Hashování (Digitální otisk dat)

Hashování je proces, při kterém vložíte na vstup data (např. slovo „Ahoj“ nebo celé video) a hashovací algoritmus (funkce) vyplivne unikátní řetězec znaků (např. ''a3f5b...'). Hashování je **jednosměrná operace** – z výsledného hashe nelze zpětně získat původní data.

Klíčové vlastnosti dobrého hashe

Aby byla hashovací funkce užitečná v informatice a bezpečnosti, musí splňovat tato pravidla:

- **Determinismus:** Pro stejný vstup musí vždy vyjít stejný hash.
- **Rychlost:** Výpočet hashe musí být velmi rychlý.
- **Lavinový efekt:** I minimální změna na vstupu (např. změna tečky na čárku) musí vést k totálně odlišnému hashi.
- **Odolnost proti kolizím:** Je prakticky nemožné najít dvě různá vstupní data, která by měla stejný hash.
- **Nezvratnost:** Z hashe nelze matematicky odvodit původní obsah.

Hlavní využití hashování

1. Bezpečné ukládání hesel

Služby by nikdy neměly ukládat vaše hesla v čitelném textu. Místo toho uloží pouze **hash vašeho hesla**.

- Když se přihlašujete, systém zahashuje vámi zadané heslo a porovná výsledek s hashem v databázi.
- Pokud útočník ukradne databázi, získá jen nepoužitelné hashe, nikoliv skutečná hesla.

2. Kontrola integrity dat

Stahujete-li velký soubor, autor často uvádí jeho hash (např. MD5 nebo SHA-256). Po stažení můžete soubor zahashovat sami. Pokud se váš hash shoduje s tím od autora, máte jistotu, že se soubor cestou nepoškodil a nikdo do něj nevložil virus.

3. Digitální podpisy a Blockchain

Hashování je základem pro digitální podpisy a technologii kryptoměn. V Bitcoinu se například hashuje celý blok transakcí, čímž se nezaměnitelně propojuje s blokem předchozím.

Nejčastější hashovací algoritmy

Algoritmus	Stav	Použití
MD5	**Zastaralý**	Již není bezpečný, používá se jen pro rychlou kontrolu integrity (ne pro hesla).
SHA-1	**Zastaralý**	Podobně jako MD5, již byl matematicky prolomen.
SHA-256	**Bezpečný**	Standard v kryptografii, těžba Bitcoinu, certifikáty webů.
bcrypt / Argon2	**Excelentní**	Speciálně navrženy pro ukládání hesel (jsou záměrně pomalé, aby bránily útokům hrubou silou).

Rozdíl: Hashování vs. Šifrování

Mnoho lidí tyto pojmy plete. Hlavní rozdíl je v **účelu**:

- **Šifrování** je **dvousměrné**. Chceme data schovat a později je zase přečíst (potřebujeme klíč).
- **Hashování** je **jednosměrné**. Chceme vytvořit unikátní identifikátor dat, aniž bychom je nutně chtěli „odemykat“.

Co je to "Sůl" (Salt)?

V souvislosti s hashováním hesel se používá tzv. **sůl**. Je to náhodný řetězec znaků, který se přidá k heslu předtím, než se zahashuje. Tím se zajistí, že i když mají dva uživatelé stejné heslo „12345“, jejich výsledné hashe v databázi budou vypadat úplně jinak. To chrání databázi před útoky pomocí tzv. Duhových tabulek (Rainbow Tables).

Související pojmy: Digitální podpis, Šifrování, RSA, AES, Blockchain, MD5, SHA-256, Sůl (Salt).