

# **OBSAH**

## **8. ročník**

- 13. Zvuk a zvukové formáty ...23
- 14. Počítačová grafika ...25
- 15. Digitalizácia videa - video formáty ...27
- 16. Dvojková a desiatková sústava- prevody ...30
- 17. Počítačové siete ...32
- 18. Elektronický podpis ...36
- 19. Počítačové vírusy ...37

## 8. ROČNÍK

### 13. ZVUK A ZVUKOVÉ FORMÁTY (8.ročník)

Digitalizácia analógového zvukového signálu sa robí meraním napätia signálu v pravidelných intervaloch. Čím kratšie budú intervaly, tým viac meraní urobíme za určitý časový úsek a tým presnejšie priebeh zvuku zachytíme. Získame tak kvalitnejší záznam. Počet meraní za určitú časovú jednotku sa nazýva **vzorkovacia frekvencia** (sampling rate) a udáva sa v kHz (napr. frekvencii 11 kHz zodpovedá 11 000 meraní za sekundu).

Najnižšie hodnoty vzorkovacej frekvencie sa používajú pri digitalizácii telefónneho hovoru (bežne je to 8000 Hz). Jednou z najnižších používaných hodnôt vzorkovacej frekvencie je 11,025 kHz. Ďalej sa používa 22,05 kHz a pre digitalizáciu veľmi kvalitnej nahrávky, zodpovedajúcej kvalite CD audio nahrávky, sa používa frekvencia 44,1 kHz a 48 kHz, čo predstavuje 44 100 a 48 000 údajov za sekundu.

Ďalším parametrom kvality nahrávky je **veľkosť vzorky** (sample size). Udáva sa v počte bitov. Čím väčší počet bitov, tým presnejší údaj získame a môžeme zachytiť väčšie rozdiely v hlasitosti. Pre uloženie nameranej hodnoty sa používa najmenej 1 byte, t. j. 8 bitov, pri kvalitných nahrávkach sa využíva 16 bitov, pri stereo hudbe potom máme dvakrát 16 bitov.

Vzorkovanie a prevod analógového signálu sa robí pomocou **prevodníka A/D** (analog-to-digital) uloženého na zvukovej karte. Pri prehrávaní záznamu je treba spätne digitálny signál previesť na analógový pomocou **prevodníka D/A**. Na kvalite analógovo-digitálneho prevodníka (zvukovej karty) závisí kvalita výsledného digitalizovaného zvuku. Najčastejšou metódou prevodu analógového signálu na digitálny je **Pulzná kódová modulácia** (PCM).

#### TYPY ZVUKOVÝCH FORMÁTOV

Zvukové súbory obsahujú zvuk v rôznych formátoch. Formáty digitalizovaného zvuku môžeme rozdeliť na nekomprimované (zaberajú na disku viac miesta) a komprimované, ktoré sú pri porovnateľnej kvalite menšie a sú vhodné aj na prenos po internete. Formáty bez kompresie ukladajú zvukové dáta v takej podobe ako boli získané digitalizáciou. Formáty s kompresiou tieto dáta ďalej upravujú. Pod pojmom kompresia sa rozumie odstraňovanie redundancie (nadbytočných dát), takže súbor zaberá menej miesta na disku. Kompresné formáty sa rozdeľujú na stratové a bezstratové. Bezstratové kompresie odstraňujú len istú časť dát tak, aby bolo možné vrátiť súbor do originálneho stavu. Stratové kompresie odstraňujú väčšie množstvo dát, takže sa nemôžeme vrátiť k pôvodnej kvalite. Štruktúra zvukového súboru pozostáva z hlavičky a samotných dát. V hlavičke sú uložené dôležité informácie ako dĺžka záznamu, počet kanálov, typ formátu, vzorkovacia frekvencia a pod. Pre hudobné účely

bol vyvinutý formát MIDI. MIDI predstavuje čisto digitálny zvuk, teda zvuk ktorý bol vytvorený priamo v počítači. MIDI súbory zaberajú na disku omnoho menej miesta ako zvukové vzorky a pritom ponúkajú vynikajúcu kvalitu zvuku.

## KODEK

Pre efektívnejšiu prácu so zvukovými súbormi sa používajú kodeky. Slovo [kodek](#) pochádza z angličtiny (codec) a je to skratka z dvoch slov COder a DECoder. Kodek slúži na zakódovanie a dekodovanie, inak povedané na kompresiu a dekompresiu zvuku. Je to ovládač, ktorý pridáva podporu pre nejaký konkrétny audio/video formát pre operačný systém. Vďaka kodeku operačný systém tento formát rozozná a dovoľí ho prehrať (decode = dekóduje ho) alebo dovoľí zmeniť ho na iný formát (encode = zakóduje).

Nájsť vhodný pomer medzi kvalitou zvuku a veľkosťou súboru je jedna z najťažších volieb pri práci s digitalizovaným zvukom. Treba vhodne zvoliť nielen parametre digitalizácie (vzorkovaciu frekvenciu, bitovú hĺbku a počet kanálov), ale aj správny formát súboru, prípadne kompresiu.

### 1.1

#### 1.2 Formáty bez kompresie

---

Nevýhodou všetkých týchto formátov je veľký objem dát v súbore.

- [AU](#) (\*.au, \*.snd) – (Audio File Format) AU je štandardom pre prostredie Unix a programovací jazyk JAVA.
- [AIFF](#) (\*.aiff, \*.aif) – (Audio Interchange File Format) Je zvukový formát, používaný v OS počítačov Apple.
- [WAVE](#) (\*.wav) – (Waveform Audio file format) Je to základný, predvolený formát na počítačoch s OS Windows.

### 1.3 Formáty so stratovou kompresiou

---

Vznik súborov so stratovou kompresiou bol podmienený hlavne potrebou podstatne znížiť objem dát zvukových súborov. Mnohé z týchto formátov našli svoje uplatnenie najmä na sieti internet.

- [MPEG](#) Audio (\*.mp1, \*.mp2, \*.mp3, \*.m2a, \*.mpa, \*.mpg, \*.mpeg, \*.swa) – MPEG je stratovou kompresnou schémou založenou na psychoakustickom modeli ľudského ucha.

MPEG má mnoho podôb, v závislosti od zložitosti použitých kompresí. Čím vyššia vrstva, tým vyššia kompresia a menšia veľkosť súboru.

- [WMA](#) (\*.wma) – (Windows Media Audio) WMA vyvinula spoločnosť Microsoft. Kvalitou mierne prekonáva obľúbený formát mp3, ale iba pri nižších dátových tokoch.
- [RealAudio](#)(\*.ra, \*.rm, \*.ram) – Tento formát získal svoju popularitu vďaka streamovaniu zvuku na webe ako prvý streamovací zvukový formát. Patrí medzi najstaršie formáty a má široké použitie. Vysoký kompresný pomer, ale nízka kvalita.

## 1.4

### 1.5 Formáty s bezstratovou kompresiou

---

- [FLAC](#) **Free Lossless Audio Codec** (FLAC) je slobodný [súborový formát](#) určený na uchovanie [audio](#) dát. Je to bezstratový kompresný formát, teda na rozdiel od stratových formátov ako [MP3](#), [AAC](#) alebo [Vorbis](#) nedochádza pri kompresii k strate informácií. Veľkosť súboru skomprimovaného týmto kodekom je asi 30-50% veľkosti pôvodného súboru.<sup>[1]</sup>
- 

## 14. Počítačová grafika

### 2D- dvojrozmerná (X,Y)

#### **Vektorová- tvoria ju geometrické útvary**

- úsečka =**vektor**
- **bezstratová**( pri zväčšení obrázka nevidno úbytok na kvalite)
- formáty súborov vytvorené vo vektorovej grafiky  
(svg,ai,pdf,eps,cdr,swf)
- software: Adobe Illustrator, Inkscape ...

#### **Rastrová - tvoria ju usporiadané body (pixle)**

- (bitmapová) -úsečka =**raster**
- **stratová**( pri zväčšení obrázka vidno úbytok na kvalite)
  - formáty súborov vytvorené vo vektorovej grafiky  
(jpg,png,tiff,raw,gif,bmp)
  - software: Adobe Photoshop, Gimp, Skicár...

### 3D- trojrozmerná (X,Y,Z)

-príbuzná vektorovej 2D grafike, dáta sú uložené v trojrozmernom koordinačnom systéme (X,Y,Z)

Software: 3Ds Max, Cinema 4D, LightWave 3D, ZBrush, Blender ...

### Farebné režimy

**RGB-** používa v monitoroch

R- red  
G- green  
B- blue

**CMYK-** používa

v tlačiarenských zariadeniach

C- cyan  
M- magenta  
Y- yellow  
K- black

**Rozmery obrázka:** šírka x výška (800 x 600)

**Rozlíšenie:** PPI- počet obrazových bodov na palec(v monitoroch)

Web grafika= 72 PPI, grafika na tlač= 300 PPI

DPI- počet vytlačených bodov na palec(v tlačiarňach)

tlačiareň= 300 -1800 DPI

**palec=2,54 cm**

## Ako sa ukladajú obrázky a video

Obrázok v počítači je uložený buď ako sieť (raster) malých farebných štvorcov (rastrový obrázok) alebo ako návod (postupnosť inštrukcií – príkazov), ako ho zostrojiť pomocou kružníc, čiar, obdĺžnikov a pod. (vektorový obrázok). Veľkosť rastrového obrázka v počítači závisí od počtu farieb, ktoré môže obsahovať. Jeden farebný bod z palety 16 farieb zaberie 4 bity, z palety 256 farieb 8 bitov (1 bajt), z palety 65 536 farieb (farebnosť High Colour) 16 bitov (2 bajty) a z palety 16 miliónov farieb (farebnosť True Colour) 24 bitov (3 bajty). Na vytváranie rastrových obrázkov môžeme použiť napr. Skicár alebo Logo Motion alebo ich získame pomocou digitálneho fotoaparátu. Vektorové obrázky vytvoríme v programoch CorelDraw alebo Zoner Callisto.

Digitálne video je séria statických rastrových obrázkov, ktoré sa rýchlo vymieňajú pred naším zrakom. Za jednu sekundu sa na obrazovke vystrieda 30 takýchto obrázkov. Ak by sme nepoužili žiaden spôsob kompresie, súbor s videom by bol obrovský. Bežne sa používajú tieto metódy na zmenšenie veľkosti súboru videa:

1. použiť menší obrázok, napr. iba 320 x 240 bodov
2. za jednu sekundu zobrazíť namiesto 30 obrázkov iba 12, pohyb na obrazovke potom nie je plynulý
3. použiť kompresiu na každý obrázok zvlášť, plynulý pohyb obrázkov si vyžaduje rýchly počítač
4. zapamätať si prvý obrázok sekvencie, a potom ďalej už len tie údaje, ktoré sa zmenia pri prechode z jedného obrázka na druhý

Zároveň je nutné zvyšovať kapacitu pamäťových médií a zlepšovať metódy kompresie.

---

## 15. DIGITALIZÁCIA VIDEO A FORMÁTY VIDEO SÚBOROV

**Formát súboru** (iné názvy: **súborový formát**, **typ súboru**) je konkrétny spôsob kódovania informácií s cieľom ich uchovania v [počítačovom súbore](#).

Keďže [pevný disk](#), a v podstate akékoľvek [pamäťové zariadenie](#) počítača, vie uchovávať iba [bity](#), počítač musí mať nejaký spôsob ako premieňať [informácie](#) na nuly (0) a jednotky (1), a naopak. Existujú rôzne druhy formátov pre rôzne druhy informácií. Ale, v rámci každého formátového typu, napr. dokumenty [slovného procesora](#), bude typicky niekoľko rozdielnych – a niekedy konkurenčných – formátov.

Niektoré formáty súborov sú navrhnuté tak, aby uchovávali veľmi konkrétne typy dát: formát [JPEG](#), napríklad, je navrhnutý iba na uchovávanie statických [obrázkov](#). Na druhej strane, iné formáty súborov sú navrhnuté na uchovávanie viacerých rozličných typov dát: formát [GIF](#) podporuje uchovávanie aj nehybných obrázkov, aj jednoduchých animácií, a formát [QuickTime](#) vie plniť funkciu obalovej nádoby pre mnoho rozličných typov [multimédií](#). [Textový súbor](#) je jednoducho taký súbor, ktorý uchováva akýkoľvek text, vo formáte napr. [ASCII](#) alebo [Unicode](#), s veľmi málo (ak vôbec nejakými) [riadiacimi znakmi](#). Niektoré formáty súborov, ako napríklad [HTML](#), alebo [zdrojový kód](#) niektorého konkrétneho programovacieho jazyka, sú v skutočnosti takisto textové súbory, ale podliehajú špecifickejšim pravidlám, ktoré im umožňujú byť použité na konkrétne účely.

Niekedy je možné spôsobiť, aby program prečítal súbor kódovaný v jednom formáte tak, akoby bol kódovaný v inom formáte. Napríklad je možné prehrať dokument [Microsoft Word](#) akoby to bola pesnička použitím programu na prehrávanie hudby, ktorý narába s „bezhlavičkovými“ audio súbormi. Výsledok však nebude znieť veľmi ľubozvučne. Je to preto, lebo zmysluplné usporiadanie [bitov](#) v jednom formáte je takmer vždy nezmyselné v inom formáte.

Asi každý, kto sa aspoň trochu orientuje vo svete počítačov a využíva ich na prehrávanie multimédií, mal určite neraz problém s prehrávaním niektorého video súboru. Pretože sa v dnešnej dobe často zamieňa pojem kodek, formát a kontajner, rozhodol som sa priniesť článok, ktorý by v tejto oblasti pomohol ujasniť aspoň základné rozdiely a tým pomohol mnohým používateľom.

Asi každý, kto sa aspoň trochu orientuje vo svete počítačov a využíva ich na prehrávanie multimédií, mal určite neraz problém s prehrávaním niektorého video súboru. Za takýmto problémom sa často skrýva problém s rôznymi použitými formátmi a kontajnermi, keďže každý formát vyžaduje niektorý z kodekov na svoje dekódovanie. Pretože sa v dnešnej dobe často zamieňa pojem kodek, formát a kontajner, rozhodol som sa priniesť článok, ktorý by v tejto oblasti pomohol ujasniť aspoň základné rozdiely a tým pomohol mnohým používateľom.

## **Kompresia**

Stratová kompresia pri komprimovaní obsahu využíva nedokonalosti ľudského oka a ucha, a tak vynecháva niektoré pre nás často nepozorovateľné informácie, ktorých strata nám pri optimálnom dátovom toku vôbec neprekáža. Problém nastáva pri nízkych dátových tokoch, pri ktorých je už strata informácií značne pozorovateľná, a tým znižuje kvalitu výsledného videa. V niektorých prípadoch pri práci s videom sa môže použiť aj bezstratová kompresia, no výsledné video je spravidla veľmi veľké, a z toho dôvodu je ho problém prenášať alebo uskladňovať. Na vyjadrenie kompresie videa a teda aj účinnosti daného kompresného algoritmu sa využíva tzv. kompresný pomer, ktorý je daný ako podiel pôvodnej a komprimovanej veľkosti videa.

## **Formát a kodek**

Mnohokrát sa názov použitého kodeku a formátu môže zhodovať, no netreba sa tým nechať pomýliť, pretože medzi kodekom a formátom je značný rozdiel. Formát je daný svojou špecifikáciou. Príkladom môže byť napríklad MPEG-4, v ktorom sa uskladňuje video. Pre jeden formát však môže existovať viacero kodekov, ktoré dokážu audio a video do tohto formátu uložiť. Pokiaľ chcete zistiť v akom formáte je vaše video, akým kodekom bolo vytvorené a mnohé ďalšie informácie, môžete použiť napríklad program VideoSpec(OSX) alebo MediaInfo(Windows) ktorý vám poskytne mnoho užitočných informácií.

Kodek (odvodené od kóder) je vlastne algoritmus, ktorý dokáže video zakódovať do určitého formátu a pomocou dekóderu aj prehrať. Existujú však kóдеры a dekóдеры, ktoré nemusia byť distribuované spoločne. Príkladom môže byť napríklad formát H264(MPEG-4 AVC) pričom na kompresiu videa do takéhoto formátu sa využíva kódér x264, no na dekódovanie sa využíva napríklad dekodér FFmpeg, CoreAVC a iné. Kvalita výsledného videa ktoré vytvoríme, a taktiež náročnosť pri prehrávaní, ale aj vytváraní videa je závislá práve od použitého kodeku (kóderu/dekóderu). [1]

## **Kontajner**

Ďalšou vecou, ktorá sa pri videách často pletie s formátom, je použitý kontajner. Ako príklad sú na obrázku 2 zobrazené dva video súbory, ktoré obsahujú úplne rovnaký formát videa aj audia, ale ich prípona je rôzna. Tento rozdiel je spôsobený práve použitím rôznych kontajnerov.

Samotné video býva distribuované spolu s audio stopou v nejakom kontajneri. Asi najznámejší kontajner je Audio Video Interleave, čiže AVI. Zvyčajne obsahuje video vo formáte MPEG-4 a audio vo formáte MP3. Niektoré kontajnery ako matroška poskytujú viac možností, ako je možnosť viacerých audio stôp, či titulkov. Samotná matroška obsahuje väčšinou video vo formáte H264. Netreba sa dať zmiast' niektorými formátmi, ako napríklad Windows Media Video (WMV), ktorý sa nachádza v rovnomennom súbore wmv, a je kódovaný a dekódovaný kodekom Windows Media Video 7,8,9 series. Ide tiež o kodek, kontajner a formát, avšak keďže je to produkt jednej firmy, tak si zvolila jeden spoločný názov.

### **Popis niektorých najpoužívanejších kontajnerov**

**AVI** (Audio Video Interleave) je jeden z najpoužívanejších kontajnerov. Bol vyvinutý spoločnosťou Microsoft v roku 1992. Štruktúra formátu kontajneru vychádza zo staršieho formátu RIFF. Prípona súborov je .avi.

**Matroska** kontajner bol vyvinutý v roku 2002. Súbory sú uložené pod príponou mkv, prípadne mka. Je to moderný kontajner, ktorý umožňuje použiť viacero audio stôp a titulkov. Veľmi často sa používa najmä s formátmi MPEG-4 ASP, MPEG-4 AVC, pre video a MPEG-4 AAC, vorbis, AC3 pre audio stopu.

**QuickTime** je kontajner vyvinutý spoločnosťou Apple Inc. Súbory QuickTime bývajú označené príponou .mov. Podpora formátov pre audio a video je v QuickTime podobná, ako pri kontajneri Matroska. V súčasnej najnovšej verzii kontajneru mov sa často stretávame s použitím MPEG-4 AVC videa v kombinácii s audio formátom AAC.

**MP4** je kontajner definovaný štandardom ISO/IEC 14496-14:2003. Je súčasťou štandardu MPEG-4. Základ kontajneru mp4 vychádza z kontajneru mov. Podporuje vkladanie video, audio a aj 3D obsahu. Tento kontajner sa používa hlavne s formátom videa MPEG-1, MPEG-2 a MPEG-4 a formátom audia v MP3 alebo AAC.

### **Prehľad najpoužívanejších kodekov pre niektoré formáty videa**

**MPEG-4 AVC** pre tento formát sa najčastejšie využíva kodek x264, ktorý je v súčasnosti asi najpokrokovejším kodekom pre tento formát. Vďaka podpore veľkého množstva možností komprimácie videa, ktoré formát MPEG-4 AVC ponúka, dosahuje veľmi dobrý pomer kvalita / veľkosť, vďaka čomu je vhodný na ukladanie napríklad HD videa. Tieto videá bývajú prevažne uložené v kontajneri MP4, MKV alebo MOV.

**MPEG-4 ASP** video je často komprimované práve kodekom DivX, alebo jeho opensource konkurentom Xvid. Video vytvorené niektorým z týchto dvoch kodekov je vo formáte MPEG-4 AVC a je ho možné prehrávať ľubovoľným kodekom pre tento formát. Možnosť prehrávať video vytvorené kodekom Xvid na zariadeniach certifikovaných iba pre DivX môže



niekedy spôsobovať problémy pre niektoré modifikácie, ktoré využíva na rozdiel od kodeku DivX. Dnešné CD/DVD prehrávače však väčšinou umožňujú prehrať video vytvorené hociktorým z týchto dvoch kodekov. Videá vytvorené týmito kodekmi bývajú často umiestnené v AVI kontajneri. Kvalita videa je však pri porovnaní s modernejším kodekom x264 pri rovnakom dátovom toku nižšia.

**WMV** (Windows Media Video) je formát, ktorý je zakódovaný rovnomenným kodekom wmv. Wmv bol vyvinutý spoločnosťou Microsoft. Pôvodne mal súžiť na prenos streamovaného videa. Kodek WMV 9 sa po štandardizácii aj pod názvom VC-1 stal jedným z troch základných kodekov pre HD obsah na BlueRay a HD-DVD médiách.

### **Najznámejšie kontajnery:**

AVI, Ogg, MPEG (mpg), QuickTime (mov), MP4, Matroška (mkv)

### **Najznámejšie kodeky:**

video: Divx Pro Codec, Xvid, Windows Media Video 9 series, libtheora, libavacodec, x264  
audio: FLAC, Apple Lossless, Windows Media Audio 9 series, FAAC(AAC), LAME(MP3)

### **Najznámejšie formáty:**

video: MPEG-1,2,4, H264 (MPEG-4 AVC), Theora, WMV  
audio: AAC, Apple Lossless, AC-3, FLAC, MP3, WAV, WMA

---

## **16. Dvojková sústava**

Desiatková čiže **dekadická sústava** je číselná sústava, v ktorej počítame my - ľudia. Je pozičnou sústavou, ktorá používa cifry 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Základom sústavy je číslo 10 a pozičnými hodnotami sú mocniny čísla 10, teda:  $10^0=1$ ,  $10^1=10$ ,  $10^2=100$ ,  $10^3=1\ 000$ ,  $10^4=10\ 000$ , ... Napr. číslo 3927 je súčtom  $3 \cdot 10^3 + 9 \cdot 10^2 + 2 \cdot 10^1 + 7 \cdot 10^0 = 3000 + 900 + 20 + 7 = 3927$ .

Dvojková čiže **binárna sústava** je číselná sústava, v ktorej pracuje počítač. Preto je základnou sústavou v informatike. Je pozičnou sústavou, ktorá používa cifry 0, 1. Základom sústavy je číslo 2 a pozičnými hodnotami sú mocniny čísla 2, teda:  $2^0=1$ ,  $2^1=2$ ,  $2^2=4$ ,  $2^3=8$ ,  $2^4=16$ , ... Napr. číslo 1101 je súčtom  $1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 4 + 0 + 1 = 13$ .

**Z desiatkovej do dvojkovej sústavy sa prevádza** celá časť čísla týmto algoritmom:

1. Desiatkové číslo vydelíme 2.

2. Zapišeme zvyšok (čiže 0 alebo 1).
3. Výsledok delenia opäť vydelíme 2.
4. Zvyšok zapišeme pred predchádzajúci zvyšok
5. Opakujeme kroky 3 a 4 tak dlho, kým výsledok delenia nie je 0.
- 6.

Napríklad prevedieme číslo 397 do dvojkovej sústavy:

$$397 : 2 = 198 \text{ zv. } 1$$

$$198 : 2 = 99 \text{ zv. } 0$$

$$99 : 2 = 49 \text{ zv. } 1$$

$$49 : 2 = 24 \text{ zv. } 1$$

$$24 : 2 = 12 \text{ zv. } 0$$

$$12 : 2 = 6 \text{ zv. } 0$$

$$6 : 2 = 3 \text{ zv. } 0$$

$$3 : 2 = 1 \text{ zv. } 1$$

$$1 : 2 = 0 \text{ zv. } 1$$



Číslo 397 je v dvojkovej sústave zapísané takto:

110001101

**Prevod dvojkových čísel na desiatkové** je veľmi jednoduchý. Robíme ho týmto algoritmom:

1. Prvým medzivýsledkom je 0.
2. Oddelíme prvú cifru dvojkového čísla.
3. Ak je oddelenou cifrou 0, medzivýsledok vynásobme dvoma.
4. Ak je oddelenou cifrou 1, medzivýsledok vynásobme dvoma a pričítajme k nemu 1.
5. Kroky 2, 3 a 4 opakujeme tak dlho, až minieme všetky cifry daného čísla. Medzivýsledok je vtedy už konečným výsledkom.

Napríklad prevedieme číslo 110001101 do desiatkovej sústavy:

$$0.2 + 1 = 1, \quad 1.2 + 1 = 3, \quad 3.2 = 6, \quad 6.2 = 12, \quad 12.2 = 24,$$

$$24.2 + 1 = 49, \quad 49.2 + 1 = 99, \quad 99.2 = 198, \quad 198.2 + 1 = 397$$

Základné číselné operácie (sčítavanie, odčítavanie, násobenie a delenie) fungujú v dvojkovej sústave rovnako, ako v desiatkovej. Nesmieme však zabudnúť na to, že základným číslom tejto sústavy nie je 10 ale 2.

Spočítajme čísla 110011 a 11011:

<b>1 11</b>	$1 + 1 = 2$ , čo je v dvojkovej sústave 10
<b>110011</b>	0 zapíšeme a 1 ide do vyššieho rádu
<b><u>11011</u></b>	$1 + 1 + 1 = 3$ , čo je v dvojkovej sústave 11
<b>1001110</b>	1 zapíšeme a 1 ide do vyššieho rádu

Veľmi šikovným nástrojom na prevod čísel medzi dvojkovou (Bin - binárnou), osmičkovou (Oct - oktálovou), desiatkovou (Dec - dekadickou) a šestnástkovou (Hex - hexadecimálnou) sústavou je vedecká kalkulačka z prostredia Microsoft Windows. Zadáme v nej číslo, ktoré chceme previesť, myšou zvolíme cieľovú sústavu a prečítame výsledok.

---

## 17. POČÍTAČOVÁ SIETĚ – spájanie počítačov, topológia

Spojovanie počítačov začína na úrovni lokálnej siete LAN. Lokálnu počítačovú sieť tvoria aspoň dva počítače navzájom spojené prostredníctvom vhodného média najčastejšie koaxiálneho kábla, krútenej dvojlinky, optického kábla alebo bezdrôtovo pomocou infračerveného signálu. LAN sú základom každej väčšej siete, pripájajú sa na mestské a ďalej na globálnu sieť. LAN možno rozdeliť podľa viacerých kritérií.

### 1.6 Topológia

Pod pojmom topológia počítačovej siete sa väčšinou rozumie spôsob fyzického prepojenia ako sú vedené káble medzi počítačmi.

Siete sú niekedy označované ako "broadcast " siete. Voľba topológie má vplyv na rad vlastností lokálnej siete:

- rozšíriteľnosť - možnosť a jednoduchosť dopĺňovania staníc do existujúcej siete
- rekonfigurovateľnosť - možnosť modifikovať štruktúru siete pri chybe niektorých komponentov.
- spoľahlivosť - odolnosť siete voči výpadku jednotlivých komponentov, zložitosť obsluhy
- výkonnosť - využitie prenosovej kapacity média

V praxi sa stretávame s topológiou zbernicovou, hviezdicovou, stromovou a kruhovou, niektoré siete jednotlivé topológie kombinujú (napríklad ARCNet alebo dnešný Ethernet).

**Hviezda:** Stanice siete sú pripojené k centrálnemu uzlu samostatnými linkami. Centrálny uzol je označovaný ako **HUB** (rozbočovač). Signál prichádzajúci z jednej linky rozdeľuje do ostatných liniek hviezd.

**Strom** (hviezdica): Stromová topológia je prirodzeným rozšírením topológie typu hviezda. Stretávame sa s ňou u širokopásmových sietí a u sietí využívajúcich pre prenos svetlovody. Vlastnosti stromovej topológie sú podobné ako u sietí typu hviezda:

- odolnosť siete voči výpadkom jednotlivých staníc a liniek
- citlivosť na výpadky uzlov
- ľahká rozšíriteľnosť
- dvojbodové spoje

Stromové (hviezdicové) siete používajú podobné metódy ako siete **zbernicové**.

**Kruh**: U kruhových sietí sú komunikačné stanice prepojené spojmi, ktoré sú využívané iba jednosmerne. Signál vyslaný jednou stanicou je postupne predávaný ostatným staniciam kruhu. Základným prvkom stanice je krátky posuvný register a po obehu sieťou sa vracia k stanici ktorá ho vyslala.

### **SIEŤ** – typ sietí, základné pojmy

**LAN** (Local Area Network): tzv. lokálna sieť, spájajúca najviac niekoľko budov (stretáme sa s ňou najčastejšie, aj keď zväčša obsahuje aj pripojenie na nejaký druh WAN)

**Intranet**: znamená využitie najmodernejších technológií, vyvinutých pôvodne pre používanie v Internete pre podporu komunikačnej infraštruktúry vo vnútri podniku alebo inštitúcie. Intranet možno nazvať lokálnym Internetom v rámci jednej firmy.

Intranet je buď celkom izolovaný od Internetu, alebo prístup z/do Internetu je prísne kontrolovaný tzv. firewall-om.

**Firewall**: predstavuje kombináciu programových a technických zariadení, ktoré umožňujú prácu v rámci organizácie a využívanie zdrojov Internetu. Neumožní však prístup užívateľom Internetu prístup do intranetu.

Ten je niekedy umožnený iba špeciálnym skupinám užívateľov na základe hesla.

**Extranet**: je vlastne privátna sieť niekoľkých kooperujúcich organizácií, umiestnená za podnikovým firewallom.

Extranet je pojem, ktorý si tiež hľadá svoje miesto a chce vystihnúť rozširovanie sa intranetu do okolitého sveta. Extranety bezpečným spôsobom spájajú intranety rozličných firiem alebo geograficky vzdialené pobočky jednej firmy.

Výhody takéhoto prepojenia sú nesporné. Prepojenie intranetov môže viesť k novej fáze medzi podnikovej spolupráce. Na najjednoduchšej úrovni si podniky môžu zasielať relevantné dokumenty, kontakty a časové rozvrhy, aby si udržali vzájomnú synchronizáciu aktivít. Toto môže byť zdrojom neuveriteľného zvýšenia produktivity, a o to tu predsa ide !

Extranetové služby využívajú existujúcu internetovú infraštruktúru, čiže po finančnej stránke je to veľmi vhodná forma rozširovania spolupráce podnikov.

**Ethernet**: je to lokálna sieť so zbernicovou architektúrou, bola vyvinutá v polovici 70-tych

rokov firmou Xerox.

Riadenie siete odpovedá metóde CSMA/CD. Stanica, ktorá behom vysielania zistí kolíziu na médiu preruší vysielanie paketu a odošle špeciálnu postupnosť (jam). Táto postupnosť je navrhnutá tak, aby vyvolala indikáciu kolízie aj u ostatných staníc. Výsledkom je uvoľnenie média všetkými stanicami najneskôr do doby odpovedajúcemu súčtu dvojnásobku doby šírenia signálu sieťou a doby vysielania kolíznej postupnosti. Tento súčet sa označuje ako kolízny slot.

#### Architektúra počítačovej siete :

- Sieť typu **peer to peer** – najjednoduchšia počítačová sieť, všetky počítače majú rovnocenné postavenie.
- Sieť typu **klient-server**:  
Častejšie sa stretávame s počítačovou sieťou, v ktorej je jeden (môže byť aj viacero) počítač so špeciálnym postavením nazývaný server.

Na pripojenie počítača na počítačovú sieť slúži **sieťová karta**. Tá dekoduje z elektrických impulzov informáciu, ktorú počítač prijíma, alebo naopak kóduje do elektrických impulzov informáciu, ktorú počítač vysiela.

Podľa **rozsahu** možno počítačové siete rozdeliť na:

- **LAN** (local area network); obvykle v jednej budove, vzdialenosť 500 – 1000 m počet pripojených počítačov nie je obmedzený prenosová rýchlosť veľká 10 Mb/s až 1 Gb/s
- **MAM** (metropolitam area network); prepojenie viacerých budov, prípadne mestské, vzdialenosti od 1km do 20 km realizované cez optické káble, prenosová rýchlosť 10 a 100 Mb/s.
- **WAN** (wide area networks); rozsiahla sieť spájajúca mestá alebo štáty, vzdialenosť 100 – 1000 km, pri spojení sa využívajú verejné prenosové siete napr. telefónne, prenosová rýchlosť 19 – 33 kb/s.
- **GAN** (global area networks); celosvetová sieť využíva okrem iných aj prenos cez družice.

Najväčšou sieťou WAN je Internet (správne sa píše s veľkým písmenom, pretože je to jej vlastné meno); internet je každá sieť pracujúca na rovnakých princípoch ako Internet.

#### **Adresovanie v internete alebo v sieti.**

**IP adresa** - každý počítač v sieti (myslím tým aj Internet) ma pridelenú numerickú adresu zaberajúcu 32 bitov tvaru xxx.yyy.zzz.www (0..255)

Celá IP adresa sa delí na dve časti. Prvá časť je identifikátorom siete – netID , druhá identifikátorom počítača – hostID

Tie čísla ale bežnému používateľovi nič nepovedia, preto sa menia pomocou DNS na domény: adresa má v tom prípade tvar www.uzol.domena

**DNS:** (domain name system), alebo (Domain Name Server); doménová adresa a systém.

Významným medzníkom sa stal aj rok 1984. V tom čase bol zavedený pojem DNS. Je to server umožňujúci prevod doménových mien v symbolickom tvare do číselnej IP adresy a naspäť.

Na Internete používajú aj symbolické mená – doménové adresy – znakové ekvivalenty IP adresy. Jednoznačné hierarchické pridelovanie symbolických adries rieši systém DNS.

Domény majú hierarchiu: najvyššiu pozíciu majú napríklad .com, .net., .org a potom skratky krajín v ktorých je doména servera zaregistrovaná.

Počítače pripojené k internetu sú rozdelené do menších skupín domén. Domény najvyššej úrovne napr. :

- Com , podniky a komerčné organizácie
- Edu , vzdelávacie inštitúcie
- Gov , americké vládne úrady
- Int , medzinárodné organizácie
- Mil , americké ozbrojené sily
- Org , ostatné organizácie

**V sieti rozlišujeme podľa funkcie dva druhy počítačov:**

- pracovné stanice (klient)
- servery.

Pracovná stanica slúži na spracovanie údajov používateľom. Je to vlastne samostatný počítač, ktorý je pripojený do siete a tak môže využívať jej služby.

Server zabezpečuje chod siete. Realizuje funkcie siete a poskytuje ostatným používateľom svoje prostriedky (pamäťové miesto na svojich diskoch, tlačiarne, plotre...). Všeobecne môže byť v sieti ľubovoľný počet serverov a pracovných staníc. Ak je serverov v sieti viac, môžu sa navzájom v poskytovaní služieb a prostriedkov dopĺňať.

**TCP/IP:** (Transmission Control Protocol / Internet Protocol)

Je to protokol, ktorý sa používa pre komunikáciu v Internete a vyznačuje najmä tým, že:

Údaje sa po sieti prenášajú v malých častiach - paketoch. Vysielací počítač najprv rozdelí prenášané údaje na pakety, ktoré sa prenesú po sieti a prijímací počítač poskladá jednotlivé

pakety do pôvodného celku. To sa realizuje časťou protokolu TCP.

**Router:** je vlastne smerovač, prepojovacie zariadenie, ktoré pracuje už na úrovni sieťovej vrstvy.

Celá komunikácia v Internete je vlastne iba prenos paketov, čo zabezpečujú špecializované komunikačné počítače, ktoré sa nazývajú smerovače (routers). Smerovače hľadajú aktuálnu najpriechodnejšiu cestu po sieti od vysielajúceho k prijímaciemu počítaču. Pri výpadku spojenia sú schopné nájsť náhradnú cestu, ak takáto cesta existuje. Toto je realizované časťou protokolu IP.

---

### Prenosová rýchlosť :

Prenosová rýchlosť – určuje, aké množstvo dát môže počítačovou sieťou prejsť za jednu sekundu. Meriame ju v bitoch za sekundu (**bps**, **kpbs**, **Mbps**).

### Príklad:

Andrej poslal Vladovi mailom video z výletu do jeho poštovej schránky na školskom serveri. Súbor mal veľkosť 10MB. Vlado si ho chcel pozrieť na počítači v školskej sieti. Školský server je pripojený k internetu rýchlosťou 128kbps, Andrej má pripojenie s rýchlosťou 56kbps a prenosová rýchlosť v rámci školskej siete je 10Mbps.

Najmenej koľko sekúnd musel Vlado čakať na prenesenie videa z jeho poštovej schránky na lokálny počítač?

(Predpokladajme, že sa prenáša iba táto informácia a zanedbajte prevádzkové straty.)

Veľkosť súboru ....  $10\text{MB} = 10\,240\text{KB} = 10485760\text{B} = 83886080\text{b} = 81920\text{kb} = 80\text{Mb}$  (Nemusíme to takto prevádzať, zaujíma nás len Mb.)  $10\text{MB} = 10 \cdot 8 = 80\text{Mb}$

Máme zistiť, ako dlho sa prenášal súbor veľkosti 80Mb zo školského servera na Vladov počítač. Veľkosť súboru je 80Mb, prenosová rýchlosť je 10Mbps  $\Rightarrow 80 : 10 = 8$  sekúnd

Odpoveď: Vlado musel čakať 8 sekúnd, kým bolo prenesené video zo školského servera na jeho počítač.

Prenosová rýchlosť siete závisí od typu spojenia, vzdialenosti medzi počítačmi a od pravidiel komunikácie – sieťového protokolu.

---

## 18. Elektronický podpis

**Elektronický podpis** sú elektronické identifikačné údaje autora (odosielateľa) elektronického dokumentu, pripojené k nemu.

Elektronickým podpisom sa v širšom význame môže označovať aj jednoduché nešifrované uvedenie identifikačných údajov ([osobné údaje](#), ďalej názov a sídlo spoločnosti, [rodné číslo](#) atď.) na konci textu v elektronickej (digitálnej) forme, ktoré umožňuje [identifikovať](#) (teda jednoznačne určiť) označenú osobu, ale nie pravosť údajov a celistvosť podpísaného dokumentu ani [autentizáciu](#) podpísaného.

**Zaručený elektronický podpis** je elektronický podpis v podobe, kde je možné overiť pravosť dokumentov a autentifikáciu podpísaného. Toto je zaručené spravidla [kryptografickými](#) metódami. Zaručený elektronický podpis môže byť vyhotovený iba pomocou certifikovanej aplikácie, bezpečného zariadenia na vyhotovenie elektronického podpisu a kvalifikovaného [certifikátu](#). Zaručený elektronický podpis dokumentu zabezpečuje:

- [autenticitu](#) – možno overiť pôvodnosť (identitu subjektu, ktorému patrí elektronický podpis),
- [integritu](#) – možno preukázať, že po podpísaní nedošlo k žiadnej zmene, súbor nie je úmyselne alebo neúmyselne poškodený,
- nepopierateľnosť – autor nemôže tvrdiť, že podpísaný elektronický dokument nevytvoril (napr. nemôže sa zriecť vytvorenie a odoslanie výhražného listu),

Rozdiel medzi jednoduchým a zaručeným elektronickým podpisom je podobný rozdielu medzi úradne neovereným a overeným vlastnoručným podpisom, pričom možnosť, obťažnosť a spoľahlivosť písomznaleckého analýzy neovereného vlastnoručného podpisu možno prirovnať k možnosti, obťažnosti a spoľahlivosti overenia autenticity nezaručeného elektronického podpisu.

---

## 19. Počítačové vírusy

Vírusy sú v podstate veľkosťou malé a jednoduché programy, ktoré sú schopné rozmnožovať sa a vykonať činnosť pre ktorú boli naprogramované. Vírusy sa skladajú z dvoch častí:

- jedna časť slúži na rozmnožovanie
- druhá časť obsahuje kód pre vonkajší efekt

Najčastejšie sa prenášajú na programoch alebo systémových súboroch prípadne v boot sektoroch na disketách. V poslednej dobe je veľkým "nebezpečenstvom" internet, kde vírusy dokážu samovoľne obiehať svet a spôsobujú veľké škody. Prvé vírusy boli napísané skôr pre pobavenie užívateľa. Tieto vírusy boli pomerne neškodné. Postupom času začali vírusy aj NIČIŤ.

Z hľadiska nebezpečnosti, by sme mohli víry rozdeliť takto:

- vírusy ktoré napádajú a ničia len spustiteľné súbory
- vírusy ktoré sú schopné zničiť údaje na disku jeho zablokovaním, prekódovaním alebo naformátovaním
- vírusy ktoré modifikujú údaje bez vedľajších príznakov
- vírusy ktoré ničia hardware

### Vírusy napádajúce programy



Vírusy, ktoré patria do tejto skupiny sú v podstate neškodné, pretože jediná vec ktorú dokážu, je prepísanie používaných programov. Takto postihnutí súbor už väčšinou nespustíme, ale väčšinou stačí postihnúť program vymazať a nainštalovať znovu.

### **Vírusy ničiace údaje**

Sú to dosť nebezpečné vírusy. Ďalej ich môžeme rozdeliť na:

- vírusy ktoré napádajú a modifikujú FAT tabuľku
- vírusy ktoré menia tabuľku partícií
- vírusy ktoré formátujú disk alebo zablokujú prístup k nemu
- vírusy ktoré prekódujú obsah disku a po ich odstránení nemožno údaje prečítať

Ak sa liečenie antivírusovým programom nepodarí prichádzame o data uložené na disku. Takejto katastrofe sa dá predísť ak máme aspoň nejaké zálohy.

### **Vírusy modifikujúce údaje**

Tento typ vírusov len čaká v počítači a sem tam zmení nejaký údaj. Niektoré ktoré pracujú podľa určitého algoritmu, tam je ešte šanca vrátiť údaje do pôvodného stavu, no existujú aj také, kde nie je možné zistiť ktoré súbory boli napadnuté. Je nepríjemné, že si ani nemôžeme byť istý tým, že sú zálohy správne.

### **Vírusy ničiace hardware**

Do tejto kategórie patria vírusy, ktoré vznikli vďaka starostlivosti o užívateľa. Niekedy bolo pri skladaní počítača nutné nastavovať všetko ručne. Dnes sa skoro všetko nastavuje automaticky a zapíšu sa do pamäte príslušného zariadenia. Takže vírusy môžu nastavenia hardware zmeniť alebo zmazať. S týmto úmyslom bolo vytvorených niekoľko vírusov, ktoré modifikujú BIOS.

Vírusy dokážu zničiť hardware aj vysielaním signálov na zariadenia tak rýchlo po sebe, že tie sa v snahe o vykonanie prehrejú a zničia.

Vírusy môžeme ďalej rozdeliť na:

### **Trójske kone**

Trójske kone po preniknutí do cudzieho systému len ticho pozorujú systém a čakajú na svoju chvíľu. Trójske kone dokážu zistiť heslo, vymazať konkrétny program, nakradnúť údaje. Tieto vírusy sú skôr doménou počítačových sietí ako samostatných počítačov. Často krát trójske kone slúžia na vypustenie nového vírusu.

## **Bootovacie**

Infikujú partition table (tabuľku rozdelenia), alebo častejšie boot sector (zavádzači sektor), čím si zabezpečia spustenie ešte pred zavedením samotného operačného systému. Originálny boot sector (ktorý musí byť zachovaný pre korektné zavedenie operačného systému) ukladajú buď na niektorý voľný sektor na 0. stope pevného disku, alebo na ľubovoľný iný sektor z dátovej oblasti pevného disku, pričom ho označia za vadný, aby nedošlo k jeho prepísaniu.

## **Makrovírusy**

Ide o programy naprogramované v jazyku na tvorbu makier v textovom procesore, alebo tabuľkovom kalkulátore a vložené do takého dokumentu (prvýkrát v roku 1989 v kalkulátore Lotus 1-2-3). Väčšinou ide o makrá programu Microsoft Word, ktoré systém vykonáva pri každom otvorení dokumentu (tzv. auto makrá), AutoExec, AutoOpen, FileSaveAs, FilePrint, FileExit. Infikovaná je najčastejšie šablóna NORMAL.DOT. Kvalitný programovací jazyk im umožňuje replikáciu, ale je diskutabilné, či ich radiť medzi vírusy, pretože neobsahujú inštrukcie procesora.

## **Súborové**

Je to najrozšírenejšia skupina vírov. Infikujú EXE, COM, OVL, BIN, STS, OBJ, DLL súbory a niekedy aj keď sú uložené v komprimovaných archíve.

## **Nerezidentné**

Vírus sa po spustení infikovaného programu replikuje, najčastejšie do súborov v danom adresári, a predajú riadenie infikovanému programu

## **Rezidentné**

Tieto vírusy ostávajú v operačnej pamäti počítača aj po ukončení vykonávania infikovaného programu použitím mechanizmu TSR (terminate and stay resident)

### Ako zabrániť nákaze.

Hovorí sa, že dôležitejšie ako samotné liečenie je prevencia.

Zabrániť nákaze môžeme takto:

- nepoužívame cudzie a nenaformátované diskety
- neotvárame neznámu poštu s prílohami
- pravidelne zálohujeme údaje
- nenechávame pri štarte počítača disketu v mechanike
- snažme sa používať originálny software
- čo najčastejšie aktualizujeme svoj antivírus a Windows

## Antivírusy

Každý antivírus by mal dokázať toto:

- 1.nájsť vírus ukrytý v pamäti, na disku alebo vonkajšom pamäťovom zariadení (CD-čku, USB kľúči)
- 2.dokázať ho odstrániť, vyliečiť
- 3.odstrániť napáchané škody
- 4.mal by byť rýchly aby príliš nespomaľoval počítač

Ďalej by mal byť schopný zapnúť ochranu počítača počas činnosti a byť neustále v pamäti "strážiť" počítač pred rizikovými operáciami. Väčšina dokáže aj zálohovať citlivé časti disku a CMOS. Štandardom je používanie kontrolných súčtov CRC. Každý vír po zapísaní zmení kód programu. Metóda kontrolných súčtov je založená na sčítaní číselnej hodnoty znakov tvoriacich súbor. Zmena CRC súčtu nemusí vždy znamenať vírus, niektoré programy si ho menia samy. Pri bežnom hľadaní (scanovanie) sa prezerajú súbory a porovnáva sa kód s kódom evidovaných vírusov. Nevýhodou scanovania je, že dokáže nájsť iba evidované vírusy. Okrem toho existujú aj vírusy ktoré počas svojej existencie menia svoj kód (polymorfne). V snahe o vyriešenie tohto problému tvorcovia antivírusov do svojich systémov heuristickú analýzu, ktorá dokáže odhaliť aj neznáme vírusy, ktoré sa prejavujú typickými inštrukciami prepracovanejšia heuristická analýza dokáže krok za krokom simulovať činnosť programu. Okrem polymorfných vírusov existujú aj stealth vírusy, ktoré zmanipulujú operačný systém tak, že dokáže skryť svoju existenciu pred antivírusom.

---