Tietojenkäsittelytiede **26** Heinäkuu 2007 sivut 32–53
Toimittaja: Antti Valmari

Kryptologia — tiedon turvaamisen tiede*

Kaisa Nyberg
Teknillinen korkeakoulu
Tietojenkäsittelyteorian laboratorio
ja
Nokian tutkimuskeskus
Kaisa.Nyberg@tkk.fi

Tiivistelmä

Tietoteknisen kehityksen myötä aiemmin vain sotilas- ja diplomaattikäyttöön tarkoitetut salaamistekniset menetelmät ovat tulleet osaksi jokaisen kuluttajan arkipäivää. Tässä artikkelissa kuvataan salaamistekniikan periaatteita, historiaa ja tieteellistä tutkimusta myöskin suomalaisten esimerkkien valossa.

1 Kahden tiimin tiede

Salaamistekniikkaa tutkiva tieteenala, jonka menetelmiä ja päämääriä tämä kirjoitus pyrkii valottamaan, tunnetaan nimellä kryptologia. Nimitys on johdettu kreikankielisestä sanasta *Kryptós*, jolla on seuraavanlaisia merkityksiä: piilotettu, arvoitus, kätkeminen, salaaminen. Siis termin kryptologia suomenkieleen pohjautuva vastine voisi olla esimerkiksi salaamistiede.

Moderni kryptologia on sovellettua matematiikkaa ja tietojenkäsittelyteoriaa. Se tutkii ja kehittää tiedon salaamisessa käytettäviä funktioita ja mekanismeja, sekä arvioi niiden ominaisuuksia matematiikan, systeemiteorian ja kompleksisuusteorian näkökulmista. Kryptologisen tutkimuksen tuloksia sovelletaan käytäntöön salaamisteknisten järjestelmien suunnittelutyössä, mikä puolestaan on sekä tarkoitukseltaan että menetelmiensä puolesta tietoteknistä tutkimus- ja kehitystyötä. Se jaetaan usein kahteen osa-alueeseen, *kryptografiaan* eli salaamisteknisten menetelmien suunnittelutieteeseen, ja *kryptoanalyysiin* eli oppiin salaamismenetelmien vahvuudesta. Jako ei perustu niinkään käytettäviin menetelmiin vaan tutkimuksen päämääriin.

Jopa hyvin kokenut suunnittelija on usein sokea luomansa menetelmän heikkouksille. Vielä varmemmin näin on laita, kun asialla on keksinnöstään innostunut ensikertalainen. Voidaan sanoa, että salaamisteknisen menetelmän suunnittelussa on äärettömän monta kohtaa, joissa voi epäonnistua. Tämä johtuu siitä, että on mahdotonta esittää täydellistä luetteloa kaikista vaatimuksista, jotka on otettava huomioon. Mutta myöskin tunnetut

*Artikkeli on alunperin kirjoitettu vuonna 2002 Tietojenkäsittelytieteen seuran toteutumatta jäänyttä 20-vuotisjuhlakirjaa varten.

OHJE KIRJAPAINOLLE: B5-arkin vasen- ja yläreuna kohdistetaan A4-arkin vasempaan ja yläreunaan. Näin pitäisi marginaaliksi tulla taitteen puolella noin 33 mm ja muualla noin 22 mm.

ratkaisumenetelmät, joita kryptologisessa ammattislangissa kutsutaan hyökkäyksiksi, muodostavat niin kirjavan ja laajan joukon, että niiden kaikkien huomioonottaminen vaatii pitkäaikaisen kokemuksen tuomaa ammattitaitoa. Kokemus on myös osoittanut, että kryptografisessa suunnittelutyössä on hyvä olla ainakin kaksi tiimiä, joista toinen vastaa suunnittelusta, ja toinen analysoi suunnittelun kohteena olevaa salaamisteknistä menetelmää.

Kryptologinen järjestelmä voidaan pelkistäen esittää kahden osapuolen välisenä kommunikaatiojärjestelmänä. On tullut tavaksi kutsua näitä osapuolia nimillä *Alice* ja *Bob*. Kummallakin heistä on mahdollisuus lähettää tai vastaanottaa viestejä sekä suorittaa laskentaa. Eri mallit eroavat suuresti sen suhteen, kuinka paljon laskentakapasiteettia Alicella ja Bobilla oletetaan olevan. Viestien välitykseen käytetään kommunikaatiokanavaa, jonka oletetaan olevan turvaton. Järjestelmässä toimii myös kolmas osapuoli *Carol*, aakkosten kolmannen kirjaimen mukaan, jolla on pääsy Alicen ja Bobin väliseen kommunikaatiokanavaan, sekä kaikkeen muuhun kyseiseen kryptologiseen järjestelmään liittyvään tietoon, jota ei ole erityisesti turvattu. Carolin pääsy järjestelmään voi olla, mallista riippuen, aktiivista kommunikaatiokanavan käyttämistä tai vain passiivista salakuuntelua, jolloin hänet tunnetaan myös nimellä *Eve* (englanninkielen sanasta *eavesdrop*, salakuunnella). Salaamisteknisen menetelmän tarkoituksena on turvata Alicen ja Bobin keskinäinen viestintä Carolin tai Even pahantahtoisilta yrityksiltä puuttua siihen. Menetelmä käsittää perheen funktiopareja, joista Alice ja Bob valitsevat yhden parin. Alice käyttää valitun funktioparin ensimmäistä funktiota ja Bob toista.

Kryptologiselle menetelmälle on luonteenomaista se, että täydellinen tieto funktioparin valinnasta on salaista. Modernissa kryptografiassa on tyypillistä, että valinta rajoittuu johonkin ennalta hyvin määriteltyyn joukkoon, jota kutsutaan *salaamistekniseksi järjestelmäksi*, ja tieto valinnasta voidaan ilmaista tehokkaasti suhteellisen lyhyttä parametria käyttäen. Tätä salaista tietoa kutsutaan kryptologisen menetelmän *avaimeksi*. Kaikki mahdolliset avaimet muodostavat siis joukon, jolla käytettävissä olevat funktioparit voidaan indeksoida.

Salaamisteknisen järjestelmän oleellisena piirteenä on salassapidettävyyden vaatimus. Modernin kryptografisen tutkimuksen tärkeimpiä saavutuksia on, että riittää, kun tuo vaatimus kohdistetaan vain ja pelkästään kryptografiseen avaimeen, ja että täydellinen tieto salaisesta avaimesta voi olla molemmilla kommunikoivilla osapuolilla tai vain toisella, mutta ei Carolilla tai Evellä. Salaisuuteen liittyy myös ennakoimattomuuden vaatimus. Siispä salaisuutta ei voi olla ilman epävarmuutta, eikä epävarmuutta ilman satunnaisuutta. Kryptologia tutkii, kuinka satunnaisuutta voidaan käyttää hyväksi tiedon turvaamisessa.

Jos Alice ja Bob eivät tee mitään viestiensä turvaamiseksi, Eve voi kytkeytyä kommunikaatiokanavalle ja salakuunnella käytyä viestien vaihtoa. Viestien luottamuksellisuuden turvaamiseksi Alice ja Bob voivat käyttää jotain vahvaa salakirjoitusmenetelmää. Salakirjoitusmenetelmä koostuu funktiopareista, joista toista käytetään salaamiseen ja toista tulkintaan. Alice ja Bob sopivat salaisesta avaimesta, joka määrää käytetyn funktioparin. Kun Alicella on viesti lähetettäväksi Bobille, hän salakirjoittaa sen salaamisfunktiolla. Saatuaan salakirjoitetun viestin Bob tulkitsee sen tulkintafunktiolla.

Miten Carol ja Eve voivat yrittää ratkaista käytetyn salaisen avaimen? Nyky-

aikainen kryptoanalyyttinen tutkimus tuntee monta erilaista tapaa. Se ei rajoitu vain mahdollisuuteen, että Eve salakuuntelee kommunikaatiota, nauhoittaa sen ja pyrkii ratkaisemaan salatun viestin tai käytetyn avaimen. Myös kaikenlainen muu sekaantuminen Alicen ja Bobin välisiin suhteisiin sallitaan, ja siten kolmiodraamojakin voi syntyä [3]. Carol voi esimerkiksi yrittää *valitun selväkielen ratkaisua*, eli antaa itse valitsemiaan viestejä Alicelle lähetettäväksi Bobille. Tai jos Carolilla on pääsy Bobin luokse, kun Bob lukee Alicelta saamiaan viestejä, niin Carolille aukeaa mahdollisuus yrittää *valitun salakielen ratkaisua*. Carol voi syöttää kommunikaatiokanavalle valitsemiaan viestejä, ja mennä sitten Bobin luokse katsomaan, mitä niistä tulkinnan jälkeen syntyy. Myöhemmin tässä kirjoituksessa esitetään todellinen esimerkki valitun salakielen hyökkäyksestä, jonka onnistuminen edellyttää ainoastaan, että Carol näkee, onko Bob pystynyt tulkitsemaan Carolin lähettämää valittua salakieltä [2].

Seuraavassa luodaan yleiskatsaus salaamistekniikan historiaan, sen keskeisiin periaatteisiin ja modernin kryptologisen tutkimuksen syntyyn. Artikkelin loppuosassa selvitetään nykyaikaisen salaamisteknisen tutkimuksen keskeisiä kysymyksiä, tutkimusmenetelmiä ja saavutettuja tuloksia.

2 Salaamistekniikan kehitys

Ennen tietokoneiden mukanaan tuomaa informaatioteknologista vallankumousta, siis vielä toisen maailmansodan aikana, salaamistekniikan ammattimainen tutkimus ja kehitys oli sotilas- ja tiedusteluorganisaatioiden käsissä. Eri maiden puolustusvoimien piirissä oli tosin julkaistu oppikirjoja ja opetusaineistoa myös salakirjoitusmenetelmistä (esimerkiksi [9]), mutta ne eivät johdattaneet lukijoitaan juuri alkeita syvemmälle. Julkinen kirjallisuus ei käsitellyt ollenkaan salakirjoitusmenetelmien ratkaisemista eli murtamista. Sitä pidettiin jopa eettisesti arveluttavana toimintana. “Herrasmiehet eivät lue toistensa kirjeitä”, kerrotaan Yhdysvaltain ulkoministerin H. L. Stimsonin lausahtaneen vuonna 1929 kuultuaan, että ministeriön tiedusteluelin *Black Chamber* pystyi tulkitsemaan eräiden muiden maiden salattua diplomaattista viestiliikennettä, minkä jälkeen hän antoi käskyn lopettaa tämä toiminta.

Ensimmäiset luotettavat ja yksityiskohtaiset esitykset siitä, kuinka liittoutuneet mursivat toisen maailmansodan aikana saksalaisten *Enigma*-salaamismenetelmän, saatiin vasta 1980-luvun taitteessa. Brittien koko sodanaikaisen kryptoanalyyttisen toiminnan olemassaolo Bletchley Parkissa, mitättömällä paikkakunnalla Cambridgen ja Oxfordin yliopistokaupunkien puolessa välissä, pysyi tarkoin varjeltuna salaisuutena kolmekymmentä vuotta sodan päättymisen jälkeen. Nykyään siellä toimii museo (http://www.bletchleypark.org.uk/).

Salaamistekniikan merkitys kansallisen turvallisuuden välineenä ei suinkaan ole vähentynyt, eikä myöskään turvallisuusorganisaatioiden kiinnostus sen tutkimusta kohtaan. Susan Landau kertoo artikkelissaan [11, s. 450], että 1970-luvun lopulla Massachusetts Institute of Technologyn (MIT) tutkijoita kiellettiin esittämästä tutkimustuloksiaan julkisesti aseiden vientirajoituksiin perustuen. Edelleenkin etenkin Yhdysvalloissa ja sen liittolaismaissa tiedon salaamismenetelmät luetaan osaksi aseteknologiaa, mistä johtuen niiden käyttöä ja vientiä jatkuvasti valvotaan. Kaikki salaamistekniik-

kaa käyttävät tuotteet, kuten esimerkiksi matkapuhelimet, kuuluvat *Wassenaar-järjestelyn* piiriin, eli luetaan *kaksikäyttötuotteiksi*, joilla on sekä siviili- että sotilaskäyttöä. Tämä 40 teollisuusmaan allekirjoittama (vuoden 2007 tilanne) Wassenaar-järjestely sääntelee salaamistekniikkaa käyttävien tuotteiden vientiä kolmansiin maihin salaamisteknisen menetelmän vahvuuden mukaan, missä vahvuutta mitataan salaamisteknisen menetelmän avaimen pituudella.

Sääntelyä tukevat äänenpainot ovat jälleen voimistuneet syyskuun 11. päivän terrori-iskun jälkeen, jonka valmistelussa väitetään käytetyn salattua sähköpostia. Katastrofin jälkimainingeissa *New York Times* haastatteli vahvojen nykyaikaisten salaamismenetelmien kehittäjiä, muiden muassa Stanfordin yliopiston professoria Martin Hellmania, kysyen, olisivatko he jättäneet julkaisematta 1970-luvulla syntyneet salaamistekniset keksintönsä, jos olisivat tienneet, mihin niiden väärinkäyttö voi johtaa. On tietenkin selvää, että tällainen kysymys voitaisiin esittää myös useiden muiden nykyaikaisten teknologisten keksintöjen kohdalla, joiden käytöstä aiheutuu paitsi ylivertaista hyötyä, myös mahdollisesti arvaamatonta haavoittuvuutta.

3 Kryptologian kehitys julkiseksi tieteeksi

Ensimmäinen salaamistekniikan tieteellinen tutkimus oli ilmestynyt jo vuonna 1949. Se oli Claude Shannonin artikkeli salakirjoitusjärjestelmien teoriasta [26], jossa hän esitti salakirjoitusjärjestelmien teoreettisen viitekehyksen. Shannonin vuotta aikaisemmin julkaisema artikkeli viestinnän matemaattisesta teoriasta [25] oli luonut perustan ja lähtökohdan nykyaikaiselle informaatioteorialle ja laukaissut alalla laajan ja voimakkaan tutkimustoiminnan jo heti ilmestyttyään. Miksi näin ei käynyt salaamistekniikan alalla? Professori James Massey arvioi syitä seuraavasti [13, s. 543]: “Ensinnäkin siinä esitetty salaamismenetelmien turvallisuuden teoria oli jo täydellinen ja johti kiistämättömään johtopäätökseen, jonka mukaan täydellinen salaus on mahdollinen vain kun salaisen avaimen pituus on suurempi kuin salattavan tiedon määrä, mikä ei tuo mitään etua käytännössä. Lisäksi näkemykset, joita Shannon esitti käytännöllisten salaamismenetelmien kehittämiseksi, näyttivät ennemminkin vain tukevan aikaisemmin tunnettuja käsityksiä kuin tuottavan mitään oleellisesti uutta.”

Mutta Massey toteaa edelleen: “Shannon esitti huomion, että hyvän salaamismenetelmän suunnittelun oleellinen kysymys on löytää sopiva, vaikea ongelma, johon perustuen, ja joidenkin lisäehtojen vallitessa, voidaan kehittää salaamismenetelmä, jonka ratkaiseminen on yhtä vaikeaa kuin tuon alkuperäisen vaikean ongelman ratkaiseminen.” Näin Shannon ennusti sen kehityksen, joka 27 vuotta myöhemmin johti ensimmäiseen konkreettiseen tulokseen. Silloin Stanfordin yliopiston tutkijat Whitfield Diffie ja Martin Hellman julkaisivat artikkelinsa *New Directions in Cryptography* [7], joka osoittautui nimensä veroiseksi uuden suunnan näyttäjäksi salaamisteknisen tutkimuksen historiassa.

Shannonin vuonna 1949 ilmestyneen artikkelin jälkeen salaamismenetelmien alalla ei siis ollut julkista tutkimustoimintaa yli neljännesvuosisataan. Suljettujen organisaatioiden piirissä toiminta kuitenkin jatkui ja kehittyi. Alan tutkijoita oli salaamisteknisiä laitteita valmistavien yritysten piirissä kuin myös kansallisten turvallisuusorganisaatioiden palve-

luksessa, jotka muodostivat ensin mainittujen yritysten pääasiallisen asiakaskunnan. Useissa maissa, myös Suomessa, salaamistekniikan käyttö oli luvanvaraista, ja käytännössä rajoittui puolustusvoimien ja valtionhallinnon sisäisen viestinnän turvaamiseen (esimerkiksi [20, s. 33–37]). Matemaatikot kehittivät salaamismenetelmiä, mutta ei tullut kysymykseenkään, että niitä olisi esitetty julkisuudessa. Julkaisurajoitukset koskivat myös matemaattisia funktioita ja konstruktioita, joilla mahdollisesti saattoi olla sovelluksia salaamistekniikassa.

Esimerkkinä mainittakoon *taivutetut funktiot*, *bent functions*, jotka Oscar Rothaus tiettävästi löysi jo 1960-luvulla, mutta joita koskeva artikkeli ilmestyi vasta vuonna 1976. Salaamistekniikan lisäksi taivutetuilla funktioilla on myös sovelluksia hajaspektritekniikassa, jota kehitettiin aluksi vain sotilaskäyttöön. Tämä myös WCDMA-lyhenteellä mainittu tekniikka tunnetaan nykyään sovelluksistaan kolmannen sukupolven matkapuhelinjärjestelmiin.

Shannonin teorian perushypoteesina oli, että vihollisella, *enemy*, on mahdollisuus saada haltuunsa analysoitavaksi koko salattu viesti. Toinen hypoteesi oli, että salaamismenetelmän turvallisuuden on perustuttava pelkästään salaamisessa käytettyyn avaimeen. Tämän, hollantilaisen A. Kerchoffin (1835–1903) mukaan nimetyn, periaatteen mukaisesti vihollisella voi olla yksityiskohtaiset tiedot käytetystä salaamismenetelmästä, mutta silti hyökkäys salatun viestin selvittämiseksi ei onnistu niin kauan kun avain pysyy salaisena. Avainten ennakoimattomuuden tärkeyttä ei kuitenkaan ole aina ymmärretty. Vielä toisen maailmansodan aikana oli yleisesti käytössä menetelmiä, joissa avain johdettiin painetusta kirjallisuudesta, kuten runoista [12] tai vaikkapa Kyösti Vilkunan historiallisesta romaanista *Kalterijääkärit* [20, s. 37].

Kerchoffin periaatteesta ei suoraan seuraa, että ainoastaan julkisesti tunnetut salaamismenetelmät voivat olla turvallisia. Aina 1970-luvun loppupuolelle kaikki salaamistekniikkaa käyttävät organisaatiot pitivät salakirjoitusmenetelmiinsä liittyvät tiedot niin salaisina kuin mahdollista, jotta estäisivät yksityiskohtaisten tietojen joutumisen vihollisten käyttöön. Kukin pyrki varmistumaan käyttämiensä menetelmien turvallisuudesta ja vahvuudesta joko omin voimin tai perustuen pitkäaikaiseen asiakassuhteeseen ja sen synnyttämään luottamukseen salaamislaitteiden valmistajan kanssa.

Vasta myöhempää perua ovat näkemykset, joiden mukaan salaamismenetelmien tulee olla julkisia. Kun tietokoneiden käyttö ja digitaalinen tiedonvälitys alkoi lisääntyä, niin tarve käyttää salaamistekniikkaa muun voimakkaasti kehittyvän digitaalisen kommunikaatiotekniikan osana laajeni perinteisten sotilas- ja diplomaattisovellusten ulkopuolelle. Oli käytettävä yhtenäistä salaamistekniikkaa, jotta laajojen järjestelmien yhtenäisyys ja yhteentoimivuus voitaisiin taata myös turvallisuuden osalta. Toisaalta laaja käyttö teki si salaamismenetelmän salaamisen pitkän päälle mahdottomaksi. Syntyi tarve suunnitella yleiseen käyttöön tarkoitettu julkinen salakirjoitusjärjestelmä.

Vuonna 1973 Yhdysvaltain kansallinen standardointijärjestö *National Bureau of Standards* teki aloitteen julkisen standardin kehittämiseksi. Lähes neljä vuotta myöhemmin, tammikuussa 1977, standardi *Data Encryption Standard* eli *DES*-algoritmi julkaistiin. Se oli syntynyt Shannonin periaatteiden pohjalta, IBM:n tutkijoiden monivuotisen työpanoksen tuloksena ja Yhdysvaltain kansallisen turvallisuusviraston NSA:n myötävaikutuksella.

1970-luvun loppupuolella alkoi kehitys, joka johti julkisen kryptologisen tutkimuksen räjähdyksenomaiseen laajenemiseen ensin Yhdysvalloissa mutta pian myös Euroopassa. Ensimmäinen tieteellinen konferenssi järjestettiin vuonna 1981 Santa Barbarassa, Yhdysvalloissa, ja se aloitti vuosittaisen *Crypto*-kongressien sarjan, joka jatkuu edelleen. Keväällä 1982 järjestettiin ensimmäinen eurooppalainen julkinen kryptologien tapaaminen Burg Feuersteinissa, Saksassa. Siitä jatkuu joka kevät eri Euroopan maissa järjestettävä *Eurocrypt*-kongressien sarja. Vuonna 1998 Eurocrypt-kongressi järjestettiin Suomessa, ja siinä oli noin 500 osanottajaa.

Oli kaksi tekijää, jotka merkittävästi vaikuttivat julkisen kryptografisen tutkimuksen laajenemiseen. Toinen oli epäilemättä DES-algoritmi, joka herätti alkuun suurta epäilyä, ja sen analysointi asetti merkittävän haasteen. Toinen oli mainittu Whitfield Diffien ja Martin Hellmanin vuonna 1976 ilmestynyt artikkeli, jossa he esittivät *julkisen avaimen menetelmän* periaatteen. Julkisen avaimen menetelmässä on kaksi avainta, joista toinen on salainen, vain avaimen omistajan tuntema parametri, jota kutsutaan myös *salaoveksi*, *trap-door*, ja toinen on julkinen, jota kuka tahansa voi käyttää turvalliseen asiointiin avaimen omistajan kanssa. Tiedon salaaminen tapahtuisi julkisella avaimella ja tulkinta vain käyttäen salaista avainta. Diffie ja Hellman huomasivat myös, että jos olisi mahdollista käyttää salaista avainta ensin, niin sillä voisi allekirjoittaa viestin, jonka sitten julkisella avaimella kuka tahansa voisi todentaa.

Tuo Diffien ja Hellmanin esittämä “matemaattisesti kaunis ajatus julkisesta avaimesta” kiehtoi matemaatikkojen mieliä (katso akateemikko Arto Salomaan haastattelu [27, s. 13]) ja herätti uusia teoreettisesti mielenkiintoisia kysymyksiä. Mutta myös käytännön tietojärjestelmien kehittyessä ja laajetessa niiden turvaamiseen liittyi monia uusia ongelmia. Siten salaamistekniikan tutkimuksen kehittyminen ja laajeneminen monipuoliseksi turvallisuusteknologiaksi oli luonnollisella tavalla sidoksissa tietotekniikan ja tietojenkäsittelytieteen voimakkaan kehityksen kanssa 1900-luvun viimeisinä vuosikymmeninä. Salaamistekniikkaa oli perinteisesti käytetty pelkästään tiedon luottamuksellisuuden turvaamiseen, mutta sen sovellusalue laajeni nopeasti.

Jo 1950-luvulla oli kehitetty salaamistekniikkaan perustuvia sotilaslentokoneiden välisiä tunnistusjärjestelmiä, *Identification of Friend or Foe*, *IFF* [5, s. 560][1], joissa käytettiin vuorovaikutteisia haaste–vaste -tunnistamisprotokollia ja sovellettiin symmetrisiä lohkosalakirjoitusmenetelmiä näiden protokollien turvaamiseen. Tällaisia tunnistusmenetelmiä sovellettiin edelleen tietokonejärjestelmiin, ja 1970-luvun alussa Roger Needham esitti, miten tietokonepalvelimeen tallennetut salasanataulukot voitaisiin turvata yksisuuntaisen funktion avulla [28, s. 91].

Muutamaa vuotta myöhemmin idea johti julkisen avaimen kryptologian syntyyn Diffien ja Hellmanin toimesta, siitä edelleen digitaalisiin allekirjoitusmenetelmiin ja myöhemmin mitä moninaisimpia turvapalveluja suorittaviin salaamisteknisiin protokolliin. Kun aikaisemmin salakirjoituksella suojattava viesti oli salaamisen pääasiallinen kohde, niin nykyaikaisissa salaamisteknisissä järjestelmissä ei useinkaan ole muuta salassa pidettävää kuin itse salainen avain, johon käyttäjän tunnistaminen perustuu. Näin on esimerkiksi matkapuhelinjärjestelmissä. Tilaajakohtainen salainen avain on tallennettuna

[1] Julkaistu myös teoksessa [6].

matkapuhelimen SIM-kortille, ja sen pääasiallinen tarkoitus on turvata, että kukin liittymä saa sille kuuluvat matkapuhelinpalvelut, ja että tilaajaa laskutetaan oikein vain käyttämiensä palveluiden perusteella.

Vähitellen salaamistekniikassa vallalla ollut sotilaallinen terminologia korvattiin paremmin siviilisovelluksiin ja tieteeseen sopivalla kielenkäytöllä. Esimerkiksi vihollisen asemesta puhutaan vastustajasta tai vain menetelmän ratkaisijasta. Enää ei puhuta hyökkäämisestä salaamismenetelmää vastaan sen murtamiseksi vaan yksinkertaisesti salaamismenetelmän ratkaisemisesta. Tämä ei kuitenkaan tarkoita sitä, että ratkaisija olisi jotenkin voimavaroiltaan heikompi kuin ennen, päinvastoin. Salaamisteknisessä tutkimuksessa oletetaan ratkaisijan omaavan kaikki tarvittavat keinot ja resurssit ja pyritään määrittämään ratkaisun kompleksisuus, eli sen vaatimien voimavarojen, laskentakapasiteetin ja -ajan määrä.

Kun salaamistekninen menetelmä julkistetaan, on eräs tärkeimmistä perusteluista menetelmän saaminen mahdollisimman laajan ja monipuolisen analysoinnin kohteeksi. Se on eräs tapa käytännössä pyrkiä approksimoimaan kaikkien mahdollisten, tunnettujen ja vielä keksimättömien, ratkaisumenetelmien saavuttamatonta kaikkivoipaisuutta. Kryptologisessa tutkimuksessa tunnetaan myös tieteellisesti pätevämpi tapa varmistua salaamisteknisen menetelmän turvallisuudesta käyttämällä reduktiota jostakin ennestään tunnetusta vaikeasta probleemista. Tällöin uutta salaamisteknistä menetelmää verrataan johonkin vanhaan, tunnetusti vaikeaan ongelmaan, ja pyritään osoittamaan, että uuden menetelmän ratkaiseminen johtaisi vanhan vaikean ongelman ratkaisuun.

4 Salaamistekniikan laskentavälineet

Tulevaisuuden uudet laskennalliset menetelmät, joista kvanttitietokoneet ja DNA-laskenta ovat jo ainakin teoriassa nähneet päivänvalon, mullistaisivat salaamismenetelmien turvallisuuden käsitteen, ja saattavat johtaa salaamistekniikan perusteiden uudelleenarviointiin. Nykyisin salaamismenetelmän katsotaan olevan turvallinen, jos sen ratkaisemiselle ei tunneta tehokkaampaa menetelmää kuin kaikkien mahdollisten avainten läpikäynti. Käytössä olevat binaariset tietokoneet pystyvät kokeilemaan yhden avaimen, tai korkeintaan suhteellisen pienen määrän avaimia kerrallaan. Kvantti- ja DNA-tietokoneet pystyvät ainakin joillekin probleemeille hakemaan kaikki ratkaisut yhdellä kertaa. Erityisesti silloin ovat vaaravyöhykkeessä eräät suosituimmat julkisen avaimen menetelmät. Mutta yleensä kvanttitietokoneen vaikutus näyttäisi olevan laskennallisen vaativuuden väheneminen neliöjuureen entisestään, mikä tarkoittaisi vain, että avaimen pituus tulisi kasvattaa kaksinkertaiseksi.

Historiallisesti tarkasteltuna ei ole mitään uutta siinä, että salaamistekniset menetelmät ovat aina sopeutuneet laskentaympäristöön ja tiedonvälityksen mediaan ja käyttäneet parhaiten muuhun tietojenkäsittely-ympäristöön istuvaa laskentatekniikkaa.

Seuraavasta, Herodotoksen muistiin merkitsemästä tarinasta on olemassa useita muunnelmia. Tässä esitettävä versio on yhdistelmä joistakin Internetissä esiintyvistä tarinan muodoista (katso myös [24, s. 14]). Vuonna 495 eKr. kreikkalainen itsevaltias Histiaeus oli pidätettynä Persian kuninkaan Dariuksen hovissa Susassa. Hän halusi lähettää vävylleen Aristagorasille Miletuksen kaupunkiin Ana-

toliaan salaisen viestin kehottaakseen tätä lähettämään sotajoukkoja Dariusta vastaan. Histiaeus kutsui luokseen orjan, ajoi hänen päänsä paljaaksi ja tatuoi viestin orjan päänahkaan. Orjalle kerrottiin, että kysymyksessä oli hoito tämän heikentyneen näön parantamiseksi. Sitten Histiaeus odotti muutaman viikon, että hiukset jälleen peittivät orjan pään, ja lähetti orjan matkaan kohti Miletuksen kaupunkia. Orjalle uskoteltiin, että hänen näkönsä paranisi ennalleen, kun hän antaisi Aristagorasin ajaa hiuksensa uudelleen ja lukea mitä hänen päänahkaansa oli kirjoitettu. Tämä tarina on ensimmäisiä esimerkkejä *steganografiasta* eli viestin piilottamisesta. Sovellettuna nykyaikaiseen mediaan steganografia on löytänyt itselleen aivan uudet ulottuvuudet Internetin määrättömissä bittivirroissa.

Histiaeuksen käyttämästä salaamistekniikasta on vaikea löytää mitään matematiikkaan viittaavaa, eikä steganografiaa varsinaisesti luetakaan kryptografiseksi menetelmäksi. Kuitenkin jo samoihin aikoihin Spartassa sotapäällikköjen välisessä viestinnässä oli käytössä menetelmä, jolla viestin kirjaimet pystyttiin tehokkaasti sekoittamaan, ja joka voidaan tulkita matemaattisin termein, matriisien avulla. Menetelmä oli seuraavanlainen. Pergamentista valmistettu suikale kierrettiin sauvan ympärille, ja viesti kirjoitettiin suikaleelle sauvan pituussuuntaan. Tulkitakseen viestin vastaanottajalla tuli olla alkuperäisen kanssa täsmälleen samanpaksuinen sauva. Menetelmä tunnetaan nimellä *scytale*, sauva. Jos nauhaa on kierretty sauvan ympärille m kertaa ja sauvan ympäri mahtuu n kirjainta, niin sama kirjainten sekoitus saadaan, jos viestin kirjaimet kirjoitettaisiin m rivin ja n sarakkeen muodostamaan matriisiin sarakkeille ja salattu viesti luetaan matriisista riveittäin. Vain hieman edistyneempi on menetelmä, jossa sarakkeiden keskinäistä järjestystä muutetaan ennen salakielisen tekstin lukemista matriisista. Tällaisia menetelmiä oli käytössä vielä ensimmäisessä maailmansodassa.

Elektronisten viestintälaitteiden integroidut salaamismenetelmät pantiin usein kokoon samoista elektronisista komponenteista, joita oli saatavilla, ja joista laite oli muutenkin rakennettu. Silloin radioteknisten koodausmenetelmien käyttämä matematiikka, eli koodausteoria, lainasi ratkaisujaan salaamismenetelmille. Ohjelmistollisesti toteutettaviin salaamismenetelmiin kohdistuvat taas aivan toisenlaiset vaatimukset, ja toisenlaiset funktiot ja matemaattiset rakenteet ovat edullisia. Nykyisin laajoissa yleisissä järjestelmissä käytettävät salaamistekniset algoritmit “valetaan rautaan” eli valmistetaan algoritmille oma, *dedikoitu* prosessori, joka suorittaa vain kyseistä algoritmia. Näin voidaan optimoida algoritmin suorituskyky ja turvallisuus sekä ottaa mahdollisimman hyvin huomioon tärkeät salaamismenetelmän käyttöympäristöstä johtuvat rajoitukset, kuten virrankulutus ja avainten vaihdosta johtuvat tekijät.

Kommunikaatiojärjestelmien siirtyminen langattomaan teknologiaan ja pyrkimys ihmisten välisten sitoumusten suorittamiseen ilman paperikuitteja ovat johtaneet salaamistekniikan käytön nopeaan yleistymiseen. GSM-järjestelmän matkapuhelimessa tilaaja tunnistetaan sirukortin prosessorille ohjelmoidulla *autentikointialgoritmilla* ja sirukortille tallennetun tilaajakohtaisen salaisen avaimen perusteella. Sirukortit ovatkin eräs tärkeimmistä käytössämme olevista salaamisteknisistä välineistä.

Jokaisessa GSM-järjestelmän matkapuhelimessa on myös dedikoidulle piirille toteutettu salakirjoitusalgoritmi, jolla turvataan matkapuhelimen ja tukiaseman vä-

linen langaton yhteys. Salakirjoittamiseen käytettävä avain johdetaan autentikoinnin yhteydessä. Langattoman yhteyden salakirjoittamisella on GSM-järjestelmässä kaksi tarkoitusta. Ensinnäkin se turvaa, ettei tilaajan avaamaa puhelinyhteyttä autentikoinnin jälkeen voi kaapata jonkin muun puhelun suorittamiseen, ja toiseksi se estää puhelun salakuuntelemisen matkapuhelimen ja tukiaseman väliltä.

Ensimmäinen GSM-järjestelmässä käytetty salakirjoitusalgoritmi A5 suunniteltiin 1980-luvun lopulla. Sitä ei ole virallisesti julkaistu, mutta tutkijat ovat pystyneet selvittämään sen toiminnan matkapuhelimen tuottaman salakirjoitetun signaalin ja joidenkin algoritmin suunnittelun alkuvaiheessa vuotaneiden luonnosten perusteella. Kolmannen sukupolven matkapuhelinjärjestelmän salaamistekniset algoritmit ovat sen sijaan alusta alkaen olleet julkisia [29], ja niitä koskevia tutkimuksia on esitetty ja arvioitu kryptologian tieteellisissä kongresseissa ja julkaisuissa.

5 Sähköinen asiointi

Digitaalisten allekirjoitusten, jotka mahdollistavat digitaalisessa muodossa olevien sopimusten, transaktioiden ja muiden vastaavien sitoumusten todennettavissa olevan allekirjoittamisen, katsotaan yleisesti olevan eräs sähköisen asioinnin teknologinen kulmakivi. Salaamistekniseen tutkimuksen tehtävänä on arvioida erilaisten allekirjoitusmenetelmien ja niissä käytettävien koodausmenetelmien turvallisuutta ja soveltuvuutta erilaisiin sähköisen asioinnin järjestelmiin.

Suurin osa sähköisen kaupankäynnin ja sähköisen asioinnin järjestelmistä perustuu vanhoihin käytäntöihin, ja kryptografian tehtävänä on ollut vanhojen paperipohjaisten turvallisuusrutiinien korvaaminen niiden sähköisillä vastineilla. Digitaaliset allekirjoitusmenetelmät ovat olleet olemassa jo parikymmentä vuotta. Täydellisen vastaavuuden saavuttaminen ei ole ollut ongelmatonta ja on vienyt aikaa. Vaikka asiaa on yritetty edistää myöskin lainsäädännön keinoin, eivät digitaaliset allekirjoitusmenetelmät ole vielä yleisessä käytössä henkilöiden välisessä asioinnissa. Suurin osa Internetin kauppapaikoista perustuu perinteiseen ideaan *à la* Amazon.com, mutta modernia salaamistekniikkaa voidaan käyttää myös mielenkiintoisemmin vaikkapa huutokaupan toteuttamiseen (http://www.ebayliveauctions.com/).

6 Nykyaikainen kryptologinen tutkimus

Salaamistekniikkaa käytetään oleellisena osana nykyaikaista tietoturvallisuustekniikkaa. Avainten pituuksista, heikkouksista ja vahvuuksista käydään keskustelua jopa lehtien palstoilla. Salaamisteknisen algoritmin turvallisuus on kuitenkin hyvin vaikeasti määriteltävissä ja arvioitavissa oleva asia, eikä sitä voi tyhjentävästi esittää minkään yksittäisen tunnusluvun, kuten esimerkiksi avaimen pituuden avulla. Avaimen pituus antaa kuitenkin erään yläarajan menetelmän ratkaisemiseen vaadittavalle työlle ja soveltuu siten Wassenaar-järjestelyn tarkoituksiin.

Myös algoritmin toteutukseen kohdistuu mitä moninaisimpia turvallisuusvaatimuksia. Esimerkiksi, jos salaamisalgoritmi vaatii salattavan datan tietynpituisina lohkoina, niin ei ole suinkaan samantekevää, kuinka vajaaksi jäävät lohkot täydennetään. Jäljempänä esitetään tästä esimerkki, jossa pitkään käytössä ollut standardimenettely joutui yllättäen uudelleenarvioinnin kohteeksi.

Salaamistekniset menetelmät jaetaan

yleensä kahteen luokkaan, symmetrisiin ja epäsymmetrisiin. Symmetrisessä menetelmässä on yksi salainen avain, jota eri osapuolet käyttävät. Epäsymmetrisessä menetelmässä eri osapuolilla on käytössään oleellisesti erilaisia avaimia. Kaksi avainta on oleellisesti erilaisia, kun ei ole olemassa tehokkaita algoritmeja, joilla yhdestä avaimesta voidaan johtaa toinen.

Avainten erilaisuuden lisäksi jakoon vaikuttaa muita tekijöitä. Symmetristen menetelmien historia on pitkä, niitä on käytetty kautta aikojen. Niissä käytetyt salaamiseen vaadittavat sekoitus- ja korvausfunktiot on pantu kokoon erilaisista osasista, joilla tiedetään olevan salausteknisesti toivottuja ja hyödyllisiä ominaisuuksia. Symmetrisen salaamistekniikan kehittämät vaikeasti ratkaistavat ongelmat ovat insinööriteknisiä rakennelmia. Mitä kauemmin ne ovat olleet olemassa ja pysyneet pystyssä niihin kohdistetuista hyökkäyksistä huolimatta, sitä suurempi on luottamus niitä kohtaan. Julkisen avaimen menetelmien historia alkoi vasta 1970-luvulla. Julkisen avaimen menetelmän turvallisuus perustuu pääsääntöisesti johonkin tunnetusti laskennallisesti vaikeaan tehtävään, siis matematiikkaan. Insinööriteknistä lähestymistapaa on kyllä myöskin yritetty, mutta toistaiseksi siten kokoonpannut epäsymmetriset algoritmit eivät ole olleet riittävän vahvoja, tai sitten avaimista on tullut epäkäytännöllisen pitkiä.

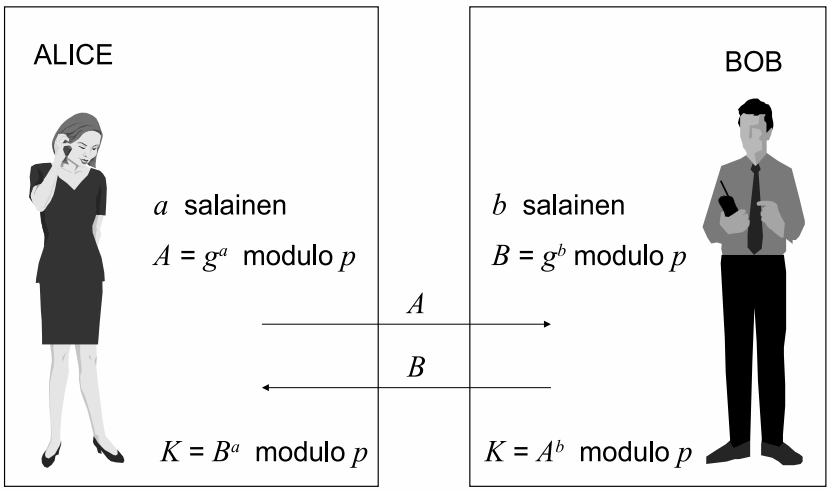
Toinen merkittävä ero on symmetristen ja epäsymmetristen salaamisteknisten algoritmien käyttöalueet sovelluksissa ja niistä johtuvat erilaiset turvallisuusvaatimukset ja ratkaisumallit.

7 Kryptologista matematiikkaa

Tietotekniikassa, tietokoneiden ohjelmoinnissa ja kommunikaatiotekniikassa käytetään soveltuvimmin määräpituisia rakenteita. Niinpä myös salaamistekniset operaatiot kohdistuvat määräpituisiin datalohkoihin. Tästä johtuen käytetyt matemaattiset struktuurit perustuvat äärellisiin algebrallisiin objekteihin, äärellisiin ryhmiin, lineaariavaruuksiin, renkaisiin tai kuntiin. Käytännössä tämä johtaa modulaariseen laskentaan, tavallisimmin jäännösluokkarenkaassa jonkin kokonaisluvun suhteen tai Galois-kunnassa jonkin jaottoman polynomin suhteen.

Olkoon n kokonaisluku. *Jäännösluokkarengas modulo n* voidaan ajatella muodostuvaksi ei-negatiivisista lukua n pienemmistä kokonaisluvuista. Kun halutaan laskea lukujen a ja b summa, lasketaan se ensin tavallisessa kokonaislukujen mielessä $a+b$. Mikäli saatu summa on suurempi tai yhtäsuuri kuin n, vähennetään siitä luku n, jolloin saadaan lukua n pienempi luku, joka on modulo n jäännösluokkarenkaan alkio. Saatu luku on lukujen a ja b summa modulo n. Samaan tapaan lasketaan lukujen a ja b tulo, ensin laskemalla kokonaislukujen a ja b tulo ja sen jälkeen vähentämällä tulosta ab luku n niin monta kertaa kuin mahdollista, eli muodostamalla luvun ab jakojäännös jakajan n suhteen.

Binäärisessä Galois-kunnassa $GF(2^m)$ lasketaan suoraan bittijonoilla, joiden pituus on m. Avuksi tarvitaan jokin astetta m oleva jaoton polynomi $\pi(x)$. Bittijonot ajatellaan astetta $m-1$ oleviksi polynomeiksi, joiden kertoimet ovat 0 tai 1, ja joita voidaan laskea yhteen, kertoa keskenään ja jopa jakaa toisillaan. Polynomien välisen laskutoimituksen tulos, joka on siis jokin {0,1}-kertoiminen polynomi, jaetaan polynomilla $\pi(x)$, jolloin saadaan



Kuva 1: Alice ja Bob muodostamassa yhteistä avainta Diffie-Hellmanin menetelmällä

jakojäännös, jonka aste on pienempi kuin m.

8 Julkisen avaimen salaamistekniikasta

Diffien ja Hellmanin uraa uurtavassa artikkelissaan esittämä ensimmäinen julkisen avaimen menetelmä oli kaksivaiheinen, vuorovaikutteinen protokolla, jota käyttäen kaksi osapuolta voi sopia yhteisestä salaisesta avaimesta lähettämällä toisilleen vain julkisia viestejä.

Protokollan alussa osapuolet, Alice ja Bob, sopivat, että he käyttävät alkulukua p ja suorittavat laskunsa tämän alkuluvun suhteen, siis jäännösluokkarenkaassa modulo p. Lisäksi he valitsevat jonkin lukua p pienemmän luvun g, joka on kuitenkin suurempi kuin 1. Tämä neuvottelu ja luvuista p ja g sopiminen voi tapahtua mitä tahansa viestintämenettelyä käyttäen.

Sen jälkeen suoritetaan salaisia toimenpiteitä. Alice valitsee jonkin luvun a, jota valintaa ei kukaan ulkopuolinen, ei edes Bob, pysty ennakoimaan. Alice korottaa luvun g luvun a ilmoittamaan potenssiin ja suorittaa kaikki laskut modulo p. Merkitään tulosta symbolilla A. Aivan samalla tavalla Bob valitsee jonkin luvun b ja laskee g^b modulo p, jota merkitsemme symbolilla B.

Alice lähettää luvun A Bobille ja Bob lähettää luvun B Alicelle. Sen jälkeen Alice laskee B^a modulo p ja Bob A^b modulo p. Nämä luvut ovat yhtäsuuret, sillä eksponentointi on vaihdannainen laskutoimitus myös modulaariaritmetiikassa, eli $(g^a)^b = (g^b)^a = g^{ab}$ modulo p. Näin Alice ja Bob ovat muodostaneet yhteisen tiedon vain julkista kommunikaatiota käyttäen.

Toisaalta uskotaan, että tällä menetelmällä laskettu salainen tieto on vain Alicen ja Bobin tiedossa. Jos olisi olemas-

sa menetelmä, jolla luvuista A, g ja p voitaisiin laskea a, jota myös kutsutaan luvun A *diskreetiksi logaritmiksi* kannan g suhteen, niin silloin luvuista A, B, g ja p voisi johtaa Alicen ja Bobin saaman yhteisen avaimen. Mutta tällaista menetelmää ei tunneta. Kun p valitaan tarpeeksi suureksi, niin kaikki tunnetut menetelmät diskreetin logaritmin määrittämiseksi ovat ylivoimaisen työläitä. Kaikki muutkin tunnetut tavat johtaa g^{ab} modulo p luvuista A, B, g ja p ovat liian työläitä. (Helposti nähdään, että menetelmä ei ole ollenkaan turvallinen, jos jompikumpi luvuista A tai B sattuu olemaan yhtäsuuri kuin 1. Itse asiassa se, että näin kävisi, voidaan estää valitsemalla g sopivalla tavalla.)

Edellä kuvatussa mielessä siis funktio, joka luvusta a laskee luvun $A = g^a$ modulo p, on *yksisuuntainen*. Tätä vaikeaa tehtävää, joka annetuista luvuista p, g ja $A = g^a$ modulo p laskee luvun a, kutsutaan *diskreetin logaritmin probleemiksi*.

Diffien ja Hellmanin saavutuksen merkitys oli siinä, että he osoittivat, kuinka yksisuuntaisista funktioista voisi olla hyötyä salaamistekniikassa. Pienelläkin laskentaresurssilla voitaisiin suorittaa lasku toiseen suuntaan, kun taas toiseen suuntaan se ei onnistu järkevässä ajassa edes vahvimmalla supertietokoneella. Eksponentointi on mahdollisesti tällainen yksisuuntainen funktio. Jos se ei ole yksisuuntainen, niin Diffie-Hellmanin avaintenvaihtomenetelmä ei ole turvallinen. On kuitenkin avoin kysymys, redusoituuko diskreetin logaritmin probleemi Diffie-Hellmanin avaintenvaihtomenetelmän ratkaisuun.

Diffie ja Hellman hahmottelivat edelleen julkisen avaimen menetelmän ideaa rohkenematta kuitenkaan antaa mitään konkreettista esimerkkiä tällaisista menetelmistä. Kesti vuoteen 1985 saakka, jolloin Hellmanin oppilas Taher ElGamal esitti ensimmäisen diskreetin logaritmin probleemiin perustuvan epäsymmetrisen salakirjoitusmenetelmän ja digitaalisen allekirjoitusmenetelmän [8]. ElGamalin allekirjoitusmenetelmä on sikäli merkittävä, että sen pohjalta on kehitetty DSA-menetelmä, joka on amerikkalainen standardi (viimeisin laitos, katso [15]) ja toinen kahdesta yleisimmin käytetystä digitaalisesta allekirjoitusmenetelmästä. Toinen on RSA-menetelmä, jota tarkastelemme seuraavaksi.

Ron Rivest, Adi Shamir ja Leonard Adleman esittivät ensimmäisen konkreettisen esimerkin salaovella varustetusta yksisuuntaisesta funktiosta [22]. Se ei perustunut diskreetin logaritmin probleemiin vaan suurten kokonaislukujen tekijöihin jakamisen vaikeuteen. Mitä suurempia luvun tekijät ovat, sitä vaikeampi niitä on löytää. Optimaalinen tilanne syntyy, kun kaksi erisuurta alkulukua kerrotaan keskenään. Olkoot p ja q kaksi erisuurta alkulukua ja $n = pq$ niiden tulo. Lisäksi RSA-menetelmä käyttää kahta eksponenttia e ja d, joilla on sellainen ominaisuus, että

$$x^{ed} = (x^e)^d = (x^d)^e = x \text{ modulo } n,$$
kaikilla kokonaisluvuilla x.

Siis funktiot x^e modulo n ja x^d modulo n ovat toistensa käänteisfunktioita. Vielä merkityksellisempää on, että, jos tunnetaan eksponentti e mutta luvun n tekijät p ja q ovat tuntemattomat, niin ei tiedetä mitään tehokasta menetelmää eksponentin d laskemiseksi tai muulla tavoin funktion x^e modulo n käänteisfunktion määräämiseksi. Niinpä, kun tunnetaan e ja n, voidaan mikä tahansa viesti x salata muotoon $C = x^e$ modulo n. Uskotaan, että tästä salatusta muodosta C viestin x pystyy ratkaisemaan vain eksponenttia d käyttäen. Siten RSA on julkisen avaimen salaamismenetelmä, jonka julkisen avaimen muodostaa pari (n,e) ja salaisen avaimen (n,d).

Kokonaisluvun n tekijät p ja q voidaankin nyt vaikka unohtaa, ja jos näin tehdään, voi olla, ettei niitä koskaan enää pystytä löytämään. Käytännössä kuitenkin laskujen nopeuttamiseksi tieto luvun n tekijöistä usein säilytetään.

Edellä nähtiin, että funktiot x^e modulo n ja x^d modulo n ovat toistensa käänteisfunktioita. Siis ne voidaan suorittaa myös toisessa järjestyksessä. Korotetaan viesti x ensin salaisen eksponentin d ilmoittamaan potenssiin, jolloin saadaan $S = x^d$ modulo n. Tätä lukua S kutsutaan viestin x allekirjoitukseksi, ja sen pystyy muodostamaan vain käyttäjä, jolla on tiedossaan salainen eksponentti d. Ja lisäksi, mikä tärkeintä, tämä allekirjoitus voidaan tarkastaa. Kun S korotetaan potenssiin e ja redusoidaan tulos modulo n, pitäisi tulokseksi tulla x, mikäli allekirjoitus oli oikein muodostettu. Siis RSA toimii myös digitaalisena allekirjoitusmenetelmänä.

9 Äänestämisen salaamistekniikkaa

Julkisen avaimen ajatusta on menestyksellisesti hyödynnetty muutettaessa yhteiskunnan ja liiketoiminnan asiointirutiineja paperilta sähköiseen muotoon. Eräs mielenkiintoinen sovellus on sähköinen äänestäminen. Turvallisilta vaaleilta vaaditaan seuraavat ominaisuudet:

1. Vain äänioikeutetut kansalaiset saavat äänestää.
2. Jokaisella äänioikeutetulla on vain yksi ääni.
3. Vaalisalaisuus on turvattava.
4. Kukaan ei saa äänestää jonkun toisen antaman äänen mukaisesti tietämättä, mikä annettu ääni on.
5. Kukaan ei saa muuttaa kerran antamaansa ääntä.
6. Äänestäjä voi varmistua siitä, että hänen äänensä on laskettu.

Suomalaisten tutkijoiden kehittämä äänestysprotokolla [17] on yksi parhaista nämä vaatimukset täyttävistä protokollista. Sillä on edellä mainitut kuusi ominaisuutta siten, että viidettä ja kuudetta ominaisuutta on vielä vahvennettu seuraavasti:

5′. Äänestäjä voi muuttaa mielensä ja vaihtaa kerran antamaansa ääntä tietyn ajan kuluessa.

6′. Jos äänestäjä havaitsee virheen äänten laskennassa oman äänensä kohdalla, hän voi korjata asian paljastamatta sitä, kuinka hän on äänestänyt.

Perinteisellä vaalitavalla on lisäksi se ominaisuus, että äänestäjälle ei jää äänestämistapahtuman jälkeen mitään keinoa todistaa äänestäneensä tietyllä tavalla. Tämä on tärkeää yleisissä vaaleissa, kun halutaan estää äänten ostaminen tai muunlainen pakottaminen äänestämään tietyllä tavalla. Niemi ja Renvall ovat kehittäneet äänestysprotokollan, jolla on tämä ominaisuus mainittujen ominaisuuksien 1–6 lisäksi [16].

10 Salaamistekniikan soveltaminen käytäntöön

Edellä esitettiin RSA-menetelmän periaate. Tästä on vielä pitkä matka ennenkuin käsillä on menetelmä, jota voidaan turvallisesti soveltaa käytännön tietoturvallisuusjärjestelmiin. Jo heti nähdään ensimmäinen heikkous RSA-allekirjoitusmenetelmässä. Valitsemalla

viestiksi $x = y^e$ modulo n, sen täysin oikea allekirjoitus on y. Siis tuntematta salaista eksponenttia kuka tahansa voi muodostaa viestejä ja niille oikeita allekirjoituksia. Tätä kutsutaan allekirjoitusmenetelmän *eksistentiaaliratkaisuksi*, ja sen onnistumista ei voida sallia. Yleisimmin käytetty menetelmä eksistentiaaliratkaisun estämiseksi on, että allekirjoitettuun viestiin lisätään määrämuotoista tietoa, eli redundanssia. Kun allekirjoitusta tarkastettaessa viesti x saadaan lasketuksi, niin heti varmistetaan, että siinä oleva redundanssi on oikean muotoista.

RSA-menetelmän käytön yksityiskohdat on määritelty standardissa PKCS #1 v 2.0 [23]. Viestin salaamiseen on määritelty kaksi vaihtoehtoista menetelmää, joilla viesti valmistetaan eli koodataan salaamisoperaatiota varten. Tarkastellaan näistä toista, EME-PKCS1-v1_5-menetelmää. Salattavan viestin pituus riippuu RSA-moduulin n pituudesta k, joka lasketaan sen mukaan, kuinka monta *oktettia*, 8 bitin lohkoa eli tavua, tarvitaan luvun n esittämiseen binäärisessä muodossa eli bittijonona. Kun RSA-moduulin pituus on k, on salattavan viestin pituus korkeintaan $k-11$ oktettia. Koodauksessa siihen lisätään kymmenen oktettia, kuten kohta kerrotaan. Merkitään salattavaa viestiä symbolilla M ja valmiiksi koodattua viestiä symbolilla EM, *encoded message*. Koodatun viestin pituus on $k-1$ oktettia. Tämä rajoitus on asetettu sen vuoksi, että koodatun viestin muodostama bittijono kokonaisluvuksi muutettuna olisi varmasti pienempi kuin RSA-moduuli n.

Menetelmä vaatii kahdeksan tavun pituisen jonon satunnaisesti valittuja bittejä. Tätä jonoa standardissa merkitään symbolilla PS, *pseudorandom sequence*, ja sillä on seuraavat RSA-menetelmän turvallisuuteen vaikuttavat tehtävät. Ensinnäkin sillä varmistetaan, että koodattu viesti on aina suuri luku. Nimittäin tehokkuuden takia saattaa olla edullista valita julkinen eksponentti e pieneksi luvuksi. Jos salattavat viestit itse ovat pieniä lukuja, niin modulaarista reduktiota ei tule suoritetuksi kertaakaan, jolloin salatun viestin tulkinta ei ole sen kummempi tehtävä kuin tavallinen juuren ottaminen kokonaisluvuille.

Toinen PS-lohkon tehtävä on laajentaa viestiavaruutta ja tasoittaa eri viestien esiintymistodennäköisyyksiä. Käytännössä usein jotkin viestit ovat paljon todennäköisempiä kuin toiset, jolloin selväkielisen viestin ratkaiseminen saattaa onnistua arvaamalla. Erikoistapaus epätasaisesta jakaumasta syntyy, jos vain hyvin pieni osa viesteistä yleensä voi esiintyä. Silloin ei ratkaisijan tarvitse tehdä muuta kuin salata kaikki viestit ja muodostaa niistä sanakirjamainen luettelo. Tällaista ratkaisua kutsutaankin *sanakirjaratkaisuksi* (*dictionary solution*). Kun salattavien viestien joukko on pieni, suositellaankin, että jokaista salaamiskertaa varten muodostetaan uusi ja ennakoimaton lohko PS.

Standardin EME-PKCS1-v1_5 mukainen koodattu viesti on

$$EM \;=\; 02 \,\|\, PS \,\|\, 00 \,\|\, M,$$

missä merkintä $\|$ tarkoittaa oktettijonojen liittämistä toisiinsa eli *katenaatiota*. Numeropari 02 on oktetin 0000 0010 esitys 16-kantaisessa lukujärjestelmässä, ja 00 tarkoittaa pelkkien nollabittien muodostamaa oktettia.

Alussa todettiin, että RSA-menetelmä, kuten useimmat muutkin julkisen avaimen menetelmät, tukeutuu matematiikan tarjoamiin vaikeisiin probleemeihin. RSA-menetelmän perustana oleva laskennallisesti vaikea probleemi on suurten lukujen tekijöihin jakaminen. Kuitenkaan se pelkästään ei riitä, vaan RSA-järjestelmän turvallinen käyttö vaatii edellä kuvatun

kaltaisia virityksiä, joiden turvallisuus ei ole matemaattisesti todistettavissa vaan perustuu salaamistekniseen tutkimukseen.

EME-PKCS1-v1_5 on kaikkein yleisimmin käytössä oleva RSA-salauksessa käytetty koodausmenetelmä. Se ei kuitenkaan ole aivan aukoton, ja sen käyttö voi jopa eräissä tapauksissa tarjota mahdollisuuden salatun viestin ratkaisemiseen ilman salaista avainta. Seuraavassa esitetään Daniel Bleichenbacherin esittämä menetelmä selväkielen määrittämiseksi [2]. Se perustuu siihen EME-PKCS1-v1_5-menetelmän ominaisuuteen, että koodattu viesti on kokonaisluvuksi tulkittuna lukujen $2 \cdot 2^{8(k-2)}$ ja $3 \cdot 2^{8(k-2)}$ välillä, missä k on RSA-moduulin n pituus oktetteina. Bleichenbacherin menetelmä edellyttää, että ratkaisija voi lähettää suuren määrän itse valitsemiaan salakieliviestejä, jotka eivät ole oikealla tavalla salattuja, ja joista vastaanottaja ilmoittaa lähettäjälle, onnistuiko tulkinta vai ei.

Kutsutaan ratkaisijaa nimellä Daniel ja RSA-menetelmän salaisen avaimen (d,n) haltijaa nimellä Alice. Daniel saa käsiinsä Alicelle lähetetyn RSA-menetelmällä salatun viestin C, joka on siis kokonaisluku ja lukua n pienempi. Alicelle lähetetty viesti M on koodattu menetelmällä EME-PKCS1-v1_5, ja merkitään symbolilla x kokonaislukua, joka saadaan, kun koodattu viesti EM tulkitaan kokonaisluvuksi. Siis $x = C^d$ modulo n.

Riittää siis, kun Daniel selvittää luvun x. Sitä varten hän valitsee suuren joukon erilaisia lukua n pienempiä kokonaislukuja S. Jokaiselle luvulle S hän laskee $C' = CS^e$ modulo n ja lähettää tuloksen C' Alicelle. Alice yrittää tulkita saamansa viestin ja suorittaa laskun $(C')^d$ modulo n. Kuten heti nähdään

$$(C')^d \;=\; (CS^e)^d \;=\; xS \text{ modulo } n.$$

Ei voida olettaa, että Alice kertoisi tämän tuloksen Danielille, mutta sen sijaan useissa tietoturvallisuusjärjestelmissä Daniel saa välittömästi tiedon, onko viesti mennyt perille. Jos Alice on pystynyt tulkitsemaan viestin, niin se tarkoittaa, että luku xS (redusoituna modulo n) noudattaa EME-PKCS1-v1_5-koodausta. Siis Daniel tietää, että

$$2 \cdot 2^{8(k-2)} \;\leq\; xS \text{ modulo } n \;<\; 3 \cdot 2^{8(k-2)}.$$

Keräämällä suuren joukon näitä epäyhtälöitä, Bleichenbacherin arvion mukaan niitä tarvittaisiin noin 2^{20} kappaletta eli noin miljoona, Daniel pystyy ratkaisemaan luvun x.

Tällainen ratkaisu saattaa hyvinkin olla mahdollinen, jos Alice on verkossa oleva palvelin, joka automaattisesti hoitaa tehtäväänsä. Toisaalta vaaditaan myös, että tietoturvaprotokolla, jonka osana palvelin suorittaa RSA-tulkintaoperaatiota, välittää lähettäjälle tiedon onko tulkinta onnistunut. Itse asiassa tällaisia RSA-menetelmää käyttäviä sovelluksia, esimerkiksi *SSL*, on ollut ja on edelleenkin käytössä. SSL eli *Secure Sockets Layer* on yleisesti muun muassa pankkien asiakasyhteyksien turvaamisessa käytetty protokolla. Bleichenbacherin ratkaisun onnistuminen voidaan kuitenkin estää lisätoimenpitein, esimerkiksi keskeyttämällä saman lähettäjän suorittamat peräkkäiset kyselyt palvelimelle, jos ilmaantuu useita viestejä, joita ei pystytä tulkitsemaan.

11 Symmetrisestä salaamistekniikasta

Kun sama tieto salaisesta avaimesta on sekä Alicella että Bobilla, sanotaan, että kryptografinen menetelmä on symmetrinen. Voi olla, että Alice ja Bob käyttävät salaista avainta eri muodossa, mut-

ta kumpikin voi halutessaan johtaa toisen käyttämän avaimen omastaan tehokkaasti laskettavissa olevalla algoritmilla. Näinhän ei ole epäsymmetrisen menetelmän tapauksessa. Yleisimmin käytetyt salakirjoitusmenetelmät, kuten DES-algoritmi, ovat symmetrisiä menetelmiä.

Tarkastellaan seuraavaa diskreetin logaritmin probleemiin perustuvaa symmetristä salakirjoitusmenetelmää, jonka Pohlig ja Hellman esittivät vuonna 1978 [21]. Olkoon p alkuluku. Alice ja Bob sopivat keskenään salaisesta luvusta d ja määrittävät sitä vastaavan luvun e, jolle pätee, että

$$x^{ed} = (x^e)^d = (x^d)^e = x \text{ modulo } p,$$
kaikilla kokonaisluvuilla x.

Tämä on helppoa, kun p on alkuluku. (Tämä ei ole ristiriidassa sen kanssa, että edellä RSA-menetelmän tapauksessa luvun e määrittäminen luvusta d on vaikeaa, koska aiemmin moduulina oli yhdistetty luku n, jonka alkutekijöitä ei tunnettu.) Edelleen Alice ja Bob sopivat, että Alice käyttää eksponenttia e ja Bob käyttää eksponenttia d. Silloin Alice voi salakirjoittaa viestin x muodostamalla luvun x^e modulo p, jonka Bob tulkitsee korottamalla sen eksponentin d ilmoittamaan potenssiin. Selvästikin menetelmä toimii myös toisin päin, eli Bob voi salakirjoittaa viestejä eksponentilla d, jotka Alice sitten tulkitsee eksponentilla e.

Salaisen avaimen ratkaiseminen Pohligin ja Hellmanin symmetrisessä salaamismenetelmässä on ainakin yhtä vaikeaa kuin diskreetin logaritmin ratkaiseminen kannan x suhteen modulo p, siis tässä mielessä todistettavasti turvallinen. Lisäksi se tarjoaa merkittävän edun, jota ei ole esimerkiksi DES-algoritmilla. Se on skaalautuva, eli menetelmän vahvuutta voidaan parantaa yksinkertaisesti kasvattamalla lukua p.

Miksei Pohlig-Hellmanin menetelmä sitten ole laajassa käytössä? Miksi mieluummin valittiin *ad hoc* -menetelmistä, sekoituksista ja korvausmenetelmistä rakennettu DES-algoritmi kuin kaunis matemaattinen ratkaisu? Syynä on yksinkertaisesti merkittävä ero soveltuvuudessa laskettavaksi tietokoneilla ja prosessoreilla. Symmetriset salaamistekniset menetelmät on kautta aikojen rakennettu sellaisista operaatioista, jotka parhaiten soveltuvat suoritettavaksi käytössä olevilla laskentavälineillä. Tämä ei kuitenkaan täysin sulje pois matematiikan hyväksikäyttöä tehokkaiden symmetristen salakirjoitusmenetelmien suunnittelussa. Koodausteoria on jo Shannonin ajoista lähtien tehokkaasti hyödyntänyt matemaattisia sommitelmia erityisesti virheenkorjauskoodien ja spektrin hajoituskoodien suunnittelussa, siis suorittamaan joitakin hyvin määriteltyjä tehtäviä.

Ongelma on siinä, että kryptografian vaatimukset matematiikalle eivät ole, eivätkä koskaan tule täysin olemaankaan, hyvin määriteltyjä. Shannonin mukaan salaamisteknisen menetelmän voisi rakentaa yksinkertaisista, pienistä osista, jotka suorittaisivat bittien keskinäistä sekoitusta ja bittilohkojen korvaamista toisilla. Näitä tehtäisiin vuoronperään kunnes tulos olisi turvassa selvitysyrityksiltä. DES-algoritmin merkitys tieteelle on siinä, että se antoi tutkijoille materiaalia pyrittäessä tarkentamaan Shannonin vaatimuksia ja selvittämään, mitä vahvalta symmetriseltä salaamismenetelmältä tarkkaan ottaen vaaditaan.

12 DES-algoritmin kryptoanalyysia

Kuluneen kahden vuosikymmenen aikana on esitetty useita DES-algoritmiin kohdistuneita analyysimenetelmiä, mutta niis-

tä kaksi on merkitykseltään aivan omaa luokkaansa, differentiaalinen kryptoanalyysi [1] ja lineaarinen kryptoanalyysi [14]. Molemmat menetelmät soveltuvat minkä tahansa iteroidun lohkosalausmenetelmän analysointiin.

Iteroitu lohkosalausalgoritmi koostuu kierroksista, joita on ennalta sovittu määrä. Yksi kierros koostuu funktiosta, jonka syötteinä on datalohko ja kierrosavain ja tuotoksena datalohko. Ensimmäisen kierroksen syötedata on salattava selväkielinen datalohko, ja viimeisen kierroksen tuotos on salakielinen datalohko. Muiden kierrosten syötedatalohkot ovat edellisen kierroksen tuotosdatalohkot. Kierrosavaimet muodostetaan salausavaimesta kierrosavainten generointimenettelyllä.

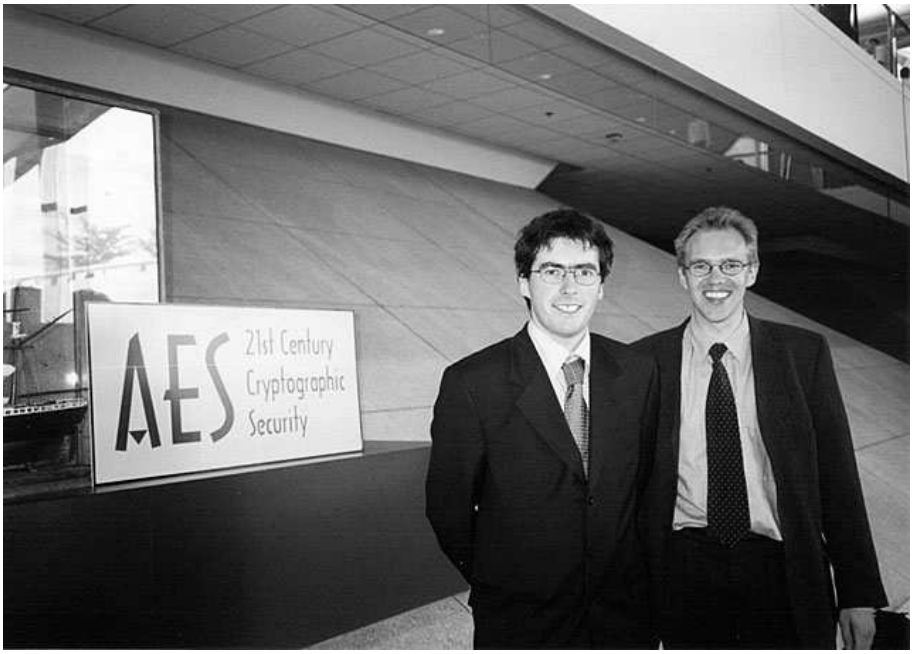
Kierrosfunktiossa on tyypillisesti permutaatioita, eli bittien tai tavujen järjestysten vaihtamista, sekä lyhyisiin bittilohkoihin kohdistuvia epälineaarisia korvausmuunnoksia. Esimerkiksi DES-algoritmin kierrosfunktiossa on kahdeksan erilaista korvausmuunnosta eli *S-boxia* (substitution box) rinnakkain. Kukin niistä ottaa kuusi bittiä sisään ja antaa neljä bittiä ulos.

Differentiaalinen kryptoanalyysi on valittua selväkieltä käyttävä analyysimenetelmä, jonka perusajatus on siinä, että jokin kiinteä erotus selväkielilohkoissa voi suurella todennäköisyydellä näkyä jonakin tiettynä salakielilohkojen erotuksena. Biham ja Shamir esittivät, miten tällaista erotusten jakautumista voidaan selvittää kunkin S-boxin osalta erikseen ja näitä tietoja sitten yhdistellä niin kutsutuiksi *differentiaaleiksi* kierrosfunktion yli ja edelleen *differentiaaliketjuiksi* koko iteroidun salausalgoritmin yli [1]. Analysoimalla suuren määrän tällaisia valittuja selväkieliparejа, joilla on kiinteä erotus, voidaan ratkaista viimeisellä kierroksella käytettyjä avainbittejä.

Biham ja Shamir arvioivat, että tarvittaisiin noin 2^{44} selväkielilohkoa ja vastaava määrä salausoperaatioita, jotta voidaan riittävällä varmuudella määrittää DES-algoritmin viimeisen kierroksen kierrosavaimesta 12 bittiä. Loput 44 bittiä DES-algoritmin 56-bittisestä avaimesta voidaan sitten hakea täydellisellä haulla. Yhteensä vaadittava työmäärä on 2^{45} salausoperaatiota. Kun verrataan tämän ratkaisumenetelmän vaatimaa työtä siihen työhön, mikä tarvittaisiin kaikkien avainten läpikäymiseksi, eli 2^{56} salaamisoperaatiota, niin saavutettu etu on huomattava.

Matsuin lineaarinen kryptoanalyysi [14] on vielä jonkin verran tehokkaampi DES-algoritmille. Ensinnäkin se vaatii vain, että selväkieli tunnetaan, tai jopa vain, että sen tietyt tilastolliset ominaisuudet tunnetaan. Lineaarinen kryptoanalyysi perustuu huomioon, että jollakin selväkielibittien osajoukolla voi olla ominaisuus, että sen pariteetti, eli onko joukossa ykkösbittejä parillinen vai pariton määrä, määrää suurella todennäköisyydellä jonkin salakielibittien osajoukon pariteetin. Tällöin sanotaan, että pariteetit korreloivat. Samoin kuin differentiaalisessa kryptoanalyysissa, tätä ominaisuutta analysoidaan kullekin S-boxille erikseen, ja sen jälkeen yhdistetään vahvimmat korrelaatiot koko algoritmin kattavaksi ketjuksi. Eräs tärkeimmistä pariteettien korrelaatioista esiintyy DES-algoritmin viidennessä S-boxissa. Tiedetään, että sen toinen syötebitti on erisuuri kuin koko tuotoslohkon pariteetti 52 tapauksessa kaikista mahdollisista 64 tapauksesta.

Jälkeenpäin DES-algoritmin suunnittelussa mukana olleilta on kysytty, kuinka hyvin he olivat perillä differentiaalisen ja lineaarisen kryptoanalyysin tapaisista ratkaisumenetelmistä. Don Coppersmithin mukaan differentiaalinen menetelmä oli tiedossa, ja se otettiin DES-algoritmin kehitystyössä huomioon [4]. Sen sijaan suoraa vastausta ei lineaarisen menetelmän tuntemisesta ole kuultu.



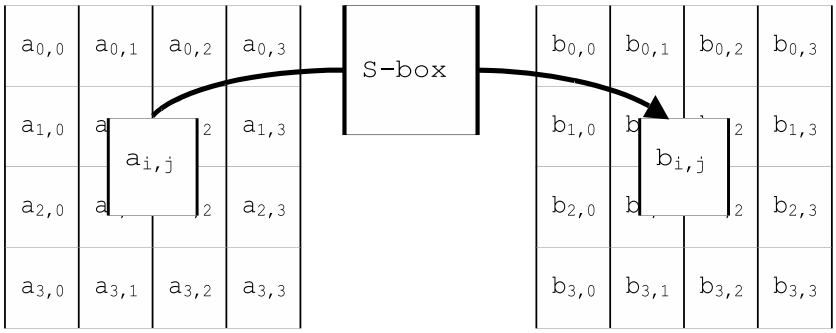
Kuva 2: Belgialaiset Vincent Rijmen ja Joan Daemen (J. Daemenin luvalla)

13 Advanced Encryption Standard

Vuonna 1998 voitiin todeta tietokoneiden laskentatehon lopullisesti ohittaneen DES-menetelmän antaman turvallisuuden, kun Electronic Frontier Foundation -niminen organisaatio julkisesti selvitti DES-algoritmilla salatun viestin 56 tunnissa tätä tarkoitusta varten kootulla tietokonejärjestelmällä, jonka hinnaksi on arvioitu noin neljännesmiljoona dollaria [11, s. 451]. DES-algoritmia oli jo pitkään suositeltu käytettäväksi kolminkertaisessa Triple-DES-muodossa, jolloin avaimen pituutta voidaan kasvattaa. Mutta ongelmana pysyy edelleenkin pieni lohkon pituus, vain 64 bittiä. Toimenpiteisiin DES-algoritmin korvaamiseksi uudella salakirjoitusstandardilla ryhdyttiin viimein vuonna 1997. Avoimessa kutsussa NIST määritteli uudelle standardille *Advanced Encryption Standard* (AES) asetettavat vaatimukset. Merkittävintä oli sekä avaimen että lohkon pituuden nostaminen 128 bittiin. Standardi tukee myös 192 bitin ja 256 bitin avaimia.

AES:in suunnittelu- ja arviointiprosessi kesti neljä vuotta. Noin kaksi vuotta kestäneen ensimmäisen vaiheen jälkeen valittiin viisi ehdokasta toiselle kierrokselle, joista loppukesällä vuonna 2000 julistettiin voittajaksi belgialaisten kryptografien Vincent Rijmenin ja Joan Daemenin suunnittelema Rijndael-algoritmi, joka löi muun muassa mukana olleiden jättiyritysten IBM:n ja NTT:n tutkimuslaboratorioissa kehitetyt kilpailevat ehdotukset.

Arviointiprosessin aikana järjestettiin julkisia seminaareja, joissa tutkijat esittivät AES-ehdokkaita koskevia tutkimus-



Kuva 3: Rijndaelin S-box operoi kuhunkin tilamatriisin alkioon.

tuloksia. Arvioinnin kohteena oli vastustuskyky erilaisia hyökkäyksiä kohtaan, mutta tarkkaan analysoitiin myös algoritmien tehokkuutta erilaisilla prosessorialustoilla. Kaikki arvioinnin yhteydessä julkaistu tieto ja tutkimustulokset löytyvät NISTin AES-sivuilta http://csrc.nist.gov/encryption/aes/, jotka säilytetään historiallisista syistä muuttumattomina. Rijndael-algoritmin vahvoja puolia oli sen joustava soveltuvuus sekä 8 bittiä että suurempaa sanakokoa käyttäville prosessoreille. Rijndaelin rakenne on myös huomattavan selkeä, ja se käyttää laajasti hyväkseen 1990-luvun lohkosalausmenetelmien tutkimusta, johon myös Rijmen ja Daemen olivat itse osallistuneet aktiivisesti.

Seuraavassa kuvataan lyhyesti joitakin Rijndael-algoritmin rakenteen pääpiirteitä. Rijndael on iteroitu lohkosalaaja kuten DES. Salattava 128 bitin datalohko jaetaan kuuteentoista oktettiin, jotka järjestetään neljän rivin ja neljän sarakkeen muodostamaan *tilamatriisiin*. Tässä sinänsä ei ole mitään uutta. Jo muinoin *scytale*-menetelmässä ja myöhemmin maailmansotien aikaisissa salakirjoitusmenetelmissä salattavia merkkejä aseteltiin matriisiin, johon sitten kohdistetaan yksinkertaisia rivi- ja sarakeoperaatioita (katso myös [12]).

Kullakin kierroksella tilamatriisin oktetteihin lisätään avaimesta johdettua dataa, eli kierrosavain, biteittäin xor-operaatiolla. Sen jälkeen kukin tilamatriisin 16 alkiosta muunnetaan korvausmuunnoksella eli S-boxilla. Rijndaelin S-box on sen ainoa epälineaarinen komponentti, ja algoritmin vastustuskyky differentiaalista ja lineaarista menetelmää vastaan perustuu oleellisesti siihen.

Tämän artikkelin kirjoittaja oli jo vuonna 1991 esittänyt, että optimaalinen vastustuskyky Bihamin ja Shamirin differentiaalista kryptoanalyysia vastaan voitaisiin saavuttaa funktioilla, joilla on sellainen ominaisuus, että kullakin kiinteällä syötelohkojen erotuksella tuotoslohkojen erotukset ovat mahdollisimman tasaisesti jakautuneet. Tämä väite sai tuekseen todistuksen yhdessä Lars Knudsenin kanssa tehdyn työn tuloksena [18]. Myöhemmin Eurocrypt ’93 -kongressissa, samassa, jossa Matsui esitti lineaarisen kryptoanalyysin, kirjoittaja esitti useita matematiikan tarjoamia differentiaalisesti tasaisia funktioita [19] (katso myös [11, s. 455]). Näiden joukossa oli myös Galois-kunnassa $GF(2^n)$ määritelty bijektiivinen funktio x^{-1}, joka tarjoaa lähes optimaalisen vastustuskyvyn myös lineaarista kryptoana-

lyysia vastaan. Tämä tulos on seurausta aiemmin koodausteorian puolella todistetusta tuloksesta [10]. Tämän funktion x^{-1}, parametrin arvolla $n = 8$, Rijmen ja Daemen päättivätkin sitten valita algoritminsa S-boxiksi.

Sitten Rijndaelin kierrosfunktiossa seuraa sarja yksinkertaisia matriisioperaatioita, joilla on tärkeä merkitys *diffuusion* eli vaikutusten hajauttamisen kannalta. Rijndaelin rivioperaatiot ovat rivin syklisiä siirtoja vasemmalle. Ensimmäinen rivi pysyy paikallaan, toista riviä siirretään askeleen verran, kolmatta kaksi askelta ja neljättä kolme askelta.

Sen jälkeen operoidaan jokaiseen neljään sarakkeeseen samalla lineaarisella muunnoksella. Tämän muunnos on valittu siten, että se levittää sarakkeen yhden alkion vaikutuksen mahdollisimman tehokkaasti koko sarakkeeseen. Tässä on käytetty hyödyksi tunnettuja virheenkorjauskoodien ominaisuuksia.

Rijndaelissa kierrosfunktiota iteroidaan 10 kertaa. Joka kierrosta varten salausavaimesta johdetaan uusi kierrosavain. Vielä lopuksi lisätään kierrosavain, joita tarvitaan siis yhteensä yksitoista.

Rijndaelin tulkintafunktio on erilainen kuin salaamisfunktio. Ensinnäkin tietysti kierrosavaimia tulee käyttää päinvastaisessa järjestyksessä. DES-algoritmin tapauksessa tämä riittää, koska sen rakenne, *Feistelin rakenne*, on oman itsensä käänteismuunnos eli *involuutio*. Tästä on huomattavaa etua, koska samalla toteutuksella voidaan suorittaa sekä salaamisfunktiota että tulkintafunktiota, kun vain kierrosavaimet johdetaan erikseen. Rijndaelilla ei ole tätä etua. Sen suunnittelussa on tosin pyritty salaamisfunktion ja tulkintafunktion samankaltaisuuteen, mutta tiettävästi käytännössä nämä funktiot useimmiten toteutetaan erikseen.

14 Lopuksi

Moderni kryptologia on hyvin pitkälle erikoistunut tietotekniikan ja matematiikan tutkimusalue, joka käyttää laajasti hyvin monenlaisia tutkimusmenetelmiä. Sen käyttämät matemaattisesti vaikeat probleemit ovat yleensä algebrallisen geometrian piiristä, jossa ongelman ratkaiseminen palautuu algebrallisten yhtälöiden ratkaisemiseen aritmeettisissa struktuureissa, kuten modulaarinen aritmetiikka kokonaislukurenkaissa ja Galois-kunnissa. Käytännön salaamisteknisten järjestelmien suunnittelemisessa käytetään systeemiteoreettista lähestymistapaa. Järjestelmän osien laadun arviointi on perustunut kokemukseen, joka on tuottanut hyviksi koettuja *paradigmoja*. Viime aikoina on turvallisuutta pystytty myös todistamaan pitkälle todellisuuden vaatimuksia vastaavien mallien puitteissa.

Tietotekniikan kehitys ja laskennan tehokkuuden kasvaminen vaikuttaa myös salaamistekniikkaan. Mooren lain mukaan laskennallisen resurssin hinta puolittuu puolessatoista vuodessa. Nykyään turvallisena pidetty kompleksisuusraja on 2^{80} operaatiota. Riittävän marginaalin saavuttamiseksi pidetään 2^{128} operaation kompleksisuutta tänä päivänä suositeltavana. Jos Mooren lain vaikutus jatkuu ennallaan, niin tämä luku on kerrottava kahdella joka 18. kuukausi. Kun suositeltava avaimen pituus symmetrisissä menetelmissä tänä päivänä on 128 bittiä, niin sadan vuoden kuluttua avaimen minimipituutta on tullut lisätyksi 67 bittiä. Silloin AES-algoritmin 192 bitin avain ei ehkä enää ole turvallinen, mutta 256 bittiä olisi vielä selvästi turvallisella puolella. Näin siis, kun kehitystä arvioidaan pelkästään Mooren lain ja avaimen pituuden perusteella.

Salaamistekniset menetelmät ovat vakiinnuttaneet asemansa tietoteknisten jär-

jestelmien turvallisuustekniikassa, ja niiden käyttö lisääntyy ja monipuolistuu. Sähköisessä kaupankäynnissä ja asioinnissa suurimpana haasteena on salaamistekniikan integroiminen turvallisuusjärjestelmään ottaen samalla huomioon käyttäjän vaatimukset. Tässä kehitystyössä tarvitaan kryptologien lisäksi asiantuntijoita ainakin seuraavilta tieteenaloilta: hallinto- ja oikeustieteet, kauppatieteet, käyttäytymistieteet sekä kommunikaatio- ja tietotekniikka.

Viitteet

[1] E. Biham ja A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems. Teoksessa: A. J. Menezes ja S. A. Vanstone (toim.), *Advances in Cryptology — Crypto '90*, Springer-Verlag1991, s. 3–21.

[2] D. Bleichenbacher, Chosen Ciphertext Attacks against Protocols Based on the RSA Encryption Standard PKCS #1. In *Advances in Cryptology — Crypto '98*, Springer-Verlag 1998, s. 1–12.

[3] M. Burmester, On the Risk of Opening Distributed Keys. Teoksessa: Y. Desmedt (toim.), *Advances in Cryptology — Crypto '94*, Springer-Verlag 1994, s. 309–315.

[4] Don Coppersmith, The Data Encryption Standard (DES) and its Strength Against Attacks. *IBM Journal on Research and Development*, 38 (1994), s. 243–250.

[5] Whitfield Diffie: The First Ten Years of Public-Key Cryptology. *Proceedings of the IEEE*, 76 (1988), s. 560–577.

[6] Whitfield Diffie: The First Ten Years of Public Key Cryptology. Teoksessa: Gustavus J. Simmons (toim.), *Contemporary Cryptology, The Science of Information Integrity*, IEEE Press, New York 1992, s. 135–176.

[7] Whitfield Diffie ja Martin E. Hellman, New Directions in Cryptology. *IEEE Transactions on Information Theory*, IT-22 (1976), s. 644–655.

[8] T. ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, IT-31 (1985), s. 469–472.

[9] Reino H. Hallamaa, *Salakirjoitustaidon perusteet*. Tekijän kustantama, Helsinki 1937.

[10] G. Lachaud ja J. Wolfmann, The Weights of the Orthogonal of the Extended Quadratic Binary Goppa Codes. *IEEE Transactions on Information Theory*, 36 (1990), s. 686–692.

[11] Susan Landau, Communications Security for the Twenty-first Century: The Advanced Encryption Standard. *Notices of the AMS*, 47 (2000), s. 450–459.

[12] Leo Marks, *Between Silk and Cyanide*. Harper Collins Publisher, 2000.

[13] James Massey, An Introduction to Contemporary Cryptology. *Proceedings of the IEEE*, 76 (1988), s. 533–549.

[14] Mitsuru Matsui, Linear Cryptanalysis Method for DES Cipher. Teoksessa: T. Helleseth (toim.), *Advances in Cryptology — Eurocrypt '93*, Springer-Verlag, 1994, s. 386–397.

[15] National Institute of Standards and Technology, *NIST: FIPS Publication 186-2: Digital Signature Standard (DSS)*, 2000.

[16] V. Niemi ja A. Renvall, How to Prevent Buying of Voters in Computer Elections. Teoksessa: *Advances in Cryptology — Asiacrypt '94*, Springer-Verlag, 1995, s. 164–170.

[17] H. Nurmi, A. Salomaa ja L. Santean, Secret Ballot Elections in Computer Networks. *Computers & Security*, 10 (1991), s. 553–560.

[18] K. Nyberg ja L. R. Knudsen, Provable Security Against Differential Cryptanalysis. Teoksessa: E. F. Brickell (toim.), *Advances in Cryptology — Crypto '92*, Springer-Verlag, 1993, s. 566–574.

[19] K. Nyberg, Differentially Uniform Mappings for Cryptography. Teoksessa: T. Helleseth (toim.), *Advances in Cryptology — Eurocrypt '93*, Springer-Verlag, 1994, s. 55–64.

[20] J. Paloposki ja J. Pekkarinen, *Jorma Vanamo, Vanhan koulun diplomaatti*. Otava 2001.

[21] S. Pohlig ja M. Hellman, An Improved Algorithm for Computing Logarithms over $GF(p)$ and its Cryptographic Significance. IEEE Transactions on Information Theory, 24 (1978), s. 106–110.

[22] R. Rivest, A. Shamir ja L. Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, 21 (1978), s. 120–126.

[23] RSA Laboratories, "PKCS #1 v2.0: RSA Cryptography Standard", October 1998.

[24] Arto Salomaa, *Public-Key Cryptography*. Springer-Verlag, Berlin 1990.

[25] Claude Shannon, A Mathematical Theory of Communication. *Bell System Technical Journal*, 27 (1948), s. 379–423 ja 623–656.

[26] Claude Shannon, Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28 (1949), s. 656–715.

[27] Pertti Suvanto, Matematiikka on lopullista kauneutta. *Apropos*, 6 (2001), s. 12–14.

[28] M. V. Wilkes, *Time-Sharing Computer Systems*. 2. painos, American Elsevier, New York, 1972.

[29] 3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, TS 350.201–350.209 (2001). http://www.3gpp.org/specs/specs.htm [5.6.2007]