SHA-4 (Budoucnost hashovacích funkcí)

SHA-4 představuje další evoluční krok v rodině Secure Hash Algorithms. Zatímco SHA-2 je založen na struktuře Merkle-Damgård a SHA-3 na konstrukci „Sponge“ (houba), u SHA-4 je kladen důraz na **odolnost proti kvantovým počítačům** a extrémní efektivitu na zařízeních s omezeným výkonem (IoT).

Hlavní kandidát: Algoritmus Ascon

V únoru 2023 NIST oznámil, že rodina algoritmů **Ascon** byla vybrána pro standardizaci lehké kryptografie. Očekává se, že prvky tohoto algoritmu se stanou základem pro to, co budeme nazývat SHA-4.

Klíčové vlastnosti:

- **Lehkost:** Navržen pro čipy v chytrých kartách, senzorech a IoT zařízeních, kde mají klasické SHA-2/3 příliš vysokou spotřebu energie.
- **Permutační založení:** Podobně jako SHA-3 využívá iterativní permutace, ale s menšími nároky na paměť.
- **Integrované šifrování:** Ascon není jen hashovací funkce, ale umožňuje i tzv. autentizované šifrování (AEAD).

Proč potřebujeme SHA-4?

S příchodem nových technologií narážejí stávající standardy na své limity:

```
1. **Kvantová hrozba:** Kvantové počítače by teoreticky mohly oslabit současné hashovací funkce (Groverův algoritmus). SHA-4 je navrhován tak, aby měl dostatečnou délku stavu pro zachování bezpečnosti i v post-kvantové éře.
2. **Internet věcí (IoT):** Standardy jako SHA-3 jsou pro malá zařízení příliš komplexní. SHA-4 cílí na co nejmenší počet hradel v křemíku.
3. **Rychlost:** Moderní procesory vyžadují algoritmy, které lze lépe paralelizovat.
```

Srovnání rodin SHA

Standard	Struktura	Rok vydání	Hlavní vlastnost
SHA-1	Merkle-Damgård	1995	Dnes již prolomen (nebezpečný).
SHA-2	Merkle-Damgård	2001	Standard (SHA-256, SHA-512). Velmi rozšířený.
SHA-3	Sponge construction	2015	Zcela jiný design než SHA-2, vysoká bezpečnost.
SHA-4 (Ascon)	Lightweight Permutation	~2023+	Zaměření na IoT a efektivitu.

Praktické využití v budoucnu

Předpokládá se, že SHA-4 se stane standardem pro:

- **Zabezpečení kritické infrastruktury:** Chytré sítě (smart grids) a autonomní vozidla.
- **Blockchain nové generace:** Kde je vyžadována odolnost proti kvantovým útokům.
- **Digitální podpisy:** V systémech s nízkým napájením (např. bezkontaktní platby).

Související pojmy: Hash, Kryptografie, SHA-3, NIST, IoT, Kvantový počítač, Blockchain.