CRC32 (Cyclic Redundancy Check)

CRC32 je kontrolní kód, který slouží k ověření, zda jsou data (soubor nebo síťový paket) kompletní a nepoškozená. Funguje na principu polynomiálního dělení, jehož výsledkem je pevné 32bitové číslo (8 hexadecimálních znaků), které slouží jako „otisk“ daných dat.

Jak CRC32 funguje v praxi?

Celý proces probíhá ve třech krocích:

```
1. **Výpočet u zdroje:** Před odesláním souboru (nebo jeho uložením) algoritmus projde všechna data a vypočítá jejich CRC32 kód (např. ''A1B2C3D4''). Tento kód se přibalí k datům.
2. **Přenos/Uložení:** Data putují sítí nebo se zapisují na disk.
3. **Kontrola u příjemce:** Příjemce vezme doručená data a znovu na nich spustí stejný výpočet.
   * Pokud se nový výsledek shoduje s kódem ''A1B2C3D4'', data jsou v pořádku.
   * Pokud se liší (byť jen o jeden bit), znamená to, že data byla cestou poškozena.
```

Klíčové vlastnosti

- **Rychlost:** Algoritmus je navržen tak, aby byl extrémně rychlý a mohl se snadno implementovat do hardwaru (např. do síťových karet).
- **Efektivita:** 32bitový kód (4 bajty) je dostatečně malý, aby nezabíral místo, ale zároveň dostatečně velký, aby zachytil většinu běžných chyb (pravděpodobnost neodhalené chyby je velmi nízká).
- **Detekce, nikoliv oprava:** Na rozdíl od parity v ECC RAM, CRC32 chybu pouze **detekuje**. Pokud zjistí poškození, musí si systém vyžádat data znovu (např. prohlížeč znovu stáhne poškozený paket).

Kde se s CRC32 setkáte?

Oblast	Použití
Archivace	Soubory ZIP, RAR a 7z ukládají CRC32 pro každý soubor. Pokud vidíte chybu „CRC Error“, soubor je poškozen.

Oblast	Použití
Sítě	Ethernet a Wi-Fi používají CRC k ověření, zda se paket cestou vzduchem nebo kabelem „nerozsypal“.
Úložiště	Tabulka GPT používá CRC32 k ochraně integrity informací o oddílech disku.
Programování	Rychlé porovnávání souborů (pokud mají různé CRC, jsou zaručeně jiné).

CRC32 vs. Kryptografické haše (MD5, SHA-256)

Je důležité neplést si CRC32 se zabezpečením.

- **CRC32** je určeno proti **náhodným chybám** (šum na lince, vadný sektor disku). Je velmi snadné vytvořit jiný soubor, který bude mít stejné CRC32 (tzv. kolize).
- **SHA-256** (a další haše) jsou určeny proti **úmyslnému pozměnění**. Jsou mnohem delší, pomalejší na výpočet a prakticky nemožné je zfalšovat.

Matematický princip (Zjednodušeně)

Data jsou vnímána jako jedno obrovské binární číslo. Toto číslo se vydělí pevně daným „generujícím polynomem“. Zbytek po tomto dělení (modulo) je výsledné CRC. Je to podobné, jako byste kontrolovali součet nákupu tím, že se podíváte jen na poslední cifru výsledné ceny.

Související pojmy: Parita, GPT, ZIP, Algoritmus, Binární soustava, Hexadecimální soustava.