Zgostitveni algoritmi

(message digest, cryptographic checksum, cryptographic hashcode, one-way hash functions)

Zgostitveni algoritmi preslikajo poljubno dolg niz znakov v blok konstantne dolžine, ki skoraj enolično določa vhodni niz znakov. Od
zgostitvenega algoritma pričakujemo, da:

- je nemogoče najti dve različni sporočili, ki bi ju preslikal v isti blok;
- isto sporočilo vedno preslika v enak blok;
- iz zgostitvenega bloka ni mogoče restavrirati sporočila;
- vsaka sprememba v sporočilu povzroči opazno spremembo v zgostitvenem bloku.

Pri imenu smo v dilemi - mogoče bi bilo bolje reči razpršitveni algoritmi, ker na nek način razpršijo informacijo. Po drugi strani pa je
rezultat običajno krajši od vhoda. Ne smemo pa jih zamenjevati s kompresijskimi postopki (zip in podobnimi).

Postopek se običajno začne tako, da konec vhodne datoteke dopolnimo do polnega bloka (padding). Potem zaporedoma obdelujemo
bloke:

Rezultat mora enolično identificirati datoteko in to uporabljamo pri digitalnih podpisih. Kako dolg pa naj bi bil povzetek, da bo drugačen
za vsako datoteko na tem svetu? Na prvi pogled se nam zdi nemogoče, da bi n.pr. 128 bitov omogočalo toliko različnih kombinacij.
Izračunajmo: 2128 = 10 38
Starost vesolja ocenjujejo na 1010 let. Torej lahko vsako leto ustvarimo 1028 datotek.

Najpogosteje omenjeni so

- MD2 (Message Digest), MD4 in MD5

Vse je razvil Ronald Rivest. MD2 najprej preuredi tekst tako, da je njegova dolžina v bajtih deljiva s 16. Potem izračuna 16-bajtni
checksum in ga doda prvotnemu tekstu, na ta vmesni rezultat pa potem izvede matematične operacije na zaporednih vhodnih blokih.
Rezultat je 128 bitov dolg. MD2 je zelo počasen algoritem, zato je bil razvit MD4. Vendar je bil ta tarča nekaterih napadov, zato se zdaj
najbolj uporablja MD5, ki je izboljšana verzija MD4, vendar malo bolj počasen.

- SHA (Secure Hash Algorithm) - zdaj verzija SHA-1

Razvili sta ga organizaciji NIST in NSA. Tekst preslika v blok dolžine 160 bitov. Je precej podoben MD4, razlike pa pomenijo podobne
izboljšave kot pri MD5. Zenkrat velja za najboljši zgostitveni algoritem.

- HAVAL

To je verzija MD5, ki so jo razvili Yuliang Zheng, Josef Pieprzyk in Jennifer Seberry. Lahko se izbere število ponovitev algoritma in
dolžino rezultata (od 92 do 256 bitov).

- SNEFRU

je razvil Ralph Merkle, rezultat je ali 128 bitov ali 256 bitov, možno je nastaviti število ponovitev notranjega algoritma. Avtor priporoča
8-kratno ponovitev, vendar je v tem primeru počasnejši od MD5 oziroma HAVAL.

Večinoma uporabljamo MD5. Odkar je izšel članek Hansa Dobbetina (maj 1996), kjer je dokazal, da za poseben primer dveh nizov

bitov, ki se razlikujeta v enem bitu, dobimo isti povzetek z MD5, so v nekaterih produktih že zamenjali MD5 s SHA.

URL: http://www.sigov.si/tecaj/kripto/kr-zgo.htm