**Maišos funkcijos**

**Maišos funkcija** (*hash function*) vadiname funkciją, kuri bet kokio baigtinio ilgio ženklų eilutei priskiria *fiksuoto ilgio* eilutę. Maišos funkcijos naudojamos ne tik informacijos vientisumo patikrinimui, bet ir dokumento santraukai gauti skaitmeninio parašo schemose, slaptažodžių saugojimui, paieškos raktų formavimui duomenų bazėse ir panašiai.

Pranešimo vientisumui užtikrinti naudojama **pranešimo** **santrauka** (*message digest*, kartais dar vadinama *Modification Detection Code* (*MDC*)). Pranešimo santrauka skaičiuojama, naudojant maišos funkciją. Pranešimo santrauka vadiname maišos funkcijos reikšmę.

Pavyzdys:

Tekstas – "*Informacijos saugumas“*

MD5 (128 bitai): 5ccb2201a7ee633d2b2dc1ff527d4c79

SHA-1 (160 bitų): 09035a1b2703a81b7a86e1abe9965b5756666591

SHA-256 (256 bitai): 7765253a2cf3996d41c2a54af094a80bfcb8f9c4b4b8d4352c3e1ab8e3c7bbfb

Maišos funkcijos yra *determinuotosios*, t. y. ne atsitiktinės.Skaičiuojant maišos reikšmę tai pačiai įvesčiai kelis kartus, visada bus gaunamas tas pats rezultatas.Kadangi galimų įvesčių yra daugiau, negu galimų išvesčių, tai maišos funkcijos nėra *injektyvios*. Gali būti, kad skirtingoms įvestims maišos reikšmės bus vienodos. Tai vadinama **sutapimu** (kolizija, *collision*).

Kadangi maišos funkcijos yra žinomos viešai, tai bet kas gali apskaičiuoti jų reikšmes. Todėl santrauka turi būti perduodama *saugiu kanalu*, nes kitaip atakuojantysis galės pakeisti ir pranešimą, ir santrauką, apskaičiavęs pakeisto pranešimo maišos reikšmę.

Be to, vientisumui užtikrinti bet kokios maišos funkcijos netinka. Pavyzdžiui, tarkime, kad maišos funkcija yra tokia, kad turint pranešimą ir jo santrauką, nesunkiai galima rasti kitą pranešimą su tokia pačia santrauka. Tada atakuojantysis galės pakeisti pranešimą į kitą pranešimą, ir gavėjas to nepastebės. Vientisumui užtikrinti reikia naudoti *kriptografines maišos funkcijas*.

**Kriptografine maišos funkcija** vadiname maišos funkciją, kuri yra:

**vienakryptė** (*preimage resistant*, *one-way*): pranešimo santrauką apskaičiuoti yra lengva, o turint santrauką rasti atitinkamą pranešimą yra skaičiavimų prasme neįmanoma (*computationally infeasible*),

**atspari sutapimams** (*2-nd preimage resistant*, *weakly collision resistant*): turint pranešimą, skaičiavimų prasme neįmanoma rasti dar vieną pranešimą su ta pačia santrauka,

**labai atspari sutapimams** (*collision resistant*, *strongly collision resistant*):skaičiavimų prasme neįmanoma rasti sutapimą, t. y. du pranešimus su ta pačia santrauka.

**Lavinos efektas**

Pageidautina, kad kriptografinė maišos funkcija tenkintų savybę, vadinamą **lavinos efektu** (*avalanche* *effect*). Taip kriptografijoje vadinama pageidaujama kriptografinių algoritmų (paprastai blokinių kriptosistemų ir kriptografinių maišos funkcijų) savybė, kai nežymiai pakeitus įvestį (pavyzdžiui, pakeitus vos vieną bitą), išvestis pasikeičia žymiai (pavyzdžiui, pusė visų išvesties bitų pasikeičia).

**Pavyzdys**. Žodžiai *Taisyklė* ir *taisyklė* skiriasi tik vienu bitu, o jų MD5 reikšmės labai skiriasi:

T – 0x54 – 0101 0100

t – 0x74 – 0111 0100

*Taisyklė*: MD5: f26ad7627a11f62e559a9a6516dd2392

*taisyklė*: MD5: f0517727eaba12da46385b6b9418ff30

**Dažniausiai naudojamos maišos funkcijos**

**MD5** (*Message-Digest algorithm* 5)

* 1992 m. sukūrė Ron Rivest.
* Santraukos 128 bitų ilgio.
* Naudojama tokiuose plačiai naudojamuose protokoluose ir programose, kaip TLS ir SSL, SSH, PGP, S/MIME, IPsec.
* UNIX šeimos operacinėse sistemose plačiai naudojama slaptažodžių santraukoms saugoti.
* Įveikta 2004 metais (surasti sutapimai).
* Iki tol plačiai naudota, ir vis dar naudojama.
* Neberekomenduojama naudoti.

**SHA-1** (*Secure Hash Algorithm* 1)

* SHA 1993 m. sukūrė JAV nacionalinė saugumo agentūra (*National Security Agency,* *NSA*). 1995 m. paskelbtas naujas variantas SHA-1, kuriame ištaisyta SHA buvusi klaida. Senasis variantas dabar dažnai vadinamas SHA-0.
* JAV paskelbta standartu.
* Santraukos 160 bitų ilgio.
* Naudojama tokiuose plačiai naudojamuose protokoluose ir programose, kaip TLS ir SSL, SSH, PGP, S/MIME, IPsec.
* Naudojama DSS (*Digital Signature Standard*) elektroninio parašo schemoje.
* Kol kas neįveikta, bet 2005 metais rasta teorinių spragų.

**SHA-224, SHA-256, SHA-384, SHA-512**

* Visos kartu vadinamos **SHA-2** maišos funkcijų šeima.
* 2001 m. sukūrė JAV nacionalinė saugumo agentūra.
* 2002 m. JAV paskelbta standartu.
* Santraukos tokio ilgio bitais, koks nurodytas maišos funkcijos pavadinime.
* Kol kas nėra labai populiarios. Pagrindinės to priežastys: SHA-1 vis dar nėra įveikta, o 2012 m. planuojama paskelbti naują maišos funkcijų standartą SHA-3.
* UNIX šeimos operacinėse sistemose planuojama naudoti SHA-256 ir SHA-512 slaptažodžių santraukoms saugoti vietoj MD5.
* Spragų kol kas nerasta, bet ji algoritmiškai panaši į SHA-1.

**SHA-3** – taip pavadintas naujas maišos funkcijų standartas, kuriam paskelbtas konkursas 2007 metais. Nugalėtojas išrinktas 2012 metais.

* SHA-3 veikia visiškai kitokiu principu, negu SHA-2.
* Santraukų ilgis - 224, 256, 384 ir 512 bitai.

