MD5 (Message-Digest algorithm 5)

MD5 vyvinul v roce 1991 Ronald Rivest jako nástupce starší verze MD4. Její hlavní úlohou je vzít libovolně velký soubor a vytvořit z něj unikátní digitální otisk o pevné délce.

Typický MD5 hash vypadá takto: `7e58d63b60197ceb55a1c487989a3720`

Hlavní využití (Dříve a dnes)

1. Kontrola integrity souborů (Stále běžné)

Pokud si stahujete velký soubor (např. instalaci Linuxu), autor často u odkazu uvádí i „MD5 Checksum“. Po stažení můžete soubor prohnat MD5 kalkulačkou. Pokud se váš kód shoduje s kódem autora, soubor je v pořádku. Pokud se liší, soubor byl poškozen nebo do něj někdo zasáhl.

2. Ukládání hesel (Dnes zakázáno!)

V minulosti webové stránky ukládaly hesla jako MD5 hashe. Dnes je to považováno za hrubou chybu, protože MD5 je extrémně rychlá a náchylná k útokům pomocí tzv. Duhových tabulek (Rainbow Tables).

Proč je MD5 považována za nebezpečnou?

Základem bezpečného hashe je odolnost proti **kolizím**. Kolize nastává, když pro dva různé vstupy vyjde stejný hash.

- **Kryptografický průlom:** V roce 2004 bylo prokázáno, že v MD5 lze kolize vytvořit velmi snadno.
- **Útok:** Útočník může vytvořit dva různé soubory (např. běžný dokument a dokument s virem), které mají identický MD5 hash. Pokud se uživatel spoléhá jen na MD5, nepozná, že mu byl soubor podstrčen.
- **Výkon:** Moderní grafické karty dokáží vyzkoušet miliardy MD5 kombinací za sekundu, což činí prolamování hesel otázkou okamžiku.

Srovnání MD5 s nástupci

Algoritmus	Délka hashe	Bezpečnost	Použití
MD5	128 bitů	**Nulová**	Pouze kontrola integrity.
SHA-1	160 bitů	**Nízká**	Zastaralé, nahrazuje se.
SHA-256	256 bitů	**Vysoká**	Standard (HTTPS, Bitcoin).
SHA-3	224-512 b	**Vysoká**	Nejmodernější standard.

Praktická ukázka lavinového efektu

MD5 je citlivá na sebemenší změnu. Podívejte se, jak se změní výsledek při změně jediného písmene:

* Vstup: Pes

- Hash: `63840784407b9736f1c402a5e4b77f88`

* Vstup: pes (malé p)

- Hash: `3763f350c2688975949d0b50337373f7`

Související pojmy: Hashování, SHA-256, Digitální podpis, Integrita dat, Kolize, Šifrování.