MAIŠOS ALGORTIMŲ PALYGINIMAS

Hash alogoritmas – funkcijų seka, paimanti bet kokio ilgio seką ir grąžina fiksuoto ilgio unikalią ženklų seką, vadinamą Hash reikšme.

Maišos algortimų savybės:

• kiekviena *Hash* reikšmė yra unikali ir tai pačiai žinutei visuomet ta pati. Pvz. „stalas“ visuomet bus paverčiama ta pačia ženklų seka - 193f70f3c0a6af82ca73ce1620bbad6096409817 (SHA-1).

• vienpusė funkcija. Pagal Hash reikšmę h turėtų būti sunku rasti žinutę m: h = hash(m);

• sunku rasti skirtingas žinutes m_1 ir m_2, kurių Hash reikšmės yra tokios pačios hash(m_1) = hash(m_2).

SHA-1 ir SHA-2 algoritmai

SHA-1 ir SHA-2 algoritmai paremti Merkle–Damgård konstrukcija: šifruojama M žinutę, kuri yra *l* bitų ilgio. Čia *l* gali įgyti reikšmes $0 <= l < 2^{64}$.

Šis kodas yra skaičiuojamas taip:

• pradinis tekstas suskirstomas į N blokų po 512 bitų (64 baitus) (SHA-512 – į blokus, po 128 baitus (1024 bitus));

• jei paskutiniame M_n bloke trūksta informacijos iki reikiamo bitų skaičiaus, bloko gale pridedamas 1 ir tiek 0, kad būtų užpildytas blokas paliekant 64 bitus pradinio teksto ilgio išsaugojimui bitais;

• naudojamos funkcijos f_0, f_1, … f_{79}. Kiekviena funkcija operuoja penkiais 32 bitų kintamaisiais a, b, c, d ir e ir grąžina vieną 32 bitų žodį. (SHA-1 algoritmui). SHA-256 algoritmui: naudojamos funkcijos f_0, f_1, … f_{63} (SHA-512 naudojamos funkcijos kaip ir SHA-1 algoritmui). Kiekviena funkcija operuoja aštuoniais 32 bitų kintamaisias a, b, c, d, e, f, g ir h. Tuomet kiekvienam tarpinį maišymo rezultatą laikantiems žodžiams yra nustatoma pradinė reikšmė. Ši reikšmė yra nustatyta iš anksto ir kiekvienam algoritmui yra vis kitokia.

Čia prasideda maišymo procesas. Rezultatas SHA-1– 160 bitų ilgio Hash reikšmė, išreiškiama 40 simbolių šešioliktainiu formatu, 224 (SHA-224) arba 256 (SHA-256) bitų ilgio Hash reikšmė.

Buvo rasti analitiniai būdai SHA-1 algoritmo nulaužimui, todėl sugeneruotas reikšmes galima laisvai “nulaužti”.

SHA-2 yra gana plačiai naudojamas. Labiausiai žinomi protokolai, kuriuose, galima pasirinkti SHA-2 naudojimą yra: TLS, SSL, PGP, SSH, S/MIME, IPSec ir BitCoin. Pirmąjį ir antrąjį SHA algoritmus naudoti galima su tais pačiais protokolais, tereikia tik pasirinkti tinkamą algoritmą kiekvienai situacijai individualiai.

SHA-2 turi dar pagrindines 2 Hash funkcijas SHA-256 ir SHA-512 bei 4 išvestines: SHA-224, SHA-384, SHA-512/224, SHA-512/256.

SHA-3 algoritmas

SHA-3 naudoja *Sponge* konstrukciją. Šiame algoritme pranešimo blokai yra apdorojami į pradinę bitų būseną, naudojantis XOR operacija. Didžiausias pavyzdys apima 5 × 5 dimensijos 64 bitų ilgio žodžių masyvą, iš viso turintį 1600 bitų. Viena pagrindinių algoritmo dalių yra blokų perstatymas. Toks keitinys apibrėţtas bet kokio laipsnio dviejų žodžių dydžiui, $w = 2^l$ bitų.

Pagrindu gali būti laikomas 5 × 5 × w bitų masyvas. Tarkime a [i,j,k] yra įvesties duomenų bitai, išdėstyti taip, kad mažiausiai reikšmingas bitas eina pirmas, o kiti išdėstyti didėjimo tvarka. Visos aritmetinės operacijos atliekamos laipsniu 5 arba w. Pagrindinė bloko perstatos funkcija turi 12 + 2l iteracijų penkiuose subcikluose, kurių kiekvienas individualiai yra labai paprastas. Keccak algoritmo naudojama Sponge konstrukcija, „įsiurbia“ pranešimą į maišos funkciją duotu momentu ir po to grąžina rezultatą. Tam, kad paimtų r bitų duomenų, yra atliekama XOR operacija su pirmaisiais bloke esančiais bitais ir po to atliekama bloko perstata.

Algoritmas yra saugus – kuo daugiau ciklo skaičių, tuo saugumas yra didesnis. Pranešimo išdėstymo schema nėra sudėtinga. Rodiklis r buvo pakeltas iki saugumo limito, o ne apvalinamas iki artimiausio dvejeto laipsnio.

Algoritmų palyginimas:

<table>
<tr><th colspan="2">Algoritmas / jo variantas</th><th>Sugeneruojama reikšmė (bitais)</th><th>Vidinė maišos suma (bitais)</th><th>Bloko dydis (bitais)</th><th>Maks. Įvesties dydis (bitais)</th><th>Iteracijų skaičius</th></tr>
<tr><td>SHA-1</td><td>-</td><td>160</td><td>160 (5 x 32)</td><td>512</td><td>2^{64}-1</td><td>80</td></tr>
<tr><td rowspan="2">SHA-2</td><td>SHA-224</td><td>224</td><td rowspan="2">256 (8 x 32)</td><td>512</td><td>2^{64}-1</td><td>64</td></tr>
<tr><td>SHA-256</td><td>256</td><td>512</td><td>2^{64}-1</td><td>64</td></tr>
<tr><td rowspan="2">SHA-3</td><td>SHA3-256</td><td>256</td><td rowspan="2">1600 (5x5 x 64)</td><td>1088</td><td rowspan="2">Neribota</td><td rowspan="2">24</td></tr>
<tr><td>SHA3-512</td><td>512</td><td>576</td></tr>
</table>