2021

Salaukset ja hash-funktio

JULKUNEN NOA

Hash – funktio

Hash-funktio on eräänlainen tiivistefunktio, joka ottaa syötteeksi merkkijonon ja tuottaa siitä tietyn mittaisen tiivisteen. Käyttökohteina esimerkiksi alkioiden taulukoinit ja tiedostojen eheyden tarkistamisessa. Salasanojen tallentaminen merkkijonoina tietokantaan on tietoturvariski, salasanat on valmis käyttöön jos ne murron yhteydessä varastettaisiin. Turvallisempaa on tallentaa salasanoista generoituja tiivistemerkkijonoja. Kirjautumishetkellä voidaan verrata kirjautumiseen käytetyn salasanan pohjalta tehtyä tiivistettä tallennettuun tiivisteeseen, jos ne on vastaavat, salasana on oikea. Yksi pääkäyttökohteista on digitaalinen allekirjoitus ja tiedoston eheyden tarkistaminen. MD-5 ja SHA-1 ovat tunnetuimmat ja käytetyimmät tiiviste funktiot (molemmat tosin murrettuja eikä enään suositella käyttöä) vaan uudempia versioita suositellaan käytettäväksi.

Lähde :

http://web.lapinamk.fi/jouko.teeriaho/krypto2019/crypto4.pdf

https://www.theseus.fi/bitstream/handle/10024/33848/Kaarnalehto_Mika.pdf?sequence=1&isAllowed=y

Symmetrinen salaus

Salausmenetelmä, jossa esimerkiksi viestin lähettäjä ja vastaanottaja käyttävät samaa salausavainta, joka määrittää salauksen. Symmetriset salausavaimet voidaan luokitella kahteen ryhmään: lohko-ja jonosalausavaimiin. Lohkosalausavain käsittelee tietoa lohkoina, jotka salataan joka kerta samalla avaimella. Tyypillisiä lohkojen kokoja on 64-128 bittiä. Jonosalausavain käsittelee tietoa lohkoina, jotka salataan bitti kerrallan, mutta avain vaihtuu jokaisen yksittäisen salausoperaation jälkeen. Itse salaus tapahtuu yhdistämällä sen hetkinen salausavain ja teksti yksinkertaisella XOR-operaatiolla salatekstiksi. Tästä syntyy avainjono, johon tarvitaan algoritmi joka alustetaan valitulla salausavaimella. Tämän jälkeen algoritmi tuottaa jatkuvasti uusia avaimia, joita salaus käyttää. DES (Data Encryption Standard) on Yhdysvaltojen virallinen salaustandardi. Sen turva riittää kotikäyttöön, mutta ei mihinkään tärkempään johtuen sen 56-bittisestä avaimesta, joka on nopea ratkoa brute force menetelmällä, kokeilemalla jokainen avain vuorotellen.
Esimerkiksi pikaviestintäsovellus Signal käyttää symmetrisiä salausavaimia estämään ulkopuolisten lukevan viestiä.
Lähde :
https://www.theseus.fi/bitstream/handle/10024/33848/Kaarnalehto_Mika.pdf?sequence=1&isAllowed=y

https://en.wikipedia.org/wiki/Signal_(software)

Asymmetrinen salaus

Salausmenetelmä, jossa salaamiseen ja salauksen purkamiseen käytetään eri avaimia. Avaimia on kahdenlaisia :julkisia ja yksityisiä. Ne ovat yhteydessä toisiinsa matemaattisella tavalla, jota on käytännössä mahdoton ulkopuolisen selvittää. Julkista avainta käytetään salaamiseen ja sitä voi levittää esimerkiksi omalla www-sivulla. Yksityistä avainta käytetään salauksen purkamiseen, ja sitä ei saa levittää ellei halua salatun tekstin päätyvän selkotekstinä ulkopuoliselle. Kuitenkin tarvitaan oikeanlainen avain, jotta salauksen voi purkaa yksityisellä avaimella.

RSA (Rivest, Shamir, Adleman) on vuonna 1977 kehitetty salausalgoritmi, joka perustuu suuriin alkulukuihin (jaollisia ykkösellä ja itsellään). Järjestelmässä avaimet ovat symmetrisiä joten ne toimivat molempiin suuntiin mahdollistaen epäsymmetrisen salauksen ja digitaalisen allekirjoituksen. Digitaalisessa allekirjoituksessa lähettäjä salaa viestin omalla yksityisellä avaimellaan ja vastaanottaja purkaa salauksen julkisella avaimella. Jos viestistä tulee luettava, voidaan olla varmoja viestin lähettäjästä.

Lähde :
https://www.theseus.fi/bitstream/handle/10024/33848/Kaarnalehto_Mika.pdf?sequence=1&isAllowed=y