovorí len to, že dva, dva o čosi vyššie, rovná sa štyri. Pre neho je to len údaj.

Veta „*I am hungry*.“ informuje adresáta o stave žalúdka odosielateľa len v prípade, ak adresát vie po anglicky. Inak pre neho informáciou nie je, nerozumie jej.

Informácie delíme na

- *analógové* - človek svojimi zmyslami vníma informácie prostredníctvom zmyslov ako spojitý sled javov (zvukové, svetelné...); informácie sa uložia tak, že sa zapíšu alebo vytlačia na papier, ofotografujú, vyšlú sa rádiom a pod.

- *digitálne* - postupnosť (reťazec) jednotiek a núl, ktoré môžu niesť informáciu aj o zvuku, obraze a pod. Digitálna informácia sa výborne uchováva a šíri.

Informácie delíme i na *záznamy* (čísla, fakty) a *návody* (postupy na výpočet, na riešenie problému a pod.). Tieto návody nazývame **algoritmus**.

Algoritmus je teda postupnosť krokov, ktoré slúžia na vyriešenie problému.

Informácie zbierame preto, aby sme mohli komunikovať, čiže šíriť ich tak, aby ich niekto prijal, porozumel im a použil ich. Informácie šírieme ústne, telefónom, literatúrou, rádiom, televíziou, pomocou výpočtovej techniky, ...

Informácie môžeme *zbierať, uchovávať, spracúvať* alebo *šíriť* (to sú štyri základné činnosti, ktoré môžeme vykonávať s informáciami). K tomu nám slúžia rôzne základné nástroje, ku ktorým patrí:
textový editor na vytváranie textových dokumentov,
grafický editor na nakreslenie alebo spracovanie obrázkov,
tabuľkový kalkulátor na prácu s tabuľkami, grafmi a jednoduchými databázami,
e-mail a mobilné telefóny na komunikáciu,
Internet a webové stránky na získavanie a zverejňovanie informácií,
prezentačné aplikácie na prezentáciu informácií,
hry a výučbový softvér na zábavu a vzdelávanie,
multimediálne nástroje na prácu so zvukom a videom na počítači.

Informatika

Informatika je vedný odbor, ktorý sa zaoberá *zberom, uchovávaním, spracúvaním a využívaním* údajov (resp. informácií). Informatika pozostáva z viacerých oblastí, prvky informatiky možno nájsť už takmer vo všetkých oblastiach ľudskej činnosti.

Cieľom informatiky je umožniť človeku rozhodovať sa s čo najväčšou pravdepodobnosťou určenia dôsledkov jeho rozhodnutí.

K informatike patria minimálne tieto disciplíny:
Výpočtová technika; Algoritmizácia; Softvérové inžinierstvo; Počítačová grafika; Počítačová simulácia; Formálna logika, teória automatov a formálnych jazykov; Kybernetika a robotika; Umelá inteligencia; knihoveda a ďalšie.

Jednotky informácie

Najmenšou jednotkou informácie je **1 bit** (číta sa bit, značka **b**). V počítačoch je vyjadrený logickými hodnotami **1** alebo **0**. V praxi vždy nadobúda jednu z dvoch navzájom vylučujúcich stavov, napr. je napätie – nie je napätie, pravda – nepravda, zapnutý – vypnutý, jedna – nula.

Ďalšie jednotky informácie (väčšie):

1 B = 2³ bitov = 8 bitov

1 Byte (číta sa bajt, značka **B**)

1KB = 1 024 B = 2¹⁰ B

číta sa 1 kilobajt

1 MB = 1 024 KB = 2¹⁰ KB = 2¹⁰ · 2¹⁰ B = 2²⁰ B

číta sa 1 megabajt

1 GB = 1 024 MB = 2¹⁰ MB = 2²⁰ KB = 2³⁰ B

číta sa 1 gigabajt

Existujú aj väčšie jednotky informácií (terabajt, petabajt, exabajt, zettabajt, yottabajt).

Digitalizácia a kódovanie informácií

Digitalizácia informácií

Človek svojimi zmyslami vníma analógové informácie (ako zvuk, obraz). Počítače pracujú iba s digitálnymi informáciami, zapisujú ich v binárnom (dvojkovom) kóde pomocou postupnosti núl a jednotiek. Najmenšia jednotka binárneho kódu je **bit**, je to **základná jednotka informácie**. Názov tejto jednotky je **bit** (binary digit).

Digitalizovať informáciu teda znamená zapísať ju v binárnom kóde. Pomocou n bitov vieme zapísať 2ⁿ rôznych hodnôt.

Ak môžeme použiť len *jeden* bit (n=1), tak máme *dva* znaky (2¹) – jeden charakterizovaný znakom 0, druhý 1. Ak môžeme použiť *dva* bity (n=2), tak máme *štyri* znaky (2²), ktoré v digitálnej forme vyzerajú takto: 00, 01, 10, 11. Ak môžeme použiť *tri* bity (n=3), tak máme *8* znakov (2³): 000, 001, 010, 011, 100, 101, 110, 111. Ak *štyri* bity (n=4), tak *16* znakov (2⁴): 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111.

Koľko núl a jednotiek je potrebných na jeden znak, aby sa dala zakódovať celá abeceda, veľké i malé písmená, číslice a aby ostala aj nejaká rezerva? Tvorcovia počítačov sa zhodli na 8 bitoch, takže písmeno

A by mohlo byť 00000001, atď. Z 8 núl a jednotiek možno vytvoriť $2^8 = 256$ kombinácií. Tejto kombinácii 8 núl a jednotiek (8 bitov) dali meno **byte** (bajt), značka B.

Teda jeden byte je jeden znak (napr. v abecede). Bežná strana „holého“ textu má asi 3 000 znakov, zaberie to teoreticky 3 000 B. Farby sa v počítači tiež ukladajú v bajtoch, nestačí však jeden bajt (8 bitov), ale niekoľko bajtov.

Najdôležitejšou vlastnosťou digitálnych informácií je *rýchlosť* a *jednoduchosť*, s akou sa dá s nimi počítať, ako rýchlo sa dajú *spracúvať*. Pretože digitálny (číslícový) zápis informácií je typický pre všetky počítače a moderné informačné a komunikačné systémy, budeme ich všeobecne nazývať **digitálne technológie** alebo **digitálne systémy**.

Digitálna informácia môže vzniknúť najčastejšie niektorým z týchto spôsobov:

- priamo v počítači prácou človeka alebo komunikáciou medzi počítačmi. Sú to reťazce núl a jednotiek, ktoré vyjadrujú nejakú textovú správu, obrázok a pod.
- sú analógového pôvodu, napr. snímky planéty, ktoré odfotoграфuje vesmírna sonda a odošle v digitálnom tvare riadiacej stanici na Zem.
- analógové informácie (farebné fotografie na fotografickom papieri, ilustrácie v knihe, nahrávky piesní na gramofónovej platni, rukou písané diela, skutočné zvuky z prírody, ...), ktoré chceme opäť použiť alebo spracovať pre ďalšie generácie, digitalizujeme (pomocou dig. fotoaparátu, skenera, ...)

Výhody digitálneho zápisu:

Digitalizovať sa dá *každý typ informácie* (text, obraz, hudba, video, ..., dokonca i vôňa). Digitálne informácie sa dajú uchovávať *v obrovských objemoch*. Dajú sa spracúvať *neuveriteľnou rýchlosťou*. Môžeme prehľadávať databázu podozrivých osôb, skúmať tisíce snímok z vesmíru, reštaurovať staré vzácne fotografie, vyrábať animované filmy, analyzovať ľudský hlas, atď.

Rozdiel medzi analógovým a digitálnym signálom:

Analógové zariadenie používa pre záznam zvuku, obrazu a pod. nejakú krivku, ktorá predstavuje priebeh magnetického poľa alebo inej fyzikálnej veličiny. Napríklad analógový magnetofón signál (hudbu, t. j. audiosignál) prevedie na nejakú krivku (priebeh magnetického poľa) a táto krivka je zaznamenaná na nejaký nosič (magnetofónovú pásku). Prenosom a kopírovaním pôvodnej krivky vždy dochádza k skresleniu a tým aj strate kvality pôvodného záznamu. Čím viac kópií, tým horšia kvalita. Čím náročnejšie podmienky prenosu (napr. cez telefón), tým je opäť horšia kvalita.

Teda: *analógový signál je pri každej kópii (resp. prenose) skreslený, preto klesá jeho kvalita.*

Digitálny (číslícový) záznam používa tzv. A/D prevodník analógového signálu. Jeho pomocou je záznam digitalizovaný a ďalej sa prenáša ako skupina 0 a 1. Pretože odlišiť 0 a 1 je možné takmer bezchybne (prípadné chyby sú hľadané tzv. kontrolnými bitmi).

Teda: *pri prenose (a kopírovaní) digitálneho signálu nedochádza k stratám a k skresleniu informácie, a teda ani kvality signálu.*

Kódovanie informácií

V živote sa stretávame s množstvom informácií. Pamätať si všetky nedokážeme. Preto ich určitým spôsobom kódujeme. Takým kódom je napr. aj naša adresa. Keď pozývame niekoho na návštevu, neopíšeme mu ako vyzerá náš dom, čo máme vysadené pred domom, aké auto nám stojí na dvore, ale zadáme jednoducho Nábrežná 42. Náš dom je zakódovaný ako ulica a číslo domu v ulici.

Podobne sa v obchodoch používa čiarový kód na zakódovanie názvu a ceny tovaru.

Kódovanie sa používa vtedy, keď vyjadrovanie bežnými slovami by bolo zdĺhavé alebo náročné na miesto a čas.

Kódovanie je proces, pri ktorom sa každému znaku alebo postupnosti znakov daného súboru znakov (vzorov) jednoznačne priradí znak alebo postupnosť znakov (obrazov) z iného súboru znakov.

Kódovanie je teda transformácia určitej informácie z jednej formy na druhú pomocou určitého postupu - *algoritmu*, ktorý je väčšinou verejne známy. Vo väčšine prípadov teda účelom kódovania nie je utajenie informácie (na rozdiel od šifrovania) ale len jej iná forma zápisu vybraná tak, aby sa informácia dala čo najlepšie alebo najúspornejšie uchovať alebo preniesť. Protimetódou je *dekódovanie*.

Ak chceme informácie šíriť utajene, musíme ju špeciálne zakódovať a hovoríme o *šifrovaní* (protimetódou je *dešifrovanie*).

Vďaka počítačom sa najčastejšie používa kódovanie údajov a informácií do číselnej podoby. Takémuto kódovaniu tiež hovoríme *digitalizácia*. Informácie zapísané v binárnom kóde nazývame *digitálne informácie*. Počítače i moderné komunikačné systémy pracujú s digitálnymi informáciami, nazývame ich *digitálne technológie* alebo *digitálne systémy*. Používa sa však aj nečíselné kódovanie. Typickým príkladom nečíselného kódovania z praxe je semafor červená = stoj, zelená = chod'. Ďalším príkladom je Morseova abeceda, príp. Braillovo písmo - písmo pre nevidiacich.

Hľadáme spôsob, ako pomocou núl a jednotiek zapísať (zakódovať) písmená slovenskej abecedy, číslice i interpunkčné znamienka, k týmto znakom pripojiť ešte „neviditeľné“ znaky ako medzera, Enter, Tab, rovnako aj české písmená Ř, ř, Ě, ě a ďalšie. Tých znakov je už viac ako 128 (2^7), ale menej ako 256 (2^8). Preto na kódovanie každého z nich použijeme 8 bitov, teda 1 byte (bajt).

Pridaním binárnych kódov znakom sa nazýva **kódová tabuľka**. Existuje však niekoľko možných kódovaní. Za posledné roky vznikli aspoň tri významné pokusy o jednotné kódovanie. Z nich najrozšírenejšie je kódovanie pomocou **ASCII** tabuľky (American Standard Code for Information Interchange, Americký štandardný kód pre výmenu informácií). Jeho nevýhodou je, že každý znak kóduje iba siedmimi bitmi, čo nám nevyhovuje, lebo možno zakódovať iba $2^7=128$ znakov.

Novým pokusom o univerzálne riešenie kódovacích problémov je jednotné kódovanie **Unicode**, v ktorom sa každý znak zapisuje pomocou 16 bitov, takže umožňuje používať $2^{16}=65\,536$ znakov zo všetkých bežných jazykov. Tento spôsob kódovania používa i kancelársky balík MS Office. Toto kódovanie zabezpečuje, že ten istý znak má rovnaký kód v každej krajine i na každom type počítača.

Nevýhodou tohto kódovania je, že znaky, ktoré sme predtým vedeli zakódovať iba ôsmymi bitmi, v kódovaní Unicode, sú kódované 16 bitmi, a teda zaberajú viac pamäte ako kód ASCII. Istým vylepšením tohto kódovania je kódovanie **UTF-8**. V tomto kódovaní je prvých 128 znakov tabuľky ASCII (tieto sú pre všetky krajiny rovnaké), zakódovaných pomocou 8 bitov a zvyšné znaky sú zakódované 16, 24, 32, 40 až 48 bitmi. Toto kódovanie je výhodné pre americky hovoriace krajiny a krajiny, v ktorých väčšinu znakov textu tvorí prvých 128 znakov tabuľky ASCII.

Tabuľka základných znakov ASCII (128 znakov)

kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	kód / znak	
0		16		32		48	0	64	@	80	P	96	`	112	p
1		17		33	!	49	1	65	A	81	Q	97	a	113	q
2		18		34	"	50	2	66	B	82	R	98	b	114	r
3		19		35	#	51	3	67	C	83	S	99	c	115	s
4		20		36	\$	52	4	68	D	84	T	100	d	116	t
5		21		37	%	53	5	69	E	85	U	101	e	117	u
6		22		38	&	54	6	70	F	86	V	102	f	118	v
7		23		39	'	55	7	71	G	87	W	103	g	119	w
8		24		40	(56	8	72	H	88	X	104	h	120	x
9		25		41)	57	9	73	I	89	Y	105	i	121	y
10		26		42	*	58	:	74	J	90	Z	106	j	122	z
11		27		43	+	59	;	75	K	91	[107	k	123	{
12		28		44	,	60	<	76	L	92	\	108	l	124	
13		29		45	-	61	=	77	M	93]	109	m	125	}
14		30		46	.	62	>	78	N	94	^	110	n	126	~
15		31		47	/	63	?	79	O	95	_	111	o	127	□

Tabuľka znakov ASCII (256 znakov)

0		44	,	88	X	132	ä	176	█	220	█
1	☺	45	-	89	Y	133	û	177	█	221	T
2	☹	46	.	90	Z	134	ć	178	█	222	U
3	♥	47	/	91	[135	ç	179		223	█
4	♦	48	0	92	\	136	l	180	-	224	Ó
5	♣	49	1	93]	137	ë	181	À	225	ß
6	♠	50	2	94	^	138	Ö	182	Á	226	Ô
7	•	51	3	95	_	139	ó	183	Ê	227	Ñ
8	▣	52	4	96	`	140	î	184	Š	228	ń
9	○	53	5	97	a	141	Ž	185	ƒ	229	ň
10	◼	54	6	98	b	142	Ä	186		230	Š
11	♂	55	7	99	c	143	Č	187]]	231	š
12	♀	56	8	100	d	144	É	188]]	232	Ř
13	♪	57	9	101	e	145	Í	189	Ž	233	Ú
14	♫	58	:	102	f	146	í	190	ž	234	ř
15	☀	59	;	103	g	147	ô	191	└	235	Ů
16	▶	60	<	104	h	148	ö	192	└	236	ý
17	◀	61	=	105	i	149	Ľ	193	└	237	Ý
18	↕	62	>	106	j	150	ŕ	194	└	238	ť
19	!!	63	?	107	k	151	Š	195	└	239	'
20	¶	64	@	108	l	152	ś	196	-	240	-
21	§	65	A	109	m	153	Ö	197	+	241	"
22	—	66	B	110	n	154	Ü	198	À	242	˘
23	↕	67	C	111	o	155	Ť	199	ã	243	˙
24	↑	68	D	112	p	156	ť	200	Ľ	244	˘
25	↓	69	E	113	q	157	Ľ	201	└	245	§
26	→	70	F	114	r	158	×	202	└	246	÷
27	←	71	G	115	s	159	č	203	└	247	,
28	L	72	H	116	t	160	á	204	└	248	°
29	↔	73	I	117	u	161	í	205	=	249	..
30	▲	74	J	118	v	162	ó	206	└	250	·
31	▼	75	K	119	w	163	ú	207	□	251	ú
32	(medzera)	76	L	120	x	164	Ą	208	đ	252	Ř
33	!	77	M	121	y	165	ą	209	Đ	253	ř
34	„	78	N	122	z	166	Ż	210	Ď	254	█
35	#	79	O	123	{	167	ż	211	Ě	255	
36	\$	80	P	124		168	Ę	212	ď		
37	%	81	Q	125	}	169	ę	213	Ň		
38	&	82	R	126	~	170	¬	214	Í		
39	'	83	S	127	△	171	ž	215	Î		
40	(84	T	128	Ç	172	Č	216	ě		
41)	85	U	129	ü	173	š	217	└		
42	*	86	V	130	é	174	«	218	└		
43	+	87	W	131	â	175	»	219	█		

Číselné sústavy

1) V bežnom živote používame **desiatkovú (dekadickú) pozičnú sústavu**, ktorej **základom** je číslo **10**. Používajú sa cifry od **0** do **9**, tj. 0, 1, ..., 9. Čísla v desiatkovej pozičnej sústave využívajú pozičný spôsob zápisu. Napr. v čísle 243 stojí cifra 3 na pozícii jednotiek (vyjadruje hodnotu tri jednotky, teda tri), cifra 4 na pozícii desiatok (vyjadruje hodnotu štyri desiatky, teda štyridsať), 2 na pozícii stoviek (vyjadruje hodnotu dve stovky, teda dvesto). Jednotky, desiatky, stovky, ... – tieto kľúčové čísla sa nazývajú **pozičné hodnoty**. Sprava doľava sú to **mocniny čísla 10**, teda sprava doľava 10^0 (čiže 1), 10^1 (čiže 10), 10^2 (čiže sto), 10^3 (čiže tisíc), ...

$$\text{Napr. } 2\ 846 = 2 \cdot 1\ 000 + 8 \cdot 100 + 4 \cdot 10 + 6 \cdot 1 = 2 \cdot 10^3 + 8 \cdot 10^2 + 4 \cdot 10^1 + 6 \cdot 10^0$$

2) Ak namiesto základnej hodnoty 10 zmeníme na **základ 2**, tak dostaneme **dvojkovú (binárnu) pozičnú sústavu**. Táto sústava používa cifry **0** a **1**. **Pozičné hodnoty** sú **mocniny čísla 2**, teda sprava doľava 2^0 (čiže 1), 2^1 (čiže 2), 2^2 (čiže 4), 2^3 (čiže 8), ...

$$\text{Napr. číslo v dvojkovej sústave } (110)_2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 1 \cdot 4 + 1 \cdot 2 + 0 \cdot 1 = (6)_{10}$$

Číslo 110 v dvojkovej sústave zodpovedá číslu 6 v desiatkovej sústave. $(110)_2 = (6)_{10}$

3) Používa sa aj **šestnástková (hexadecimálna) sústava**, ktorej **základom** je číslo **16**. Táto sústava používa cifry **0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F**. Pritom platí: A – 10, B – 11, C – 12, D – 13, E – 14, F – 15. **Pozičné hodnoty** sú **mocniny čísla 16**.

Napr. číslo v hexadecimálnej sústave

$$(A7E)_{16} = A \cdot 16^2 + 7 \cdot 16^1 + E \cdot 16^0 = 10 \cdot 16^2 + 7 \cdot 16^1 + 14 \cdot 16^0 = (2686)_{10}$$

Číslo A7E v šestnástkovej sústave zodpovedá číslu 2686 v desiatkovej sústave.

$$(A7E)_{16} = (2686)_{10}$$

Príklady:

dvojková sústava	desiatková sústava
0	$0 \cdot 2^0 = 0$
1	$1 \cdot 2^0 = 1$
10	$1 \cdot 2^1 + 0 \cdot 2^0 = 2$
11	$1 \cdot 2^1 + 1 \cdot 2^0 = 3$
100	$1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 4$
101	$1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 5$
110	$1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 6$
111	$1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 7$

Prevody v číselných sústavách

1) Prevod čísel z desiatkovej sústavy do dvojkovej a naopak

Pr. 1 Preveďte číslo 20 z desiatkovej sústavy do dvojkovej. Zápis: $(20)_{10} = (?)_2$

Riešenie:

20	2	0	↑
10	2	0	
5	2	1	
2	2	0	
1	2	1	
0			

Výsledok: $(20)_{10} = (10100)_2$

Ak chceme 8 bitové číslo, tak doplníme nuly pred číslo, ktoré sme dostali tak, aby sme získali osem bitov.

$(20)_{10} = (00010100)_2$

Pr. 2 Zapište číslo $(00110110)_2$ v desiatkovej sústave. Zápis: $(00110110)_2 = (?)_{10}$

Riešenie:

$$(00110110)_2 = 0 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 0 + 0 + 32 + 16 + 0 + 4 + 2 + 0 = (54)_{10}$$

Výsledok: $(00110110)_2 = (54)_{10}$

2) Sčítanie čísel zapísaných v dvojkovej sústave

Pr. Spočítajte čísla 1001101 a 100110 v dvojkovej sústave.

Riešenie: Sčítame rovnako ako v desiatkovej sústave, tj. sprava doľava

$$\begin{array}{r} 1001101 \\ 100110 \\ \hline 1110011 \end{array}$$

Pozor!

1+1 je síce 2, ale pracujeme v dvojkovej sústave, preto namiesto čísla 2 píšeme 10.

Takže zapíšeme 0, 1 sa zvýši, pripočítame to k ďalšiemu číslu.

Výsledok: $(1001101)_2 + (100110)_2 = (1110011)_2$

3) Násobenie čísel v dvojkovej sústave

Pr. Vynásobte čísla 10111 a 110 v dvojkovej sústave.

Riešenie:

$$\begin{array}{r} 10111 \\ \cdot 110 \\ \hline 00000 \\ 10111 \\ 10111 \\ \hline 10001010 \end{array}$$

Pozor!

1+1+1 je síce 3, ale pracujeme v dvojkovej sústave, preto namiesto čísla 3 píšeme 11.

Takže zapíšeme 1, 1 sa zvýši, pripočítame to k ďalšiemu číslu.

Výsledok: $(10111)_2 \cdot (110)_2 = (10001010)_2$

Ak chceme zistiť, či máme správny výsledok, stačí činitele vyjadriť v desiatkovej sústave, roznásobiť ich a porovnať s výsledkom vyjadreným v desiatkovej sústave.

$$(10111)_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 16 + 0 + 4 + 2 + 1 = (23)_{10}$$

$$(110)_2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 4 + 2 + 0 = (6)_{10}$$

$$(23)_{10} \cdot (6)_{10} = (138)_{10}$$

Vyjadríme výsledok v desiatkovej sústave:

$$(10001010)_2 = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 128 + 8 + 2 = (138)_{10}$$

4) Prevod čísel zo šesnástkovej (hexadecimálnej) sústavy do desiatkovej

Pr. Preveďte číslo $(B9E)_{16}$ do desiatkovej sústavy.

Riešenie:

$$(B9E)_{16} = 11 \cdot 16^2 + 9 \cdot 16^1 + 14 \cdot 16^0 = 2816 + 144 + 14 = (2974)_{10}$$

Výsledok: $(B9E)_{16} = (2974)_{10}$

5) Prevod čísel z desiatkovej do šesnástkovej sústavy

Pr. Preveďte číslo $(1442)_{10}$ do šesnástkovej sústavy.

Riešenie:

Desiatkové číslo delíme šesnástimi, zvyšky zapisujeme dovtedy, kým podiel nebude 0.

1442	16	zvyšok	2	↑	Výsledok: $(1442)_{10} = (5A2)_{16}$
90	16	10 (A)			
5	16	5			
0					

Komprimácia (kompresia, pakovanie, zbalenie, compression)

Súbory, ktoré obsahujú údaje (najmä obrázky a zvuky) bývajú veľmi veľké. Farebná fotografia z digitálneho fotoaparátu, ktorú chceme použiť napr. do školského časopisu, sa niekedy nedá uložiť ani na celú disketu. Pracovať s takýmito súbormi je náročné a pomalé. Preto sa vyvinuli metódy, ako už zapísané údaje znovu prekódovať – **kompresovať** (komprimovať, zhustiť) tak, aby zaberali čo najmenší objem.

♣ **Kompresia** údajov je séria metód ako prekódovať údaje tak, aby zaberali *menší objem* (ide teda o šetrenie miesta na disku) a aby sa dali opačným postupom opäť *odkódovať*.

Existuje mnoho rôznych komprimačných techník. Pri kompresii obrázka sa využíva to, že sa v ňom často opakujú dlhé úseky bodov rovnakej farby. Takýto úsek sa v kóde nahradí iba údajom o farbe a počte rovnakých bodov.

Vo všeobecnosti:

♣ **Kompresné algoritmy** obvykle hľadajú v komprimovaných údajoch často sa opakujúce vzorky, ktoré sú na výstupe reprezentované jedným opakovaním vzorky a počtom opakovaní.

Základné operácie komprimačných programov sú:

- ♪ komprimácia (pakovanie), dekomprimácia (rozpakovanie)
- ♪ vytvorenie archívu – vytvorenie jedného súboru z viacerých súborov
- ♪ rozbaľovanie archívu (extrakcia)
- ♪ pridanie do archívu, odobratie z archívu, prehliadanie obsahu archívu, používanie hesiel, možnosť ovplyvniť mieru komprimácie, ...

So skomprimovaným súborom môžeme vykonávať bežné operácie (kopírovanie, mazanie, presúvanie), ale nie je možné sa dostať k údajom v komprimovanom súbore. Skomprimovaný súbor je potrebné dostať najprv do pôvodnej podoby – dekomprimovať (rozbaľiť, rozpakovať).

Pomer veľkosti pôvodného a skomprimovaného súboru sa nazýva **kompresný pomer**. Udáva sa prostredníctvom pomeru (3:1 - skomprimovaný súbor je 3-krát menší ako pôvodný) alebo v percentách (77 % - nový súbor má veľkosť 77 % pôvodného). Najlepšie sa komprimujú databázové a textové súbory.

Medzi algoritmy dosahujúce najlepší kompresný pomer patria algoritmy programov WinRar, WinZip, Lha, Arj, Gzip, Bzip2, Rzip, ... Komprimáciu možno dosiahnuť i uložením súboru napr. vo formáte gif, jpg, jpeg, mpeg, mp3, ...

Na základe spôsobu komprimovania údajov možno kompresiu rozdeliť na:

♣ **bezstratový**, ktorá umožňuje rekonštruovať skomprimovaný súbor do pôvodnej podoby – ide o štandard, ktorý zrejme očakávame pri komprimovaní dokumentov, databáz a pod.

♣ **stratový**, ktorá prostredníctvom komprimácie niektoré údaje z pôvodného súboru vypustí a pri spätnej rekonštrukcii (dekomprimácii) ich už nedokáže obnoviť. Typické použitie je pri grafických súboroch, videu, zvuku. Využíva skutočnosť, že pri porovnaní originálneho a skomprimovaného obrazu či zvuku človek nevníma rozdiely medzi jemnými farebnými prechodmi a používa sa na miestach, kde je možné zánik niektorých informácií tolerovať a ich strata je vyvážená významným zmenšením súboru.

Šifrovanie

Kódy veľmi často používajú vojaci, námorníci alebo policajti. Napr. kód 22 môže znamenať *nepriateľ na dohľad*, kód 75 – *naháňam zlodēja* a pod.

Pokiaľ je účelom kódovania aj určité utajenie informácií a ich ochrana pred zneužitím, hovoríme o šifrovaní (kryptovaní).

Veda zaoberajúca sa šiframi sa nazýva *kryptológia*. Kryptológia pozostáva z *kryptografie*, ktorej cieľom je vytvoriť nerozlúšiteľnú šifru a *kryptoanalýzy*, ktorá ju má rozlúštiť.

Pokiaľ chceme údaje zašifrovať, potrebujeme na to minimálne *šifrovací/dešifrovací algoritmus* – postup, na základe ktorého sa pôvodná správa zmení na zašifrovanú (i naopak). Väčšina algoritmov vyžaduje na šifrovanie a dešifrovanie **klúč** (šifrovací, dešifrovací). Klúč by mal byť známy len odosielateľovi, ktorý na základe neho správu zašifruje a prijímateľovi, ktorý zvyčajne na základe toho istého kľúča správu dešifruje.

Jedným z najjednoduchších spôsobov je zámena písmena za iné. Algoritmus spočíva v zamieňaní písmen, kľúčom je tabuľka so zodpovedajúcimi dvojicami.

K šifram patrí Scytale, Cézarova šifra, taktiež Cardanova šifra, Verdanova šifra a ďalšie.

Šifry možno rozdeliť do dvoch základných kategórií:

♣ **Symetrické šifry** predstavujú kategóriu šifier, v ktorých sú šifrovacie kľúče pre šifrovanie a dešifrovanie rovnaké (resp. možno ich navzájom odvodiť). Všetky zúčastnené strany poznajú kľúč, pomocou ktorého je možné údaje šifrovať a dešifrovať.

Tieto šifry sa označujú aj ako šifry tajného kľúča a vyžadujú, aby sa príjemca aj odosielateľ vopred dohodli na kľúči, ktorý budú používať a potom ho tajili. Ak sa ten istý kľúč používa dlhšiu dobu, vzniká nebezpečenstvo jeho prezradenia alebo v prípade mnohonásobného používania i jeho dešifrovania (napr. prostredníctvom matematických výpočtov), preto sa kľúče často obmieňajú.

♣ **Asymetrické šifry** sú založené na myšlienke používania dvojice kľúčov – *verejného* a *súkromného*. Prostredníctvom *verejného* kľúča sa správa *zašifruje*, prostredníctvom *súkromného* kľúča *dešifruje*. Prijemca správy *nemúsi* poznať kľúč, prostredníctvom ktorého boli údaje zašifrované a odosielateľ *nesmie* poznať kľúč, ktorý správu dešifruje.

Majiteľ svoj verejný kľúč poskytne všetkým partnerom, s ktorými chce komunikovať a oni správy prostredníctvom neho zašifrujú. Dekódovať takto zašifrovanú správu možno už len prostredníctvom súkromného kľúča, ktorého jediným vlastníkom je prijímateľ správy, tento kľúč musí byť uchovávaný na bezpečnom mieste. Sila tohto typu šifrovania spočíva v tom, že komunikujúci svoje kľúče nemusia poznať a z toho dôvodu ich nemôžu ani poskytnúť nikomu ďalšiemu.

V súčasnosti sa na šifrovanie a podpisovanie často používa softvér PGP, alebo program GnuPG, ktorý vykonáva rovnakú funkciu, ale má voľnejšiu licenciu.

Typy šifier:

Substitučné šifry

- pre túto kategóriu je typické nahrádzanie znakov či skupín znakov inými znakmi alebo skupinami (napr. postupnosť AHA bude nahrádzaná skupinou FTG). Podmnožinou substitučnej šifry šifra je Cézarova šifra (posuvná) i Scytale, resp. Vigenérova šifra a ďalšie.

Cézarova šifra (nazýva sa aj posuvná šifra)

- spočíva v posúvaní znakov o zadanú hodnotu. Napr. pre text „Ahoj“ a hodnotu 3 sa všetky znaky posunú o 3 miesta a výsledkom bude „Dkrm“. V prípade, že sa pri presúvaní prejde za koniec abecedy, začína sa zasa od jej začiatku (napr. Z by sa zakódovalo ako C). Dešifrovanie spočíva v opačnom poradí.

Cardanova šifra

- je založená na použití mriežky, v ktorej sú vystrihnuté otvory. Do týchto sa napíše správa, mriežka sa odloží a prázdne miesta sa vyplnia náhodnými znakmi.

Pokročilejší variant: umiestnenie otvorov v mriežke tak, aby pri otáčaní o 90° pokrývali vždy iné políčka. Týmto spôsobom síce nezmetieme nepriateľa náhodnými znakmi, ale dokážeme naplno využiť všetky políčka tabuľky.

Otázky a úlohy

1. Vysvetlite pojmy údaj, informácia, informatika.
2. Definujte rozdiel medzi pojmom údaj a informácia.
3. Aký je rozdiel medzi alfanumerickými a číselnými (numerickými) typmi údajov?
4. Ako sa uchovávali prvé informácie?
5. Aký je vzťah medzi údajom a informáciou?
6. Napíšte činnosti, ktoré sa vykonávajú s údajmi resp. informáciami. (sú štyri)
7. Ako sa uchovávajú analógové informácie a ako digitálne?
8. Čo je algoritmus?
9. Ktoré nástroje slúžia k vykonávaniu rôznych operácií s informáciami?
10. Vymenujte niekoľko disciplín, ktoré patria k informatike.
11. Čo je najmenšou jednotkou informácie?
12. Čo je to jeden bit a ako sa označuje?
13. Akými logickými hodnotami je vyjadrený jeden bit?
14. Koľko bitov je jeden bajt (B)?
15. Koľko bajtov je jeden bit?
16. Charakterizujte bit a bajt. Aké jednotky množstva informácií poznáte?
17. Koľko rôznych znakov môžeme zakódovať pomocou 8 bitov, resp. jedným bajtom? Prečo?
18. Koľko B je jeden KB?
19. Koľko B je jeden MB a koľko jeden GB?
20. Prečo je 1 KB presne 1 024 a nie 1 000 B?
21. Prečo sa kilobajt (KB) píše s veľkým K a kilogram (kg) s malým k?
22. Koľko MB je jeden GB?
23. DVD disk má kapacitu 4,7 GB. Koľko je to MB, KB a B?
24. Koľko bajtov je jeden znak (písmeno, čiarka, bodka, výkričník a pod.) v texte?
25. Usporiadajte hodnoty podľa veľkosti od najmenej po najväčšiu:
 - a. 0,5 KB; 128 B; 1 024 b; 500 B
 - b. 0,25 KB; 500 B; 1 MB; 5 000 b
26. Uveďte niekoľko príkladov analógových a digitálnych informácií.
27. Prečo sa pri spracúvaní údajov prostredníctvom počítača využíva práve dvojková sústava?
28. Aké sú výhody digitálneho zápisu informácií?
29. Napíšte, či sa kopírovaním a) digitálneho signálu, b) analógového systému signál skresľuje alebo nie.
30. Čo je kódovanie?
31. Kedy sa používa kódovanie informácií?
32. Aký je rozdiel medzi kódovaním a šifrovaním?
33. Čo je kryptológia?
34. Charakterizujte šifrovací (dešifrovací) algoritmus.
35. Popíšte rozdiely medzi symetrickým a asymetrickým šifrovaním.
36. Na akom princípe sú založené substitučné šifry?
37. V čom spočíva Cardanova šifra?
38. V čom spočíva Cézarova (posuvná) šifra?

39. Vysvetlite pojem digitalizácia.
40. Uveďte zariadenia, ktoré možno využiť na digitalizáciu.
41. Aké nečíselné kódovanie poznáte?
42. Na čo slúži kódová tabuľka?
43. Vysvetlite ako vyzerá kódová tabuľka ASCII (koľko znakov obsahuje, koľkými bitmi zapisuje jednotlivé znaky, aké znaky našej abecedy tam nie sú).
44. Vysvetlite ako vyzerá kódová tabuľka Unicode (koľkými bitmi sa zapisuje každý znak, koľko znakov umožní zapísať táto tabuľka, koľko pamäte zaberú znaky v porovnaní s kódovaním ASCII).
45. Vysvetlite kódovanie pomocou tabuľky UTF-8.
46. Vypočítajte:
- $(10110110)_2 = (\quad)_{10}$
 - $(625501)_8 = (\quad)_{10}$
 - $(9412)_{10} = (\quad)_2$
 - $(AF10)_{16} = (\quad)_{10}$
 - $(24EE0)_{16} = (\quad)_{10}$
47. Aký zápis má číslo 123 v dvojkovej sústave?
- 1100111
 - 1111011
 - 1001111
 - 1110011
 - žiadna z uvedených možností
48. Vypočítajte:
- $(10110)_2 + (1000110)_2 =$
 - $(1110)_2 + (11111)_2 =$
 - $(1001)_2 \cdot (101)_2 =$
 - $(111011)_2 \cdot (111)_2 =$
49. Preveďte
- a) do dvojkovej sústavy číslo 578 z desiatkovej sústavy
 - b) z dvojkovej sústavy do desiatkovej číslo 10110011.
50. Vysvetlite pojem komprimácia a popíšte jej princíp.
51. Čo viete o kompresii údajov, kedy sa používajú komprimačné programy?
52. Aké typy komprimácie poznáte? Vysvetlite rozdiel medzi nimi.