SHA-256 (Secure Hash Algorithm 256-bit)

SHA-256 je kryptografická hashovací funkce, která z libovolně velkého vstupu vytvoří unikátní digitální otisk o fixní délce **256 bitů**. Tento otisk se obvykle zapisuje jako řetězec 64 šestnáctkových znaků.

Na rozdíl od svého předchůdce MD5 nebo SHA-1 nebyl algoritmus SHA-256 dosud úspěšně prolomen a je považován za bezpečný standard pro ochranu nejcitlivějších dat.

Klíčové technické parametry

- **Délka výstupu:** 256 bitů (32 bajtů).
- **Počet kombinací:** Existuje 2^{256} možných výsledných hashů. To je tak nepředstavitelně velké číslo, že pravděpodobnost náhodného nalezení dvou stejných hashů (kolize) je prakticky nulová.
- **Jednosměrnost:** Z hashe SHA-256 je absolutně nemožné rekonstruovat původní data.

Typický SHA-256 hash vypadá takto:
`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`

Hlavní využití SHA-256

1. Kryptoměny (Bitcoin)

SHA-256 je srdcem **Bitcoinu**. Používá se v procesu zvaném „těžba“ (Mining) k vytváření důkazů o práci (Proof of Work) a k propojení jednotlivých bloků v blockchainu. Každý blok v sobě nese hash předchozího bloku, což zajišťuje neměnnost celé historie.

2. Digitální certifikáty a SSL/TLS

Většina webových stránek používá protokoly HTTPS, kde digitální certifikáty využívají SHA-256 k potvrzení pravosti identity serveru. Váš prohlížeč si tak může být jistý, že komunikuje se správnou bankou nebo e-shopem.

3. Integrita softwaru

Vývojáři velkých projektů (např. distribucí Linuxu) poskytují SHA-256 otisky ke staženým obrazům

disků. Je to modernější a bezpečnější náhrada za zastaralé MD5.

Srovnání bezpečnosti: MD5 vs. SHA-256

Vlastnost	MD5	SHA-256
Rok vydání	1991	2001
Délka otisku	128 bitů	256 bitů
Odolnost proti kolizím	**Prolomena** (velmi slabá)	**Vysoká** (dosud neprolomena)
Rychlost výpočtu	Extrémně vysoká (slabina)	Vysoká, ale náročnější než MD5
Vhodné pro hesla	Ne (příliš snadno se prolamuje)	Ano (v kombinaci se „solí“)

Budoucnost: Je SHA-256 ohrožena?

Ačkoliv je SHA-256 dnes považována za bezpečnou, kryptografové již připravili standard **SHA-3**, který využívá úplně jinou vnitřní strukturu. To je pojistka pro případ, že by byla v matematickém principu SHA-2 nalezena skrytá slabina.

Rovněž se spekuluje o vlivu **kvantových počítačů**. Očekává se, že SHA-256 bude vůči nim relativně odolná (na rozdíl od asymetrického šifrování RSA), pouze bude nutné časem přejít na ještě delší variantu, například SHA-512.

Související pojmy: Hashování, MD5, Blockchain, Bitcoin, RSA, Digitální podpis, SSL/TLS.