Salakirjoitusmenetelmien historia

Nuutti Varis
nvaris@cs.helsinki.fi

Helsinki 12.5.2004

Seminaariaine

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

Salakirjoituksen syntymisen on sanottu tapahtuvan kaikissa sivilisaatioissa samoihin aikoihin kuin kirjoitustaidonkin. Historiassa salakirjoituksella on ollut muitakin tarkoituksia kuin tiedon salaaminen, kuten erilaisten alytehtävien luonti. Salakirjoituksen eräänä ongelmana on aina ollut menetelmien monimutkaisuus. Tietokoneiden kehittyminen on muuttanut salakirjoitusmenetelmiä rankasti.

Salakirjoitusmenetelmät voidaan jakaa kahteen pääryhmään, joihin valtaosa salakirjoitusmenetelmistä perustuu. Ensimmäinen menetelmä on korvausmenetelmä, missä normaali teksti korvataan jonkin avaimen avulla salakirjoitetulla tekstillä. Toinen menetelmä on sekoitusmentelmä, jossa normaaliteksti siirtymien avulla muutetaan salakirjoitukseksi, jota on hankala purkaa.

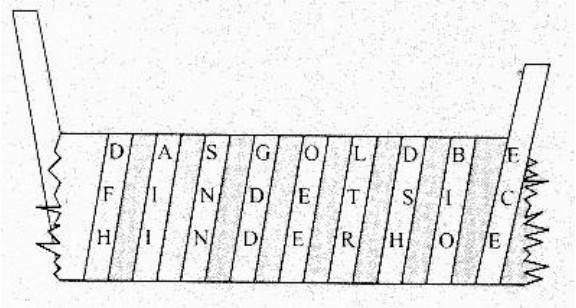
Seuraavissa kappaleissa käsitellään erilaisia salausmenetelmiä kronologisessa järjestyksessä. Kappaleessa 2 esitellään salakirjoituksen alkuvaiheita tuhansia vuosia sitten. Kappale 3 esittelee ajanjakson vuodesta noin 500 jKr. 1800-luvun loppupuolelle. Kappaleessa 4 käsitellään nykyaikaisia salakirjoitusmenetelmiä 1900-luvun alusta noin 1970-luvulle. Viimeinen kappale 5 tekee yhteenvedon salakirjoitusmenetelmien historiasta ja siitä miten salakirjoitusmenetelmät liittyvät tai vaikuttivat nykyaikaiseen tietojenkäsittelytieteeseen.

2 Salakirjoituksen ensiaskeleet

Salakirjoituksen ensiaskeleet otettiin lähi-idässä. Egyptiläinen kirjuri käytti epänormaaleja hieroglyfisymboleita kirjoittaessaan hallitsijansa elämäkertaa. Tämä on ensimmäinen tähän päivään saakka säilynyt kirjoitus, jossa tietoisesti tekstin merkitystä on muutettu korvausmenetelmällä. Ensimmäisten kolmen tuhannen vuoden aikana salakirjoituksen kehitys ei ollut tasaista. Sen käyttötarkoitus oli lähinnä antaa tiedolle tärkeämpi merkitys, kätkien sen älyllisten tehtävien taakse. Tiedon salaus ei ollut pääasia, vain tiedon arvon tai mystisyyden nostaminen [Kah97, s. 71-72].

Skytale (kuva 1) oli kreikkalaisten keksimä laite noin 487 eKr., jonka luullaan olleen

varhaisimpia, ellei ensimmäinen salakirjoituslaite. Se oli keppi, jonka ympärille kiedottiin materiaali, jolle haluttiin kirjoittaa. Vastaanottajalla tuli olla samanlainen keppi, jonka ympärille hän kietoi materiaalin, jolle viesti oli kirjoitettu [Kah97, s. 82]. Tämän jälkeen vastaanottaja luki korostetut kirjaimet materiaalin pinnalta. Skytalen käyttötarkoituksista ei ole säilynyt varmaa tietoa nykypäivään ja saattoi myös olla käytetty muuhun tarkoitukseen kuin salakirjoitukseen [Kel98].



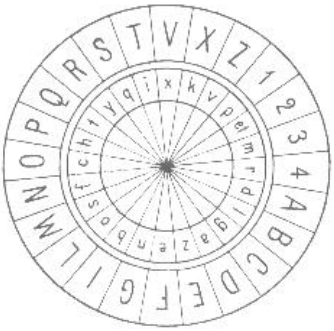
Kuva 1: Kuva ”skytale” laitteesta

Kreikkalainen kirjailija nimeltä Polybius keksi erään yleisimmän salakirjoitusmenetelmän perusteet. Hänen ideana oli laittaa kaikki aakkoston kirjaimet kaksiulotteiseen taulukkoon ja merkata rivit sekä sarakkeet numeroilla. Näin jokaista kirjaimiston merkkiä vastasi kaksinumeroinen luku. Polybiuksen neliöllä on ollut erittäin suuret vaikutukset moderneihin salakirjoitustekniikoihin. Myöhemmin, antiikin Rooman aikana keisari Julius Ceasar käytti yksinkertaista kirjainten korvaukseen perustuvaa salakirjoitusta [Kah97, s.83-84].

3 Keskiajalta 1800-luvun loppuun

Salakirjoituksen kehitys ei edennyt tasaisesti keskiajalla. Varsinkin euroopassa varhaiskeskiajalla salakirjoitusta pidettiin mystisenä asiana ja mustana magiana, ja sen käyttöä kartettiin joka puolella kristillistä maata. Tästä johtuen salakirjoitus ei kehittynyt euroopassa vasta kuin 1400-luvun jälkeen ja useita salakirjoitukseen littyviä julkaisuja katosi tänä aikana. Salakirjoitus kuitenkin kehittyi varhaiskeskiajalla joidenkin arabivaltioiden sivilisaatioiden kehittyessä. Varhaiskeskiajan jälkeisessä euroopassa salakirjoitusmenetelmät kehittyivät eteenpäin suurin askelin.

1400-luvun puolivälissä italialainen arkkitehti nimeltä Leon Battista Alberti kehitti salakirjoitusmenetelmän, johon lähes kaikki modernit salakirjoitusmenetelmät perustuvat. Hänen järjestelmänsä oli ensimmäinen maailmassa, joka käytti moniaakkosellista salakirjoitusmenetelmää hyväkseen tiedon kätkemiseen. Tätä järjestelmää varten Alberti loi välineen, jolla voitiin valita esimerkiksi kunkin normaalin tekstin sanan salakirjoitusaakkosto. Väline oli kaksitasoinen kiekko (kuva 2), jossa oli kaksi kehää normaaleja aakkoston kirjaimia. Sisempää kiekkoa voitiin liikuttaa niin, että sen avulla valittiin ulkokehältä normaalin tekstin aakkosto siirtämällä jokin ennalta sovittu kirjain jonkin sisäkehän kirjaimen kohdalle. Nyt salakirjoittaja valitsee ulkokehällä olevien normaalimuodossa olevien kirjainten sijasta sisäkehällä olevat kirjaimet. Mikä erottaa albertin menetelmän kaikista muista aikaisemmin ilmestyneistä menetelmistä on salausavaimen muuttaminen. Albertin menetelmässä salausavain muuttuu esimerkiksi joka sanan jälkeen, jolloin syntyy kokonaan uusi salausaakkosto seuraavalle sanalle. Tähän menetelmään perustui myös useat myöhemmin keksityistä salakirjoitusmenetelmistä [Kah97, s. 127-129].



Kuva 2: Albertin salakirjoituskiekko

Albertin salakirjoituskiekossa oli myös numerot 1-4. Numeroiden avulla voitiin luoda yhdistelmiä, joilla oli jokin ennalta määrätty tarkoitus. Esimerkiksi numerosarja 114 voisi tarkoittaa Albertia itseään normaalitekstissä. Tällä tavoin Alberti tuli keksineeksi salakirjoituksen erään tärkeän menetelmän, salakirjoitetun koodin [Kah97, s. 129-130].

Vuonna 1563 italialainen monilahjakkuus Giovanni Battista Porta julkaisi teoksen, jossa kehitettiin edelleen Albertin sekä muiden menetelmiä. Teos myös esittelee ensimmäisen karkean jaon salakirjoitusmenetelmien luokittelulle sekoitus- sekä korvausmenetelmiin.

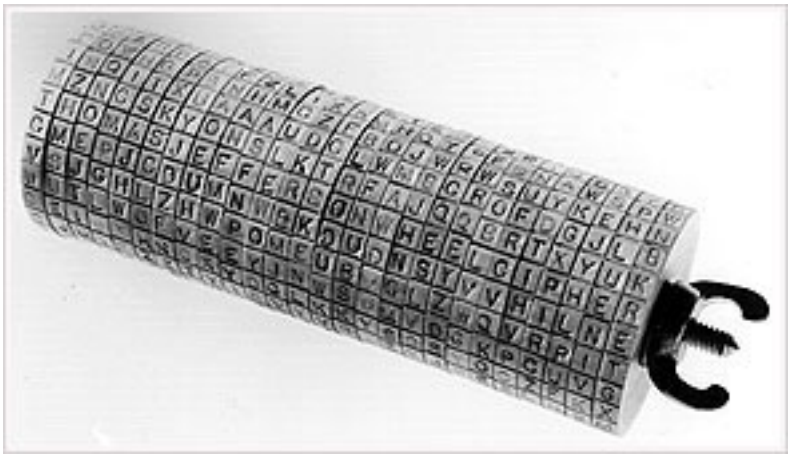
Kuitenkin tärkein asia kirjassa on uudenlaisen salakirjoitusmenetelmän esittely. Portan salakirjoitusmenetelmässä jokaista kahta normaalin tekstin kirjainta vastaa yksi symboli.

Kuva 3: Giovanni Portan salakirjoituskiekko

Ensimmäisen binääriaakkostollisen salakirjoitusmenetelmän keksi Sir Francis Bacon 1600-luvun alkupuolella. Siinä jokainen aakkoston merkki korvattiin viisibittisellä yhdistelmällä. Bitteinä Bacon käytti a ja b merkkejä. Esimerkiksi kirjaimiston merkki A kuvattiin viisibittisenä yhdistelmänä ’aaaaa’. Muunnoksen jälkeen Bacon sisällytti koodatun viestinsä johonkin normaalin tekstiin, esimerkiksi siten, että jokainen bitti ’a’ kuvattiin normaaliksi kirjaimeksi, ja jokainen ’b’ kuvattiin kursiivikirjaimeksi. Kirjasimien muuntaminen tällä tavoin paljasti usein salakirjoituksen muillekin kuin vastaanottajalle, joten Bacon usein muutti vain joitakin tiettyjä kirjaimia erittäin vähän, jolloin salakirjoitusta ei pystynyt havaitsemaan kuin sen vastaanottaja, joka tiesi mitkä kirjaimista toimivat bitteinä.

Kuva 4: Francis Baconin binääriaakkoston ratkaisuavain

1700-luvun loppupuolella amerikkalainen valtionmies Thomas Jefferson keksi uudenlaisen salakirjoituslaitteen. Hän kutsui sitä ”wheel cipher”-nimellä (kuva 5). Laite oli pienikokoinen sylinteri, jossa oli erillisiä pyöriviä levyjä. Jokainen pyörivä sylinterin levy oli jaettu 26 erilliseen osaan. Jokaisessa osassa oli yksi aakkoston kirjain merkattuna musteella. Sylinterissä oli tällöin 26 ”riviä”, joita käytettiin salakirjoitukseen. Laite toimi siten, että salakirjoitettava teksti pyöritettiin sylinterin osien avulla selväkielisenä yhdelle riville. Tällöin selväkielisen tekstin pystyi lukemaan sylinterin vaakariviltä. Sen jälkeen salakirjoittaja valitsi jonkin muista, täysin sattumanvaraisista riveistä jossakin muualla sylinterin pinnalla, ja käytti tätä riviä salakirjoituksena. Kun vastaanottajan piti selvittää salakirjoitettu teksti, hän yksinkertaisesti asetteli sylinterin osat sillä tavoin, että salakirjoitettu teksti oli näkyvissä sylinterin vaakarivillä. Sen jälkeen normaali teksti oli jollakin toisella vaakarivillä sylinterin pinnalla [Kah97, s.192-194].



Kuva 5: Kuva Jeffersonin ”wheel cipher” laitteesta.

4 Modernit salakirjoitusmenetelmät

1900-luvulla kryptografian historiassa tapahtui merkittävä muutos. Langattoman viestinnän yleistyessä myös viestien salakuuntelu kävi helpommaksi. Maailmansotien seurauksena valtiot myös ymmärsivät, että tehokkaat salakirjoitusmenetelmät näyttelisivät entistä suurempaa osaa sotilasviestinnässä.

Vuoden 1917 loppupuolella amerikkalainen tutkija Gilbert Vernam kehitti ensimmäisen täysin automatisoidun salausjärjestelmän. Tämä järjestelmä oli ensimmäinen, jossa koneellisesti muutettiin reaaliajassa salattu teksti takaisin normaalimuotoon. Järjestelmä muutti tekstin morseaakkoston tapaisiksi sarjoiksi ja salakirjoitti ne jollakin avaimella, joka oli vastaanottajan tiedossa. Kummassakin päässä oli kone, joka sekä muunsi normaalin tekstin salakirjoitukseksi, että purki salakirjoitustekstin takaisin normaalitekstiksi. Vernamin keksintö oli mullistava, mutta sillä oli myös toinen erittäin suuri vaikutus salakirjoituksen historiassa. Vernamin keksinnön nähtyään amerikkalainen majuri Joseph Mauborgne kehitti Vernamin salakirjoitusmenetelmää eteenpäin, luoden siitä maailman ensimmäisen ja ainoan täysin turvallisen salakirjoitusmenetelmän. Kuitenkin salakirjoitusmenetelmä on täysin turvallinen vain niin kauan kuin jokainen viesti, joka järjestelmällä salakirjoitetaan, on luotu täysin yksikäsitteisen salakirjoitusavaimen avulla [Kah97, s. 395-398]. Menetelmä on edelleen käytössä yksinkertaisissa huippusalaisissa kommunikaatioissa.

Toinen tärkeä moderniin salakirjoitukseen liittyvä menetelmä keksittiin neljän eri tahon toimesta 1900-luvun alkupuolella. Tämä keksintö oli uudenlainen salakirjoituskone, joka perustui sekoitinmekaniikkaan salauksen luomiseksi. Sekoittimet olivat usein kiekkoja, joiden avulla laitteelle annettu normaaliteksti muutettiin salakirjoitukseksi. Jokaisen normaalitekstin kirjaimen jälkeen sekoittimissa tapahtui liikahduksia, jolloin seuraava kirjain salattiin uudella salausavaimella. Jokaisessa sekoitinkiekossa oli yleensä noin 19-35 erilaista kirjainta tai symbolia, ja kiekkojen määrä vaihteli yleensä yhdestä viiteen. Tämän kaltainen salausmenetelmä oli siihen aikaan jo melko turvallinen, koska sekoitinkiekkojen aakkoston jaksosta tulee niiden merkkien tulo, esimerkiksi koneella, jossa on kolme 26 merkkistä kiekkoa, aakkoston jaksoksi tulee 17576 kirjainta. Näin ollen alle 17576 merkkisillä viesteillä sekoitinkiekkojen tarjoama salausavain ei mene ympäri, ja viestin purkaminen ilman avainta voi olla hyvin vaikeaa [Kah97, s. 410-415].

Tunnetuin aikansa sekoitinkone oli Arthur Scherbiuksen luoma Enigma (kuva 6). Enigmassa oli kuitenkin kaksi selkeää eroa muihin koneisiin. Ensinnäkin, Enigma salasi kaiken normaalitekstin kahteen kertaan. Tämä oli myös Enigman heikkous, koska menetelmä, jolla kaksinkertainen salaus luotiin, aiheutti myös sen, että salaus oli samalla käänteinen. Esimerkiksi normaali kirjain e salakirjoitettiin kirjaimeksi x, niin samoin tavoin normaali

kirjain x salakirjoitettiin kirjaimeksi e. Toinen ero muihin sekoitinkiekkomenetelmiin oli kiekkojen pyörimisen satunnaistaminen erillisten rattaiden avulla. Alkuperäisessä Enigmassa rattaiden pyörähdys oli niin pieni, että Enigman aakkoston jakso oli vain 53,295 kirjainta [Kah97, s. 420-421].

Kuva 6: Kuva alkuperäisestä Enigma-salakirjoituskoneesta

Tietokoneiden yleistyttyä 1970-luvulla salakirjotusmenetelmissä myös siirryttiin uusiin järjestelmiin. Salakirjotusmenetelmät jaettiin kahteen eri luokkaan, symmetrisiin ja asymmetrisiin menetelmiin. Symmetriset salakirjoitusmenetelmät ovat sellaisia, joissa salakirjoitusavaimella sekä puretaan että luodaan salakirjoitettu viesti. Asymmetrisissä menetelmissä on kumpaakin prosessia varten erillinen toisistaan eroava avain. Ennen 1970-lukua kaikki käytetyt salausmenetelmät olivat olleet symmetrisiä. Salaus ja purku tapahtui joko samalla avaimella, tai avaimen muuntamiseen käytettiin erittäin yksinkertaista muutosoperaatiota. Samaan aikaan siirryttiin kirjainpohjaisesta salauksesta erillisillä koneilla tietokonemaailmaan ja sen mukana bittipohjaisiin salausalgoritmeihin, jotka toimivat tietokoneissa.

Ensimmäinen laajalti käytössä ollut bittipohjainen salakirjoitusmenetelmä on DES (*Data Encryption Standard*) [NIS77]. DES-algoritmin kehitti IBM, joka lähetti sen Yhdysvaltojen kansalliselle turvallisuuspalvelulle (*National Security Agency, NSA*) ehdotuksena standardoiduksi salakirjoitusmenetelmäksi, ja tästä johtuen se sai ristiriitaisen vastaanoton maailmalla. Kuitenkin sitä ruvettiin käyttämään eri yritysten toimesta. DES menetelmän

avain on 56-bittinen ja se salaa tekstin lohkoissa. Salaus tekee 16 erillistä kierrosta, joilla jokaisella tehdään muunnoksia salakirjoitettuun tekstiin [Kah97, s. 979-984].

Vuoden 1976 lopulla julkaistiin artikkeli [DiH76], joka mullisti modernin salakirjoitustieteen ja tulisi olemaan perustana suurimmalle osalle nykyään käytettävistä salakirjoitusmenetelmistä. Whitfield Diffie ja Martin E. Hellman esittivät artikkelissa uudenlaisen salausmenetelmän, joka perustui julkisiin salausavaimiin. Tämä salakirjoitusmenetelmä oli ensimmäinen, jossa salakirjoituksen luonti ja purkuavaimet olivat erilaiset. Menetelmän toimii siten, että jokainen henkilö antaa julkiseen jakeluun oman luontiavaimensa. Sen avulla muut henkilöt voivat salakirjoitaa viestin, jonka vastaanottaja voi purkaa omalla ei julkisella purkuavaimella. Menetelmän huomattavana etuna on luontiavainten vapaa jakelu, enää ei tarvittu erillistä avaintenvaihto-operaatiota kommunikoivien henkilöiden välillä jonkin turvallisen kanavan kautta (esimerkiksi kuriirin väliyksellä). Artikkeli esitteli tämän perusperiaatteen, mutta kokonaista järjestelmän implementaatiota siinä ei ollut.

Pian Diffien ja Hellmanin artikkelin jälkeen Ron Rivest, Adi Shamir ja Leonard Adleman suunnittelivat ensimmäisen julkisiin avaimiin perustuvan salausmenetelmän. Menetelmän nimeksi tuli RSA [RSA78] suunnittelijoiden sukunimien ensimmäisten kirjainten mukaan, ja se sai valtaisan suosion heti artikkelin julkaisun jälkeen. RSA algoritmi perustuu alkulukujen ominaisuuksiin ja niiden avulla tehtäviin normaaleihin matemaattisiin operaatioihin.

5 Yhteenveto

Salakirjoituksen historia on edennyt samaa tahtia kuin ihmiskunnankin historia. Kirjoitustaidon synnyttyä syntyi luontainen tarve salata tietoa, antaa se vain tiettyjen henkilöiden nähtäväksi. Salakirjoituksen kehitys ei aina ole mennyt eteenpäin, mutta ajallisesti ajateltuna salakirjoitus on kehittynyt samaa vauhtia tekniikan kanssa, savitauluista moderneihin tietokoneisiin ja niissä ajettaviin monimutkaisiin algoritmeihin.

Tietojenkäsittelytieteen kannalta salakirjoitus on varsin uusi asia, niin kuin koko tietojenkäsittelytiede. Salakirjoitusmenetelmät kehittyivät yksinkertaisista koneista tietokoneis-

sa toimiviksi algoritmeiksi 1900-luvun puolivälin jälkeen. Tällöin tapahtui myös laajamittainen siirtymä merkkipohjaisista salausmenetelmistä bittipohjaisiin menetelmiin. Kuitenkin salakirjoitusmenetelmien perusperiaatteet tietojenkäsittelytieteessäkin ovat tulleet useiden satojen vuosien takaa.

Salakirjoitusmenetelmät ovat kehittyneet monimutkaisemmiksi ajan kuluessa, mutta perusajatus menetelmien kahtiajakoon pätee edelleen. Vasta asymmetristen salakirjoitusmenetelmien syntymisen myötä tämä jaottelu muuttui käsitteiksi symmetrisistä ja asymmetrisistä salakirjoitusmenetelmistä, joka pätee tähän päivään saakka. Nykyiset salakirjoitusmenetelmät ovat niin turvallisia, että vanhan ajan salakirjoitusten purkajia ei enää ole käytännössä mahdollista käyttää. Tämän johdosta yksi salakirjoitustieteen alue on häviämässä kokonaan.

Lähteet

DiH76 Diffie, W. ja Hellman, M., New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22,6(1976).

Kah97 Kahn, D., *The Codebreakers: The Story of Secret Writing*. Scribner, revised painos, 1996.

Kel98 Kelly, T., The myth of skytale. *Cryptologia*, XXVII,3(1998), sivut 244–260.

NIS77 National Institute of Standards and Technology, Data Encryption Standard (DES). FIPS PUB 46, NIST, tammikuu 1977.

RSA78 Rivest, R. L., Shamir, A. ja Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21,2(1978), sivut 120–126.