SALAUSTEKNIIKKA KOKONAISTIETOTURVALLISUUDEN OSANA

Everstiluutnantti, FL Hannu Koukkula

1 Johdanto

Tietoturvallisuuden merkitys on kasvanut nopeaan tahtiin kuluvan vuosikymmenen aikana matkaviestinnän ja kansainvälisten tietoverkkojen räjähdysmäisen kehityksen myötä. Sama tahti näyttää jatkuvan edelleen nopeasti kiihtyvänä. Merkittävää on myös ollut, että aikaisemmin pääasiassa sotilas-, poliisi- ja diplomaattiviestiyhteyksien turvaamiseen käytetyt salausmenetelmät ovat levinneet lähes kaikkien yhteiskunnan sektorien ja jopa yksityisten henkilöiden laajaan käyttöön tietoturvallisuuden tehokkaina kehitystyökaluina.

Eräänä lähivuosien kehitysnäkymänä Suomessa mainittakoon monet sähköiset kansalaispalvelut avaava, jo pitkälle kehitetty "kansalaiskortti". Sen samoin kuin "verkkokaupan" ja monien muiden tietoverkkoihin perustuvien sovellusten vääjäämätön rynnistäminen yleiseen käyttöön asettaa nyt ja tulevaisuudessa kovat vaatimukset tunnistettujen, konkreettisten uhkien torjunnalle. Tietoturvallisuutta ei enää yleensä saada riittävälle tasolle millään yksittäisillä tai yksinkertaisilla keinoilla. Asiaa joudutaan ainakin suuremmissa organisaatioissa yleensä lähestymään määrittelemällä organisaation tärkeimmät toiminnot osatoimintoineen (= ydinprosessit) samoin kuin näiden osien turvallisuusvaatimukset tietoturvallisuuden kaikilla osa-alueilla. Turvallisuutta kehitettäessä joudutaan ydinprosessien määritykseen liittyen päättämään toimenpiteistä useilla osa-alueilla.

Tässä kirjoituksessa tarkastellaan tietoturvallisuuden laaja-alaisuutta ja sen kehittämisen monitahoisuutta pääosin määritelmätasolla. Kirjoituksen pääpaino on salaustekniikan keskeisimmissä asioissa. Aihepiirin laajuudesta johtuen yksityiskohtiin ulottuva tarkastelu ei ole yleensä ollut mahdollista. Useat, tärkeätkin salaustekniikan aiheet on jouduttu tällä kerralla jättämään käsittelemättä.

2 Tietoturvallisuuden osa-alueet

Tietoturvallisuudella tarkoitetaan asiantilaa, jossa

* tiedot
* järjestelmät ja
* palvelut

ovat asianmukaisesti suojattuja sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla.

Tietoturvallisuus muodostuu periaatteessa viidestä osa-alueesta:

- pääsynvalvonnasta,
- luottamuksellisuudesta,
- eheydestä,
- käytettävyydestä ja
- kiistämättömyydestä

Pääsynvalvonta ja kiistämättömyys voidaan haluttaessa tulkita myös kolmen muun osa-alueen osiksi.

Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä sekä pääsynvalvontaa ja kiistämättömyyttä turvataan:

- laitteisto- ja ohjelmistovikojen,
- luonnontapahtumien sekä
- tahallisten, tuottamuksellisten ja tapaturmaisten inhimillisten tekojen aiheuttamilta uhkilta ja vahingoilta.

Pääsynvalvonta perustuu luotettavaan todentamiseen ja sitä käytetään käyttäjien (henkilö, prosessi, sekä muut oliot) oikeuksien tarkistamiseen sekä antamaan pääsy hyödyntämään vastaavia palveluja.

Luottamuksellisuudella tarkoitetaan, että tiedot ovat vain rajoitetun henkilöpiirin saatavissa eikä niitä paljasteta tai saateta sivullisten käytettäväksi.

Eheydellä tarkoitetaan, että tietoaineistoa tai tietojärjestelmiä ei ole muutettu tai tuhottu oikeudettomalla tavalla.

Käytettävyys merkitsee, että järjestelmät tietoineen ja palveluineen ovat tarvittaessa niihin oikeutettujen henkilöiden, yhteisöjen ja muiden olioiden esteettä hyödynnettävissä.

Kiistämättömyydellä tarkoitetaan, että yksi tai useampi tietojen käsittelyn/siirron osapuoli (olio) ei voi jälkikäteen kiistää osuuttaan niihin.

Olio on tietojärjestelmien yhteydessä käytettävä yleisnimitys, joka voi tarkoittaa

* fyysistä oliota (avointa järjestelmää)
* loogista oliota (OSI-kerrosten oliot, tiedostot, organisaatiot ja yritykset) tai
* henkilökäyttäjää

OSI-mallin yhteydessä puhutaan usein vertaisoliosta (peer entity), jolla tarkoitetaan samassa OSI-kerroksessa olevaa oliota.

Tietoturvallisuuden toteutusperiaatteet ja toteutuksen osa-alueet

Tietojärjestelmän tietoturvallisuus on kokonaisuus, joka koostuu teleoperaattoreiden toimenpitein aikaansaadusta televerkon perusturvallisuudesta ja käyttäjien omien tarpeidensa perusteella toteuttamasta lisäturvallisuudesta. Sekä teleoperaattoreiden että käyttäjien toimenpiteet (suunnittelu, toteutus ja valvonta) tietoturvallisuuden viiden osa-alueen toteuttamiseksi voidaan jakaa kahdeksaan osa-alueeseen seuraavasti:

1) hallinnollinen tietoturvallisuus
2) henkilöstöturvallisuus
3) fyysinen turvallisuus
4) tietoliikenneturvallisuus

5) laitteistoturvallisuus
6) ohjelmistoturvallisuus
7) tietoaineistoturvallisuus ja
8) käyttöturvallisuus

Tietojärjestelmän turvallisuusvaatimuksilla tarkoitetaan televerkkojen siirtoteille, keskuksille ja päätelaitteille sekä tietojärjestelmän elemeneille asetettavien vaatimusten samoin kuin muun tietoturvallisuuden toteutusta koskevien määräysten muodostamaa kokonaisuutta. Vaatimusten ja määräysten on katettava kaikki tietoturvallisuuden viisi osa-aluetta.

Televerkkojen osalta turvallisuusluokitus voidaan määrittää joko vain siirtoverkkoa tai koko televerkkoa kattavaksi. Molemmissa tapauksissa on määriteltävä tarkasti erikseen, mitä verkon osia, toimintoja ja käyttötapoja luokittelu koskee.

Televerkkojen palveluja hyödyntävien käyttäjien, prosessien yms (<=> olioiden), tietojärjestelmät mukaan luettuina, on määritettävä palvelun kohteena olevien asioiden turvallisuusvaatimukset ja suunnattava käyttönsä näiden vaatimusten edellyttämiin verkkoihin ja niiden osiin sekä toteutettava muut tarvittavat turvallisuustoimenpiteet.

4 Riskien arviointi ja analyysi

4.1 Perusteet

Tietoliikenneverkkoihin kohdistuu erilaisia tietoturvallisuusuhkia. Uhkien olemassaoloa ja niiden toteutumisen mahdollisia seurausvaikutuksia on pystyttävä arvioimaan ja analysoimaan jollakin tavalla, jotta niitä vastaan voidaan suojautua. Uhkien ja riskien tunnistamiseksi ja niiltä suojautumiseksi on tarpeen suorittaa riskien arviointi ja riskianalyysi.

Tässä yhteydessä riskien arvioinnilla (Risk Assessment) tarkoitetaan kaikkia niitä järjestelmällisiä toimenpiteitä, joiden avulla voidaan arvioida löydettyjen tai havaittujen tietoturvallisuusuhkien seurausvaikutuksia siinä tapauksessa, että nämä uhat toteutuvat. Riskien arviointiin sisältyy myös tulosten raportointi. Riskien arviointiin voi sisältyä riskianalyysin suorittaminen jollakin rajatulla alueella.

Riskianalyysi (Risk Analysis) on suppeampi ja teknisempi käsite kuin riskien arviointi. Riskianalyysi tarkoittaa yksityiskohtaista tutkintaprosessia, jonka tavoitteena on selvittää tutkinnan kohteeseen kohdistuvat uhat. Riskianalyysi sisältää useita yksityiskohtaisia työvaiheita, jotka voivat olla manuaalisia, osaksi automatisoituja tai täysin automatisoituja.

Riskien arviointi ja riskianalyysi voidaan suorittaa erilaisilla tekniikoilla. Suorittamistavan valinnassa on syytä olla tarkkana, sillä väärin sovellettuna nämä tekniikat voivat johtaa virheellisiin lopputuloksiin. Kvantitatiivista (määrällistä) riskien arviointia (Quantitative Risk Assessment) ja kvantitatiivista riskianalyy-

siä ei suositella käytettäväksi kuin poikkeustapauksissa ja silloinkin tietoturvallisuusalan ammattilaisen avustuksella suoritettuna. Ne antavat järkeviä lopputuloksia vain siinä tapauksessa, että laskennassa tarvittavien uhkien todennäköisyydet voidaan määritellä luotettavasti.

Riskien arviointi ja riskianalyysi voidaan suorittaa muun muassa tarkistuslista- ja peruslinjamenetelmillä. Tarkistuslistat ovat sopiva ja yksinkertainen tapa aloittaa riskien selvittäminen ja kokemuksen karttuessa voidaan siirtyä käyttämään peruslinjamenetelmää.

4.2 Tarkistuslistat

Yksinkertaisin tapa suorittaa riskien arviointi ja riskianalyysi perustuu ns. tarkistuslistojen hyväksikäyttöön. Tarkistuslistat (Checklists) ovat yksinkertaisesti kysymyssarjoja, joissa kysellään erilaisia tarkasteltavan kohteen tietoturvallisuuteen liittyviä asioita. Näihin kysymyksiin vastaamalla pyritään selvittämään mahdolliset tietoturvallisuusuhat, niiden seurausvaikutukset ja olemassa olevat suojausmenetelmät. Tarkistuslistojen käyttö vaatii vain vähän tietämystä itse tietoturvallisuusasioista ja arviointi voidaan suorittaa lyhyessä ajassa. Lopputuloksena saadaan karkean tason kuvaus arvioinnin kohteen tietoturvallisuusasioiden tilasta.

4.3 Peruslinjamenetelmä

Edellistä hieman monimutkaisempi mutta selvästi tehokkaampi tapa arvioida ja analysoida riskejä on ns. peruslinjamenetelmä (Baseline Method). Se perustuu tämän kirjoituksen johdannossa mainittujen ydinprosessien määrittämiseen ja "asianmukaisen huolellisuuden" noudattamiseen kaikilla tietoturvallisuuden osa-alueilla. Tarvittavat suojaukset valitaan niiden suojauskeinojen joukosta, jotka ovat yleisesti hyväksyttyjä ja joita käytetään laajasti vastaavanlaisissa hyvin hoidetuissa organisaatioissa. Näin saadaan aikaan tarvittava perusturvallisuus uhkien ja riskien torjumiseksi. Tämä yleisesti hyväksytty ja laajasti käytetty riskien arviointimenetelmä muodostuu seuraavista vaiheista:

1) tunnistetaan suojausta vaativat kohteet ja niiden luonne
2) määritellään tarvittavat perussuojaukset ja niiden tavoitteet
3) tunnistetaan nykyiset (olemassaolevat) perussuojaukset ja selvitetään, puuttuuko joitakin tarvittavia kohdassa 2 määriteltyjä perussuojauksia
4) valitaan tarvittavat perussuojaukset yleisimpien uhkien torjumiseksi sekä tehdään suunnitelma suojausten toteuttamiseksi
5) priorisoidaan suojausten toteutus ja tehdään suositus organisaation johdolle määriteltyjen perussuojausten toteuttamiseksi.

5 Salausmenetelmät ja -algoritmit

5.1 Yleistä

Salausmenetelmällä (cipher = ciphersystem) tarkoitetaan niiden menettelytapojen yhdistelmää, joilla selväkieli muutetaan *salakieleksi* tai päinvastoin. Salausmenetelmään kuuluu yleensä salaus- ja tulkinta-algoritmi sekä avainten hallinta. Salausmenetelmiä käytetään "työkaluina" useissa erityisesti korkeimpien turvatasojen tietoturvamekanismeissa.

Salausalgoritmilla tarkoitetaan niiden matemaattisten ja loogisten sääntöjen muodostamaa kokonaisuutta, joiden mukaan algoritmin sisäänmenoinformaatio muunnetaan ulostuloinformaatioksi ainakin osittain salassapidettävien parametrien kontrolloimana. Salausalgoritmityypistä ja algoritmin käyttötarkoituksesta riippuen joko sekä yksittäisen salaus- ja tulkintamuunnoksen määrittelyssä (= *symmetrinen* tai salaista avainta käyttävä *epäsymmetrinen algoritmi*) tai toisessa niistä (= *julkisen avaimen epäsymmetrinen algoritmi*) käytettävä parametrijoukko = *avain* on huolellisesti salassa pidettävä. Salausalgoritmia käytetään salausmenetelmän oleellisena osana tai se voi olla myös itse salausmenetelmä.

Eniten tunnettuja, julkaistuja salausalgoritmeja ovat symmetrinen DES-algoritmi ja epäsymmetrinen julkisen avaimen RSA-algoritmi. Julkaistujen algoritmien lisäksi on kehitetty ja kehitetään jatkuvasti uusia, valmistaja- tai käyttötarkoituskohtaisia algoritmeja (= proprietary algorithms), joiden suunnittelukriteerit ja rakenteelliset yksityiskohdat pidetään vain valmistajien ja lisäksi mahdollisesti käyttäjien tiedossa.

Salausmenetelmillä ja niihin perustuvilla tietoturvamekanismeilla saavutettava turvallisuustaso riippuu ratkaisevasti käytetyistä salausalgoritmeista sekä erityisesti tarvittavien salaisten avainten (= algoritmin salaisten parametrien) hallinnasta. Ne on tutkittava, hyväksyttävä ja järjestettävä sovelluskohtaisesti erikseen.

5.2 Tärkeimmät julkaistut algoritmit ja niiden pääominaisuudet

5.2.1 DES (= Data Encryption Standard) -algoritmi

DES-algoritmi on symmetrinen lohkosalausalgoritmi. National Bureau of Standards (NBS) julkaisi sen 15.1.1977 käytettäväksi Yhdysvaltain keskushallinnon luokittelemattomissa sovelluksissa (NBS77). Standardi määrättiin astumaan voimaan 15.7.1977.

Standardin kehitystyön taustana oli 1970-luvun alussa tiedostettu tarve saada käyttöön menetelmä, jolla pystyttäisiin turvaamaan tietoliikenteessä siirrettävien tietojen luottamuksellisuus. Tästä syystä NBS käynnisti projektin, jonka tarkoituksena oli kehittää salausstandardi keskushallinnon tarpeita varten kuitenkin niin, että sitä voitaisiin käyttää myös yksityisellä sektorilla. Vuonna 1973 NBS julkai-

si tiedotteen, jossa pyydettiin ehdotuksia standardiksi sopivista salausmenetelmistä. Standardin tarpeellisuutta perusteltiin sillä, että erilaisten salausmenetelmien käyttö johtaa avoimissa tiedonsiirtoverkoissa yhteensopimattomuuteen ja että helposti käytetään heikon turvan antavia salausmenetelmiä.

Saamistaan esityksistä soveliaimmaksi NBS totesi International Business Machines Corporation'in (IBM) ehdotuksen. Ehdotus perustui IBM:n aikaisemmin suorittamaan tutkimus- ja kehitystyöhön (Lucifer-algoritmi), jonka kohteena oli ollut tietojenkäsittelysovelluksiin sopiva salausmenetelmä.

NBS oli standardiehdotuksia pyytäessään asettanut seuraavat vaatimukset:

- Menetelmän on annettava korkeatasoinen turva tiedoille.
- Menetelmän on oltava helposti ymmärrettävä, mutta silti niin monimutkainen, että ratkaisemisen kustannukset ovat huomattavasti suuremmat kuin sitä kautta saatava hyöty.
- Menetelmän turvallisuuden on perustuttava ainoastaan salassa pidettävään avaimeen itse menetelmän ollessa julkinen.
- Menetelmän on oltava tehokas ja taloudellinen.
- Menetelmää on voitava soveltaa erilaisiin käyttötilanteisiin.
- Menetelmän on oltava kaikkien käyttäjien ja toimittajien käytettävissä samalla tavalla ja kohtuullisin kustannuksin.

DES-algoritmi on ollut maailmanlaajuisesti eniten käytetty symmetrinen salausalgoritmi yli 20 vuoden ajan. Se on iteroitu (16 kierrosta) lohkosalaaja, joka käsittelee 64 bittisiä datalohkoja. Avain on 64 bittinen. Siitä käytetään salaukseen 56 bittiä, loput 8 ovat tarkistebittejä. Kullakin kierroksella suoritetaan epälineaarinen korvausmuunnos, jonka osittain salaisina pidettyjä suunnitteluperiaatteita on tutkittu paljon. Käytetyistä bittipermutaatioista johtuen ohjelmalliset toteutukset ovat varsin hitaita joskin tietotekniikan kehitys on erityisesti viime vuosien aikana muuttanut tätä tilannetta nopeasti. DES-algoritmia on toteutettu myös nopeina piireinä, joiden saatavuutta ovat hankaloittaneet amerikkalaiset vientirajoitukset. Nämä rajoitukset ja niiden mahdolliset muutokset ovat olleet laajan kansainvälisen tarkastelun kohteena parin viime vuoden aikana. DES:n tarkempi rakenne ja toiminnan yksityiskohdat on esitetty muun muassa lähteessä [1].

5.2.2 RSA (Rivest-Shamir-Adleman) -algoritmi

RSA on epäsymmetrinen julkisen avaimen lohkosalausalgoritmi, joka on saanut nimensä kehittäjiensä mukaan. Sen kehityksen ehkä voimakkaimpana vaikuttimena oli 1970-luvun alkupuolella, DES-algoritmin kehityksen myötä tapahtunut salausmenetelmien käyttöönoton ja tutkimuksen räjähdysmäinen kasvu. Tutkimus- ja kehitystyö toivat konkreettisesti tietoisuuteen salaisiin avaimiin perustuvien salausmenetelmien avainten jakeluvaikeudet. Käytännössä todettiin, että runsaasti käyttäjiä käsittävissä salausverkoissa erityisesti käyttäjien vaihtuessa usein salaisten avainten jakelu ja niiden riittävän usein tapahtuva vaihtaminen voivat olla jopa mahdottomia tehtäviä. Näistä syistä samoin kuin alan voimakkaasti lisääntyneen teoreettisen tutkimuksen tuottamien tulosten perusteella

alettiin kehittää vaikeisiin matemaattisiin ongelmiin perustuvia kaksiavaimisia salausmenetelmiä. Kaksiavaimisten menetelmien kehittämisen päätavoitteena oli vapautua salaisten avainten käsittelystä ja siirtää salaisten avaintietojen käsittely kokonaisuudessaan jokaisen käyttäjän tehtäväksi.

Ensimmäisen tällaisen menetelmän esittivät Diffie ja Hellman (Diff76). Tämän mallin pohjalta Pohlig ja Hellman (Poh178a) julkaisivat salausmenetelmän, joka perustuu potenssiin korottamiseen äärellisissä modulokunnissa. Samoihin aikoihin Rivest, Shamir ja Adleman (Rive78a) julkaisivat samantapaisen, kuitenkin eräiltä yksityiskohdiltaan hieman edellisestä eroavan menetelmän, joka antoi MIT:lle (= Massachusetts Institute of Technology) sysäyksen toteuttaa julkisen avaimen salausmenetelmä. Martin Gardner (Gard77) kuvasi Scientific American'ssa RSA-menetelmää "uudentyyppiseksi salausmenetelmäksi, jonka ratkaiseminen kestää miljoonia vuosia". Outona sattumana voitaneen pitää sitä, että sama lehti julkaisi täsmälleen 60 vuotta aikaisemmin, vuonna 1917, artikkelin, jossa Vigenéren menetelmää kuvattiin "mahdottomaksi ratkaista" (Kahn67).

RSA-menetelmä perustuu modulo-n kunnassa suoritettavan potenssiinkorottamisen käänteismuunnoksen matemaattisen ratkaisun vaikeuteen, kun ratkaisijalla ei ole käytettävissään "salaovi-informaatiota" = salaista avainta. Modulokunnan kantaluku n on kahden suuren alkuluvun, p ja q tulo:

$$n = pq. \qquad (1)$$

Sanomalohko $M \in [0,n-1]$ salataan potenssiinkorotusta käyttäen seuraavasti:

$$C = M^e \bmod n, \qquad (2)$$

missä e ja n ovat yksiselitteisen salausmuunnoksen vaatimat avaimet. Tulkinnassa käytetään samaa operaatiota, mutta eri eksponenttia d, jolloin salakielestä saadaan alkuperäinen selväkieli:

$$M = C^d \bmod n \qquad (3)$$

Menetelmän kolmesta avaimesta, e, d ja n voidaan julkistaa n ja toinen kahdesta muusta (yleensä e) ilman menetelmän ratkaistuksi tulemisen vaaraa. Käytännön tietojärjestelmissä julkiset avaimet on varmennettava (= sertifioitava). Tämä varmentaminen on tärkeä osa järjestelmän "laillisen käytön" järjestämistä ja varmistamista. Julkisten avainten varmentaminen voi olla eräs tässä esityksessä myöhemmin käsiteltävän luotetun kolmannen osapuolen (= TTP) tärkeimmistä tehtävistä.

e:n ja d:n määrittämiseksi jokaiselle käyttäjälle generoidaan käyttäjäkohtaiset suuret alkuluvut p ja q, jotka pidetään salassa. Generointiin liittyy laatuvaatimuksia, joiden toteuttaminen ja noudattaminen vaikuttavat ratkaisevasti RSA:lla saavutettavaan turvallisuustasoon. Tämän jälkeen lasketaan käyttäjäkohtaiset moduulit, n = pq. Tällöin

$$\phi(n) = (p - 1)(q - 1), \tag{4}$$

missä ø(n) on Eulerin totienttifunktio.

Avaimet e ja d valitaan niin,että

$$ed \bmod \phi(n) = 1 \tag{5}$$

Tämä voidaan tehdä niin, että d:ksi valitaan joku f(n):oon nähden suhteellinen alkuluku (= luku, jolla on ø(n):n kanssa yhteisenä tekijänä vain ø(n) tai 1) ja lasketaan sen jälkeen d:n käänteisluku mod ø(n) käyttäen Eukleideen algoritmia. Laskettu käänteisluku on avain e:

$$e = inv(d, \phi(n)) \tag{6}$$

RSA on patentoitu 20.9.1983. Patentti on voimassa 20.9.2000 asti. Siihen liittyviä yksityiskohtia on esitetty liitteessä [2].

5.2.3 BLOWFISH

BLOWFISH on symmetrinen lohkosalausalgoritmi. Sen tärkeimmät suunnittelukriteerit ovat:

1. Nopea, salaa dataa 32-bittisellä mikroprosessorilla 26 kellotuksella/tavu.
2. Yksinkertainen, Blowfish käyttää vain yksinkertaisia operaatioita: yhteenlaskua, XOR:a, taulukkohakuja 32-bittisillä operandeilla. Sen rakenne on helppo analysoida, mikä antaa hyvät mahdollisuudet eliminoida sovellusvirheet.
3. Valittavissa oleva turvallisuustaso, Blowfish'n avainpituutta voidaan vaihdella ja se voi olla jopa 448 bittiä.

BLOWFISHin tärkeimpiä ominaisuuksia on esitetty seuraavassa:

* Tarkoitettu toteutettavaksi suurilla mikroprosessoreilla.
* Suunnittelija Bruce Schneier USA:sta
* Patentoimaton.
* C-koodi saatavissa muun muassa lähteestä [1]
* Blowfish on optimoitu sovelluksiin, joissa avain ei vaihdu usein.
* Blowfish on merkittävästi DES:a nopeampi, kun sitä käytetään 32-bittisellä mikroprosessorilla, johon liitty suuri cache-muisti, kuten Pentium tai Power-PC.
* Blowfish ei ole sopiva sovelluksiin, joissa avainta vaihdetaan usein, kuten pakettiliikenne tai yksisuuntaiset tiivistefunktiot.
* Suuren cache-muistin vaatimus tekee siitä huonosti soveltuvan toimikorttisovelluksiin.
* Blowfish'n avainten luontiproseduuri on huomattavan monimutkainen. Tämä saattaa merkitä luontiproseduuriin liittyvien ratkaisutapojen löytymistä jatkotutkimuksen myötä.

* Blowfish'sta on jo löydetty "heikkoja avaimia", joiden käyttö heikentää merkittävästi algoritmin antamaa turvallisuutta. Koska Blowfish on melko uusi algoritmi, on hyvin mahdollista, että jatkotutkimus paljastaa lisää heikkoja avaimia tai muita heikkouksia.
* Blowfish'a ei tule käyttää versiona, jossa on määriteltyä vähemmän kierroksia.

Blowfish'in tarkempi rakenne ja toiminnan yksityiskohdat on esitetty muun muassa lähteessä [1].

5.2.4 IDEA

IDEA on symmetrinen lohkosalausalgoritmi. Sen kehitysvaiheet ja tärkeimmät ominaisuudet on esitetty seuraavassa:

* Ensimmäinen versio (PES = Proposed Encryption Standard) julkaistiin vuonna 1990, suunnittelijoina olivat Xuejia Lai ja James Massey.
* Vuonna 1991, Bihamin ja Shamirin esittelemän differentiaalisen kryptoanalyysin jälkeen tekijät paransivat PES'a, tuloksena IPES (= Improved Proposed Encryption Standard).
* IPES muutti nimensä IDEA'ksi (= International Data Encryption Algorithm) vuonna 1992.
* IDEA on patentoitu sekä Euroopassa että USA:ssa. Patentin haltija on Ascom-Tech AG. Lisenssimaksua ei vaadita "ei-kaupalliselta käytöltä".
* Käsittelee 64 bittisiä selväkielilohkoja, jotka jaetaan neljään 16-bittiseen alilohkoon: X_1, X_2, X_3 ja X_4.
* Algoritmi on iteroitu ja käsittää yhteensä kahdeksan kierrosta.
* Käytettävät algebralliset operaatiot ovat XOR, yhteenlasku mod 2^{16} sekä kertolasku mod $(2^{16}+1)$ (tätä operaatiota voidaan pitää IDEA:n S-box'na)
* Avain = 128 bittiä.
* IDEA on monien mielestä paras julkisesti saatavissa oleva lohkosalausalgoritmi tällä hetkellä.
* Patentoitu Euroopassa ja USA'ssa. Patentin haltija on Ascom-Tech AG. Vaatii lisenssin kaupallisiin sovelluksiin.
* On osa PGP'a.

IDEA'n tarkempi rakenne ja toiminnan yksityiskohdat on esitetty muun muassa lähteessä [1].

5.2.5 SAFER

SAFER on symmetrinen lohkosalausalgoritmi. Sen tärkeimmät ominaisuudet on esitetty seuraavassa:

* Secure And Fast Encryption Routine = SAFER
* Suunnittelija on Jim Massey Sveitsistä.
* Ei patentteja, kopiosuojauksia tai muita käyttörajoituksia.
* Käsittelee 64 bittisiä selväkielilohkoja.

* Avain = 64 bittiä, josta muodostetaan kaksi osa-avainta jokaista kierrosta varten, osa-avaimet /kierros = K_{2r-1} ja K_{2r}, kumpikin pituudeltaan 64 bittiä.
* Singaporen Ministry of Home Affairs on kehittänyt 128-bittistä avainta käyttävän version, jonka osa-avaimet, K_a ja K_b ovat kumpikin puolet = 64 bittiä käyttäjäavaimesta. Singaporen hallitus aikoo käyttää tätä Safer K-128'a laajaan valikoimaan sovelluksia.
* 64-bittinen selväkielilohko jaetaan kahdeksaan tavun pituiseen osalohkoon, jotka joka XOR'aan tai lisätään osa-avaimen K_{2r-1} tavuihin, sen jälkeen saaduille 8 osalohkolle tehdään toinen kahdesta epälineaarisesta muunnoksesta:

$y = 45^x \bmod 257$ tai
$y = \log_{45} x$

* Massey on osoittanut, että SAFER K-64 on immuuni differentiaaliselle kryptoanalyysille 8 kierroksen jälkeen ja riittävän turvallinen tätä hyökkäystä vastaan 6 kierroksen jälkeen.
* Jo kolmen kierroksen jälkeen lineaarinen kryptoanalyysi on tehoton tätä algoritmia vastaan.
* Knudsen on havainnut eräitä heikkouksia algoritmin avainten luonnissa. Nämä heikkoudet eivät todennäköisesti vaikuta SAFER'n turvallisuuteen salausalgoritmina mutta heikentävät turvallisuutta selvästi, jos algoritmia käytetään yksisuuntaisena tiivistefunktiona.
* Knudsen suosittelee joka tapauksessa vähintään 8 kierroksen käyttöä.
* Knudsen'in havaitsemat heikkoudet avainten luonnissa voitaneen välttää käyttämällä SAFER K-128 versiota. Muutoin SAFER K-128 versiota ei voida pitää merkittävästi SAFER K-64'a parempana.

SAFER'in tarkempi rakenne ja toiminnan yksityiskohdat on esitetty muun muassa lähteessä [1].

5.2.6 A5

A5 on GSM-matkapuhelimissa liikkuvan aseman ja tukiaseman välisen puheluliikenteen salauksessa käytettävä jonosalausalgoritmi. Se on digitaalisten matkapuhelimien "ei-amerikkalainen" standardi. On huomattava, että A5-salausta käytetään vain liikkuvan aseman ja tukiaseman välillä, muu osa GSM-puheluyhteydestä on salaamaton.

A5 koostuu kolmesta LFSR'sta, joiden pituudet ovat 19, 22 ja 23. Kaikki takaisinkytkentäpolynomit ovat primitiivisiä. Algoritmin ulostulona on siirtorekisterien ulostulojen modulo-2 summa (=XOR). A5 käyttää vaihtelevaa kellotusta. Kutakin rekisteriä kellotetaan sen keskimmäisen bitin perusteella. XOR muodostetaan kaikkien kolmen rekisterin keskimmäisten bittien muodostaman kynnysfunktion käänteisfunktion perusteella. Yleensä kullakin kierroksella kellotetaan vain kahta rekisteriä.

5.3 Toimintamuodot

5.3.1 Salausalgoritmien perusominaisuudet

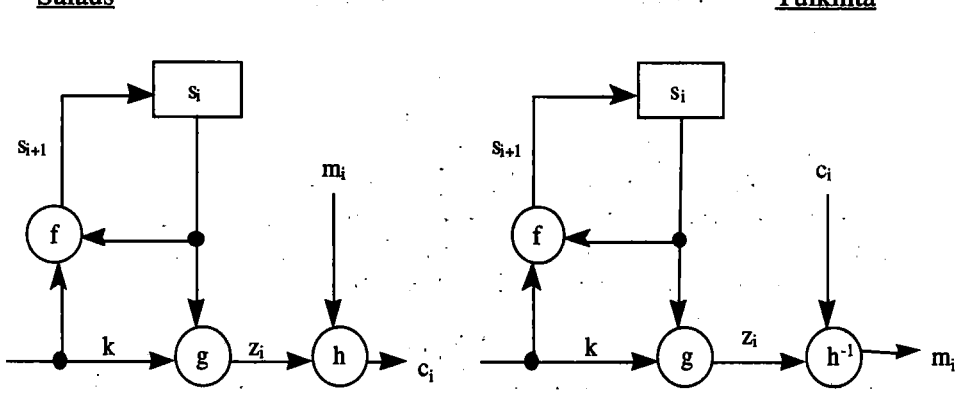
Salausalgoritmit ovat itse asiassa algoritmiperheitä, joista jokainen avain valitsee tietyn yksittäisen algoritmin. Avaimet voivat olla salaisia tai julkisia. Tietoturvamekanismien perusvaatimus on, että määrätyn lopputuloksen saavuttaminen on mahdollista vain yhtä, tarkkaan määrättyä avainta käyttäen.

Tiedon *luottamuksellisuuden* turvaamiseen käytettävällä salausalgoritmilla tieto muunnetaan sellaiseen muotoon, että vain tietyn salaisen avaimen haltija pystyy tulkitsemaan sen käyttäen mainittua avaimella määriteltyä tulkinta-algoritmia.

Todentamismekanismeissa tiedon muuntaminen tiettyyn muotoon on mahdollista vain tietyn avaimen haltijalle. Tämä toteutetaan antamalla tietty avain vain määrätyn käyttäjän tietoon. Tällöin tällä avaimella suoritettavat toiminnot voidaan rajoittaa vain kyseiselle käyttäjälle.

5.3.2 Symmetriset salausmenetelmät

Symmetriset salausmenetelmät ovat joko jono- tai lohkosalaajia. Jonosalaajat voidaan jakaa edelleen kahteen pääryhmään, synkroonisiin ja itsesynkronoituviin jonosalaajiin. Synkroonisen jonosalaajan toimintaperiaate on esitetty kuvassa 1 ja sen toimintaa kuvaavilla yhtälöillä. Itsesynkronoituvan jonosalaajan toimintaperiaate on esitetty kuvassa 2 ja sen sen toimintaa kuvaavilla yhtälöillä. Synkroonisen jonosalaajan nykyisin tärkein sovellus on binääristä yhteenlaskua käyttävä jonosalaaja. Sen toimintaperiaate on esitetty kuvassa 3.



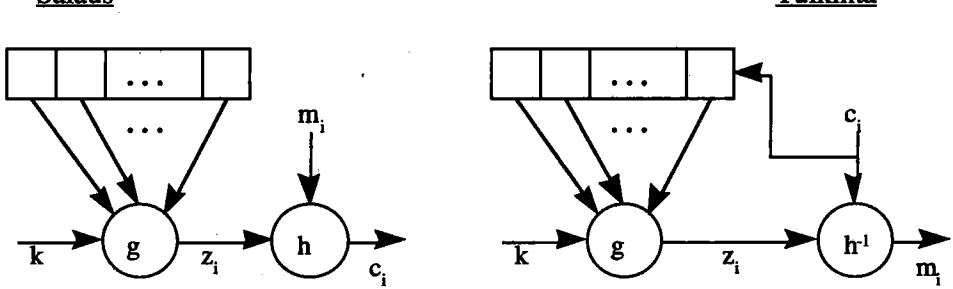
Kuva 1: Synkroonisen jonosalaajan yleinen malli

Selite: m_i = selväkieli z_i = avainjono
c_i = salakieli s_i = tila

k = avain

Synkroonisen jonosalaajan salausprosessi voidaan kuvata seuraavilla yhtälöillä:

$s_{i+1} = f(si, k)$,
$z_i = g(si, k)$,
$c_i = h(zi, mi)$, missä s_0 on alkutila, joka määritellään avaimella k,
f on seuraavan tilan määrittävä funktio,
g on funktio, joka tuottaa avainjonon z_i ja
h on ulostulofunktio, joka yhdistää avainjonon ja selväkielen mi tuottaen salakielen c_i.

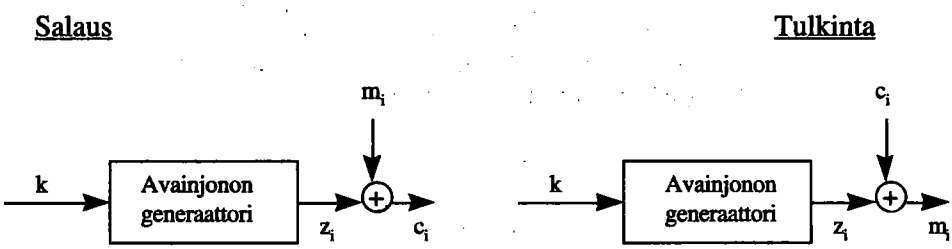


Kuva 2: Itsesynkronoituvan jonosalaajan yleinen malli

Itsesynkronoituvan jonosalaajan salausprosessi voidaan kuvata seuraavilla yhtälöillä:

$s_i = (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1})$,
$z_i = g(s_i, k)$,
$c_i = h(z_i, mi)$, missä

$s_0 = (c_{-t}, c_{-t+1}, \ldots, c_{-1})$ on ei-salainen alkutila
k on avain,
g on funktio, joka tuottaa avainjonon z_i ja
h on ulostulofunktio, joka yhdistää avainjonon selväkieleen m_i tuottaen salakielen c_i.



Kuva 3: Binääristä yhteenlaskua käyttävän jonosalaajan yleinen malli

Jonosalaaja salaa tietoa lyhyt lohko (yksi bitti tai tavu) kerrallaan kukin lohko eri muunnoksella. *Lohkosalaaja* salaa dataa pitkä lohko (tyypillisesti 64-128 bittiä) kerrallaan samalla monimutkaisella, avaimesta riippuvalla muunnoksella.

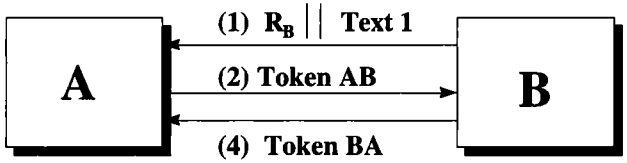
* Suurin osa laitevalmistajien omista (proprietry), yleensä salaisina pidettävistä salausmenetelmistä on jonosalaajia.
* Suurin osa julkistetuista menetelmistä on puolestaan lohkosalaajia (esimerkiksi DES).
* Synkroonisilla jonosalaajilla on hyvä siirtotiellä syntyneiden virheiden sietokyky. Tästä syystä ne eivät toisaalta sovellu käytettäväksi todentamismekanismeissa.
* Synkronoituvassa jonosalauksessa ja lohkosalauksessa virheet leviävät laajemmalle alueelle (riippuen algoritmin käyttötavasta). Tästä ominaisuudesta johtuen ne soveltuvat paremmin myös todentamismekanismeihin.
* Lohkosalaajia voidaan käyttää myös eheyden tarkisteiden (MAC) muodostamiseen [ISO-standardi ISO/IEC 9797 (1993)] sekä tiivistysfunktiona (ISO-standardi ISO/IEC 10118-2). Jonosalaajille ei ole standardoitu vastaavanlaisia käyttötapoja. Lohkosalaajia voidaan myös usein käyttää sellaisenaan vertaisolion todentamiseen [ISO-standardi ISO/IEC 9798-2 (1994)].
* Symmetrisiä lohkosalaajia voidaan käyttää luotetun kolmannen osapuolen (Trusted Third Party = TTP tai Key Escrow) välityksellä myös kiistämättömyyspalveluihin (ISO-luonnos ISO/IEC CD 13888-2) sekä istuntoavainten muodostamiseen (ISO-standardiluonnos ISO/IEC DIS 11770-2).
* Jonosalaajilla voidaan saavuttaa suuria nopeuksia (= luokkaa > 100 Mtavua/s), lohkosalaajilla saavutettavat nopeudet ovat yleensä oleellisesti alhaisempia.
* Jonosalaajilla voidaan käsitellä kaikenlaista tietoa, lohkosalaajat edellyttävät tiettyä lohkomuotoa.

5.3.3 Symmetriset todentamismekanismit

Tällaisessa mekanismissa lähettäjä muodostaa symmetristä salausmenetelmää (symmetrinen algoritmi ja salainen avain) käyttäen todentamistarkisteen ja liittää sen itse tietoon. Vastaanottajalla on käytettävissään sama symmetrinen menetelmä, jota käyttäen hän muodostaa tarkisteen ja vertaa saamaansa tulosta lähettäjän muodostamaan.

* Symmetristä todentamismekanismia voidaan käyttää vertaisolion todentamiseen [ISO-standardi ISO/IEC 9798-4 (1995)].

Eräs standardin kuvaamista mekanismeista on esitetty kuvassa 4.



Token AB = Text 3 || $eK_{AB}(R_A$ || R_B || B || Text 2

Token BA = Text 5 || $eK_{AB}(R_B$ || R_A || Text 4

Kuva 4:Kolmivaiheinen todentamismekanismi; symmetrinen salaus

Selite: R_A = A:n generoima satunnaisluku
R_B = B:n generoima satunnaisluku
eK_{AB} = A:lla ja B:llä oleva symmetrisen salausmenetelmän salainen avain
|| = Konkatenaatio (= tietolohkot peräkkäin)

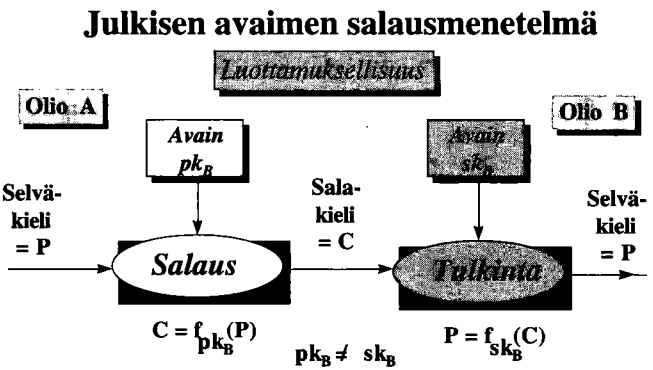
* Koska symmetrisissä todentamismekanismeissa vähintään kahdella osapuolella on sama salainen avain, niitä voidaan käyttää kiistämättömyyden turvaamiseen vain luotetun kolmannen osapuolen välityksellä (ISO-luonnos ISO/IEC 13888-2).

5.3.4 Julkisen avaimen salausmenetelmät

Kuka tahansa, jolla on tiedossaan tietyn käyttäjän julkinen avain, voi salata tätä avainta käyttäen tiedon sellaiseen muotoon, että ainoastaan kyseinen käyttäjä, jolla on vastaava salainen avain, pystyy tulkitsemaan sen.

Julkisen avaimen salausmenetelmän toimintaperiaate käytettäessä menetelmää luottamuksellisuuden turvaamiseen olioiden A ja B välillä on esitetty kuvassa 5. Julkisen avaimen menetelmää käytetään tähän tarkoitukseen suhteellisen hitauden vuoksi yleensä vain sovelluksissa, joissa salattavat tietomäärät ovat pieniä tai sovelluksen nopeusvaatimukset ovat pieniä.

(Vertaa toimintaperiaatetta aikaisemmin esitettyyn RSA:n toimintaperiaatteeseen).

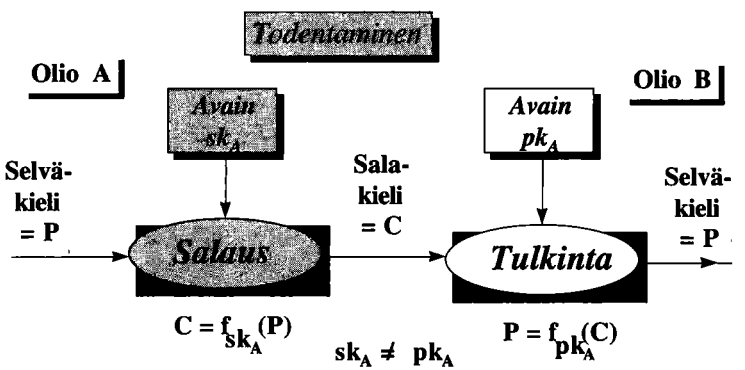


Kuva 5: Julkisen avaimen menetelmä; luottamuksellisuuden turvaaminen

Selite: pk_B = olion B julkinen avain
sk_B = olion B salainen avain

Julkisen avaimen salausmenetelmiä käytetään paitsi tiedon luottamuksellisuuden turvaamiseen, myös käyttäjän todentamiseen sekä automaattiseen avainten vaihtoon. Nämä on ainakin toistaiseksi julkisen avaimen menetelmien tavallisimmat käyttökohteet.

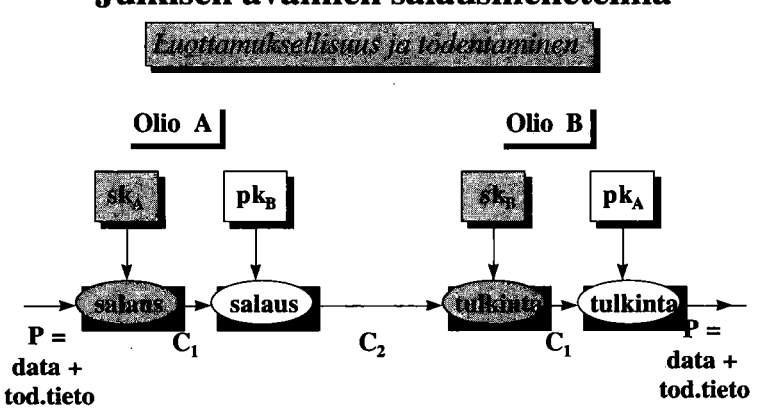
Julkisen avaimen salausmenetelmän toimintaperiaate käytettäessä menetelmää todentamiseen olioiden A ja B välillä on esitetty kuvassa 6.



Kuva 6: Julkisen avaimen menetelmä; todentaminen

Selite: pk_A = olion A julkinen avain
sk_A = olion A salainen avain

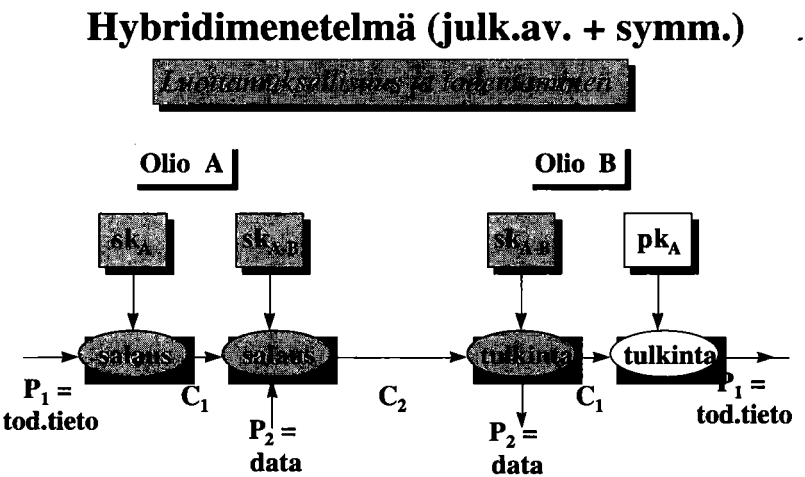
Automaattisessa avainten vaihdossa yhdistetään molemmat edellä esitetyt periaatteet. Tämä toimintaperiaate olioiden A ja B välillä on esitetty kuvassa 7.



Kuva 7: Julkisen avaimen menetelmä; automaattinen avainten vaihto

Selite: pk_A = olion A julkinen avain
sk_A = olion A salainen avain
C_1 = salakieli 1
data = uusi avain
tod.tieto = todentamisen turvaamiseksi tarvittava lisäinformaatio
pk_B = olion B julkinen avain
sk_B = olion B salainen avain
C_2 = salakieli 2

Sovelluksissa, joissa tarvitaan sekä luotettavaa todentamista että tehokasta ja nopeaa luottamuksellisuuden turvaamista, voidaan käyttää symmetrisen ja julkisen avaimen menetelmän yhdistelmää, josta käytetään nimitystä *hybridimenetelmä*. Sen toimintaperiaate on esitetty kuvassa 8.



Kuva 8: Hybridimenetelmä; luottamuksellisuus ja todentaminen

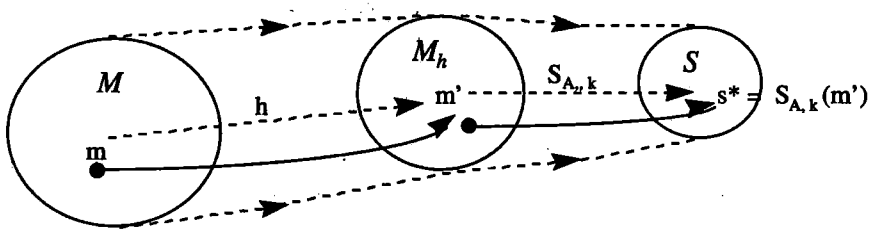
Selite: pk_A = olion A julkinen avain
sk_A = olion A salainen avain
C_1 = salakieli 1
P_1 = todentamisinformaatio
P_2 = salattava "massa"-data
sk_{A-B} = olioiden A ja B hallussa oleva salainen avain
C_2 = salakieli 2

5.3.5 Sähköiset allekirjoitukset

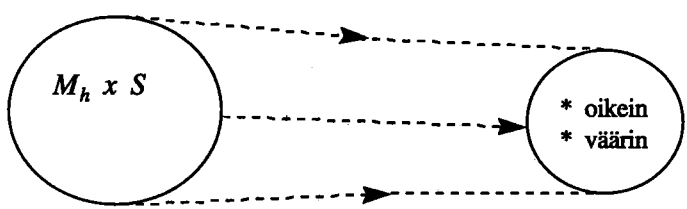
Käyttäjä muuntaa allekirjoitettavan tiedon allekirjoitetuksi sähköiseksi dokumentiksi allekirjoitusalgoritmia ja omaa salaista avaintaan käyttäen. Kuka tahansa, jolla on tiedossaan vastaava julkinen avain, voi todentaa tämän allekirjoitetun dokumentin olevan kyseisen käyttäjän muodostama.

Sähköisiä allekirjoituksia käytetään tietolähteiden varmistamiseen (data origin authentication), eheyden varmistamiseen (digital signature scheme with recovery) sekä kiistämättömyyden varmistavana mekanismina ilman luotettua kolmatta osapuolta. Sähköistä allekirjoitusalgoritmia käytettäessä allekirjoitettavan tiedon on ehdottomasti sisällettävä riittävästi redundanssia ("ylimääräistä informaatiota", joka yksilöi allekirjoituksen), joko luonnostaan tai keinotekoisesti lisättynä esimerkiksi tiedoista lasketun tiivisteen muodossa ("törmäyksettömyys").

Sähköiset allekirjoitukset jaetaan kahteen pääryhmään, tiivisteen allekirjoittaviin (digital signature schemes with appendix) ja allekirjoitetun tiedon palauttaviin (digital signature schemes with message recovery) menetelmiin. Ensin mainitut ovat ainakin toistaiseksi eniten käytettyjä käytännössä. Tiivisteen allekirjoittavan menetelmän toimintaperiaate on esitetty kuvassa 9.



(a) Allekirjoitusprosessi



(b) Todennusprosessi

Kuva 9:Tiivisteen allekirjoittavan sähköisen allekirjoituksen menetelmä

Selite: m = sanoma-avaruuden M yksi sanoma h = tiivistefunktio
m' = sanoman m tiiviste M_h = tiivisteiden avaruus
k = kertakäyttöinen satunnaistieto S = allekirjoitusten avaruus
$S_{A,k}$ = A:n ainutkertainen allekirjoitusfunktio
s = A:n ainutkertainen allekirjoitus sanomalle m

5.3.6 Tietoturvatiivisteet

Tiivistealgoritmeilla (hash function) lasketaan mielivaltaisen pituisesta tiedosta lyhyt, määrätyn kokoinen tiiviste (esimerkiksi 128 bittiä). Tietoturvatarkoituksiin käytettävältä tiivistefunktiolta vaaditaan, että se on:

* yksisuuntainen (one-way): annetulle tiivisteelle on laskennallisesti mahdotonta muodostaa sellaista dataa, jonka tiiviste se on sekä
* törmäyksetön (collision-resistant): laskennallisesti on mahdotonta löytää kahta eri dataa, joilla on sama tiiviste.

Eniten käytännössä käytetty tiivistefunktio on vielä tällä hetkellä MAC-algoritmi (Message Authentication Code), joka perustuu DES-algoritmin käyttöön.

5.4 Avainten hallinta

5.4.1 Symmetriset algoritmit

Symmetrisellä algoritmilla saavutettavan turvallisuuden edellytyksiä avainten hallinnalle ovat:

* avaimet ovat vain oikeutettujen, mahdollisimman harvojen käyttäjien tiedossa,
* edellinen vaatimus koskee sekä käytössä olevia, myöhemmin käyttöön tulevia että joskus käytössä olleita avaimia,
* avaimet on generoitava satunnaislähdettä käyttäen; tällä varmistetaan, että kaikki teoreettisesti mahdolliset avaimet tulevat käyttöön yhtä suurella todennäköisyydellä,
* "verkot" on pidettävä mahdollisimman pieninä,
* kussakin sovelluksessa ja eri organisaatiotasoilla eri avaimet, jos samaa algoritmia käytetään eri sovelluksissa,
* varsinkin ylimmillä organisaatiotasoilla tulisi olla kutakin käyttötarkoitusta varten vähintään kaksi, vaihtoehtoista, toisistaan riippumatonta salausmenetelmää,
* kutakin avainta käytetään mahdollisimman lyhyen ajan, tavoitteena "keskusteluavain" -periaate,
* avainten hallinnan hallinnollinen, organisatorinen ja fyysinen turvallisuus on järjestettävä mahdollisimman tehokkaaksi (kirjanpito, säilytys, hävittäminen, käytön jatkuva jäljitettävyys, ilmoitukset, toipumismenettelyt)

MUISTA !

1) Salaustekniikalla pyritään saamaan lisäturvallisuutta tilanteissa, joissa käyttöön liittyvä turvallisuus on kaikin osin kunnossa.

2) Salausmenetelmät ja algoritmit ovat ainakin periaatteessa julkisia; niillä saavutettava turvallisuus riippuu ainoastaan avainten hallinnan turvallisuudesta.

3) Historiaa tarkasteltaessa lähes kaikki salausmenetelmien ensimmäiset ratkaisut ovat perustuneet avainten hallinnan virheisiin tai muihin käyttöturvallisuuden puutteellisuuksiin.

5.4.2 Epäsymmetriset algoritmit

Epäsymmetriseen algoritmiin perustuvat palvelut (todentaminen, automaattinen avainten jakelu, allekirjoitusmenetelmät yms) edellyttävät päätelaitteisiin ja tiettyihin verkkojen osiin tai käyttäjäkohtaisille tietovälineille (esimerkiksi toimikortti) tallennettuja laite- tai käyttäjäkohtaisia, salaisia avaimia sekä niistä loogisesti riippuvien, koko järjestelmälle ja sen kaikille käyttäjille julkisten avainten generointia ja hallintaa.

Avainten generoinnissa ja hallinnassa on noudatettava soveltuvin osin edellä, symmetristen algoritmien yhteydessä lueteltuja periaatteita.

5.4.3 Automaattinen avainten hallinta

Manuaalisen avaintenhallinnan vastuun jakautuminen useille eri organisaatiotasoille asettaa suuria toiminnallisia, ajallisia ja sisäiseen turvallisuuteen liittyviä vaatimuksia ja paineita näiden tasojen tietoturvapäälliköille, henkilöstöille ja laitteistoille. Näitä paineita voidaan vähentää usein merkittävästi ottamalla käyttöön yhteysavainten (= keskusteluavainten) jako tiedonsiirtoyhteyksiä ja tietojärjestelmiä käyttäen.

Käyttöön on tulossa yhä enemmän laitteita ja järjestelmiä, joissa on perinteisen, manuaalisen avaintenhallinnan lisäksi tai sijasta automaattinen avaintenhallinta. Kehitys näyttää johtavan siihen, että automaattinen avainten hallinta tulee syrjäyttämään perinteisen manuaalisen avainten hallinnan ainakin tavallisten käyttäjien ympäristössä. Salaustekniikka näyttää tavallisten käyttäjien osalta muuttuvan yhä enemmän "läpinäkyväksi" oheistoiminnaksi, johon tavallinen käyttäjä ei voi vaikuttaa. Automaattisen avainten hallinnan pysyminen turvallisena edellyttää avaintenhallinnasta huolehtivien laitteiden, niiden osien ja ohjelmistojen käytön ja toiminnan tarkkaa seurantaa sekä salaisten avaintietojen vaihtamista ajoittain. Lisäksi on mietittävä sovelluskohtaisesti tarvitaanko esimerkiksi toipumismenettelyissä automaattisen avainten hallinnan lisäksi myös manuaalista avaintenhallintaa. Saattaa olla myös sovelluksia, joissa manuaalisen avainten hallinnan käyttö päämenetelmänä on perusteltua.

5.4.4 Avainten hallinnasta eri käyttösovelluksissa

Jo käytössä olevien samoin kuin käyttöön tulossa olevien, lähiverkkojen pohjalta rakennettujen hajautettujen tietojärjestelmien salaustekniikkaan perustuva tietoturvallisuus edellyttää järjestelmän tekniikkaan sekä sovelluksiin sopivaa avaintenhallintajärjestelmää.

Monista teknisistä syistä johtuen tietojärjestelmissä käsiteltävien ja siirrettävien tietojen luottamuksellisuutta turvataan yleisesti symmetrisiä salausmenetelmiä (DES, IDEA, SAFER, BLOWFISH, A5, ...) käyttäen. Nämä puolestaan edellyttävät käytettävien avainten turvallista jakoa ja muuta hallintaa. Tietojen käytettävyyden varmistamiseksi avaimet on useissa sovelluksissa saatava käyttöön

myös siinä tapauksessa, että käyttäjä tai käyttäjät ovat hävittäneet käytössään olleet avaimet. Symmetristen menetelmien avaintenhallinta toteutetaan yleisesti epäsymmetrisiä tai julkisen avaimen salausmenetelmiä (Diffie-Hellman, RSA, ElGamal, ...) käyttäen.

Paitsi symmetristen algoritmien avaintenhallinnassa, epäsymmetrisiä ja julkisen avaimen menetelmiä käytetään myös erilaisissa todennusratkaisuissa, eheyden valvontamekanismeissa, digitaalisissa allekirjoituksissa ja kiistämättömyyden varmistusmekanismeissa. Epäsymmetristen algoritmien käyttö edellyttää useissa tapauksissa keskitettyä, yksi- tai useampitasoista avainten hallinta- ja tarvittaessa myös hakemistopalvelua. Tällöin puhutaan tavallisesti luotettavista kolmansista osapuolista (Trusted Third Party = TTP). USA:ssa on kehitetty oma kansallinen TTP-versio, josta käytetään nimeä Key Escrow -järjestelmä (= KE). KE:n oleellisin ero eurooppalaiseen TTP'een verrattuna on avainten saanti tarvittaessa eri viranomaisten (tiedusteluorganisaatiot, poliisi, ...) käyttöön. KE:ssa tämä on mahdollista ilman kohdeorganisaation myötävaikutusta ja sen tietämättä. TTP:ssa tätä mahdollisuutta ei välttämättä ole lainkaan. Jos TTP sisältää mainitun mahdollisuuden, sitä voidaan käyttää vain yhteistoiminnassa kohdeorganisaation kanssa.

6 Salaustekniikan hyvyys

6.1 Salaustekniset turvapalvelut

6.1.1 Yleistä

Salausteknisillä tietoturvapalveluilla tavoitellaan yleensä korkeampia tietoturvallisuuden tasoja kuin mitä sovelluksiin sisältyvillä ratkaisuilla voidaan saavuttaa. Tästä syystä salausteknisille ratkaisuille tulee yleensä asettaa korkeat laatuvaatimukset.

Salaustekniikkaan perustuvilla mekanismeilla voidaan toteuttaa seuraavia tietoturvapalveluja:

6.1.2 Luottamuksellisuus (Confidentiality)

■ Tiedolle asetettu vaatimus, jonka mukaan tietoa ei ole luvattomien henkilöiden, olioiden tai prosessien saatavissa, eikä sitä paljasteta niille

n ISO:n OSI-mallin tietoturvallisuusosan mukaan sisältää 4 ala-aluetta (= yhteyden, yhteydetön, valitun kentän ja liikennevirran luottamuksellisuus)

* symmetriset eli yhden salaisen avaimen salausalgoritmit: jonosalaajat (stream cipher), lohkosalaajat (block cipher)

* epäsymmetriset salausalgoritmit: julkisen avaimen (public key) ja muut moniavaimiset (dual or multiple key asymmetric) algoritmit

6.1.3 Todentaminen (Authentication)

■ Käsittää yksittäisen käyttäjän, koneen, ohjelmistokomponentin tai minkä tahansa muun olion väitetyn identiteetin todentamisprosessin, (entity authentication) sekä tietolähteen todentamisen (data origin authentication)

■ ISO:n OSI-mallin tietoturvallisuusosan mukaan 6 kohdealuetta (tietolähteen todentaminen, yhteyden eheys toipumisineen ja ilman, yhteyden eheys valitulle kentälle, yhteydetön tiedon eheys sekä valitun kentän yhteydetön eheys)

* symmetriset salausalgoritmit: todennus- ja eheystarkisteet, (e.g. message authentication code)
* julkisen avaimen salausalgoritmit
* salaustekniset tarkistusfunktiot
* nollatietotekniikkaan perustuvat mekanismit
* sähköiset allekirjoitukset

Todentamisen johdannaisia ovat:

* kiistämättömyys
* tekijänoikeus, luotetun tekijänoikeusviranomaisen avulla
* hakemistopalvelu (directory) ja
* varmennepalvelu (certificate)

6.1.4 Automaattinen avainten jakelu ja vaihto

* symmetriset menetelmät luotetun avainten hallintakeskuksen avulla
* julkisen avaimen menetelmät

6.1.5 Pääsyn valvonta

* salasanat
* yhden avaimen algoritmin avulla (salaus tai MAC)
* julkisen avaimen algoritmin avulla
* nollatietomenettelyt

Lueteltujen tietoturvallisuuspalvelujen toteutuksessa saatetaan lisäksi tarvita seuraavia apualgoritmeja:

* tiivistefunktiot (hash functions)
* redundanssin muodostaminen
* satunnaislukujen generointi
* alkulukujen generointi

6.1.6 Salausmenetelmien käyttösovelluksista

Salausmenetelmien käyttösovelluksia ovat:

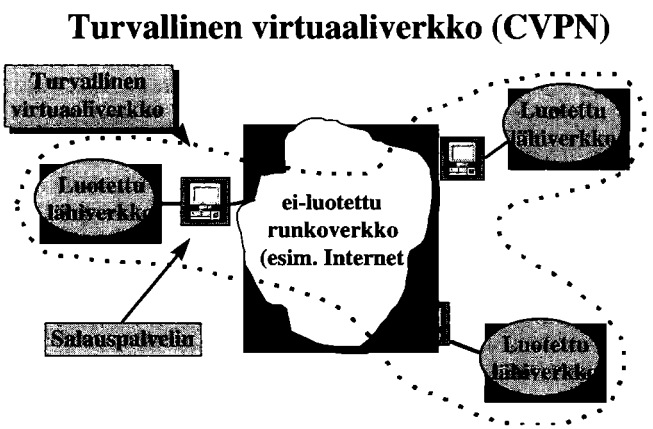
* Ohjelmallisesti tai moduleina järjestelmiin integroidut salausmenetelmät ja
* Erillisten salauslaitteiden käyttö. Erityisesti tiedonsiirrossa käytetään siirtolaitteisiin (päätelaitteet, modeemit yms) kytkettäviä, erillisiä salauslaitteita, jotka

turvaavat siirrettävien tietojen luottamuksellisuuden salaamalla ja tulkitsemalla siirtosuunnan mukaan automaattisesti kaiken niiden kautta kulkevan liikenteen sisällön. Kaksisuuntaisilla yhteyksillä voidaan käyttää salausmenetelmäsovelluksia, jotka turvaavat siirrettävien tietojen luottamuksellisuuden lisäksi myös liikennevirran luottamuksellisuuden. Tällöin mahdollinen salakuuntelija ei saa selville edes aikoja, jolloin informaatiota siirretään.

Salausmenetelmiä voidaan käyttää televerkoissa ja tietojärjestelmissä eri kohteissa ja eri tasoilla.

Tietojen siirrossa salaus voi käsittää ainoastaan siirrettävät tiedot (*sanomasalaus*) tai niiden lisäksi myös ohjaustiedot (*linjasalaus*). Viimeksi mainitussa tapauksessa salattu lähete joudutaan usein tulkitsemaan solmukohdissa ohjaustietojen selville saamiseksi.

Salaustekniikan käyttöä muodostamaan turvallinen "putki", salattu virtuaalinen yksityisverkko = CVPN (= Ciphered Virtual Private Network) yli turvattoman verkon (esimerkiksi Internet) on esitetty kuvassa 10.



Kuva 10: Salattu virtuaalinen yksityisverkko, CVPN

6.1.7 Salausmenetelmät ja kokonaistietoturvallisuus

Kokonaistietoturvallisuus edellyttää yleensä salauksen lisäksi monia muita turvallisuuden parantamiseen tähtääviä toimenpiteitä. Laajimmillaan salausmenetelmiin perustuvia, loogisia turvallisuuden kehittämiskeinoja (= *turvapalveluja*) käytetään hajautetuissa tietojärjestelmissä. Kokonaiskuvan saamiseksi hajautetun tietojärjestelmän turvattavista kohteista ja turvapalveluista on tarkasteltava avointen järjestelmien tietoturva-arkkitehtuuria ISO:n (International Organization for Standardization) OSI-mallin (The Basic Reference Model for Open Systems Interconnection) avulla.

Uusimmilla salausmenetelmien teknisillä sovelluksilla voidaan pyrkiä turvatason parantamiseen tietoturvan kaikilla viidellä osa-alueella. Teknisten sovellusten kehitystyössä pyritään nykyisin noudattamaan mahdollisimman paljon ISO:n OSI-mallin tietoturvalisäyksessä standardoituja/standardoitavia palveluja. OSI-mallin tietoturvalisäyksessä tietoturvan viisi osa-aluetta jaetaan edelleen tässä kirjoituksessa aikaisemmin mainittuihin *tietoturvapalveluihin, joita on yhteensä 14 kappaletta. Tietoturvapalvelut toteutetaan käyttäen kahdeksaa mekanismia.* Mekanismit ovat:

- tietojen sisällön salaaminen
- sähköinen allekirjoitus
- pääsynvalvonta
- eheyden valvonta
- todentaminen
- liikenteen täyttö
- reitityksen valvonta ja
- tapahtumien kirjaaminen

6.2 Salausalgoritmien ratkaisutavat

Salausmenetelmien ja -algoritmien *ratkaisemista* koskevaa tiedettä ja oppia kutsutaan *kryptoanalyysiksi* (engl. Kryptanalysis). Kryptoanalyysin tavoitteena on joko salattuna olevan selväkielen ratkaiseminen tuntematta salausmuunnoksessa käytettyä avainta tai käytetyn avaimen ratkaiseminen. Lähtökohtana pidetään, että ratkaisija (= kryptanalyst) tuntee täysin käytetyn salausalgoritmin.

Tärkeimpiä perusratkaisutapoja ovat:

1) Vain salakieleen perustuva ratkaisu (Ciphertext-only attack)
* Ratkaisijalla on samalla algoritmilla salattuja sanomia
* Tavoitteena on ratkaista sanomia tai avain/avaimia
* "Työvälineenä" on muun muassa kielen statistiikka
* "Varma tapa" = Kaikkien avainten kokeilu (= Brute Force Attack)

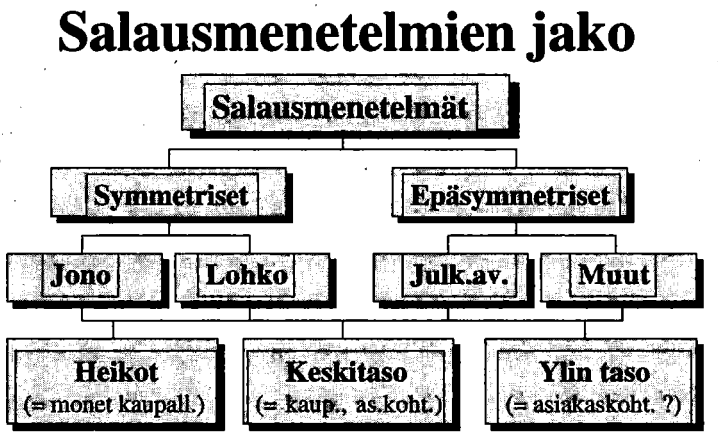
2) Tunnettuun selväkieleen perustuva ratkaisu (Known-plaintext attack)
* Ratkaisijalla on salakieli-selväkieli pareja
* Tavoitteena on päätellä käytetty avain/avaimet tai
* algoritmi kaikkien samaa avainta käyttäen salattujen sanomien ratkaisemiseksi

3) Valittuun selväkieleen perustuva ratkaisu (Chosen-plaintext attack)
* Ratkaisijalla on salakieli-selväkieli pareja sekä
* mahdollisuus valita tietty selväkieli (ja sitä vastaava salakieli)
* Peruste: Tietyt selväkielet (tai selväkielilohkot) "siirtävät" enemmän tietoa avaimesta salakieleen
* Tavoitteena on päätellä käytetty avain/avaimet tai
* algoritmi kaikkien samaa avainta käyttäen salattujen sanomien ratkaisemiseksi

6.3 Valintakriteerit

6.3.1 Salausmenetelmien jako

Salausmenetelmät voidaan jakaa karkeasti luokkiin kuvassa 11 esitetyllä tavalla. On kuitenkin huomattava, että yksittäisen salausmenetelmän sopivuus määrättyyn sovellukseen ja / tai turvapalveluun on arvioitava jokaisessa erityyppisessä tilanteessa erikseen ottaen huomioon muun muassa organisaation tietoturvapolitiikassa sovellukselle asetetut tietoturvallisuusvaatimukset sekä mahdollisimman konkreettinen uhkatilanne esimerkiksi organisaation ydinprosessien turvallisuusanalyysiin perustuen. Erityisesti valmistajakohtaisten algoritmien käyttöönotto edellyttää lisäksi algoritmien yksityiskohtien asiantuntevaa analysointia.



Kuva 11: Salausmenetelmien eräs jako

6.3.2 Salausmenetelmien tärkeimpiä "laatukriteerejä":

* mahdollisten salaisten avainten (= käyttäjän määritettävissä olevien erilaisten salausohjelmien) lukumäärä,
* jaksollisten menetelmien jakson pituus,
* satunnaisuus,
* matemaattinen kompleksisuus

HUOM !

1) Edellisen luettelon kahdessa ensimmäisessä kohdassa mainittuja ominaisuuksia kuvataan tunnusluvuilla, joiden on oltava riittävän suuria.

2) Mikäli nämä tunnusluvut ovat riittävän suuria, niiden perusteella ei yleensä voida verrata eri menetelmien keskinäistä hyvyyttä.

6.4 DES:n turvallisuudesta tänään

Varma tapa ratkaista DES on kaikkien avainten järjestelmällinen kokeilu (Brute Force Attack). Tätä ratkaisutapaa varten on mallinnettu erikoistietokone, joka kykenee vuoden 1993 arvioiden mukaan ratkaisemaan käytetyn avaimen noin 3 1/2 tunnissa. Koneen hinnaksi arvoitiin vuonna 1993 noin 1 M$. DES on niin laajalle levinnyt, että olisi lapsellista kuvitella, että NSA ja vastaavat organisaatiot eivät olisi rakentaneet kyseessä olevaa konetta. On myös syytä muistaa, että kustannusten arvoidaan putoavan viidenneksellä kymmenessä vuodessa. DES siis heikkenee koko ajan.

Kaikkien avainten järjestelmällisen kokeilun ohella voidaan käyttää edistyneempiä ratkaisutekniikoita. Eräs niistä on differentiaalinen kryptoanalyysi, jonka NSA tunsi jo paljon ennen 1970-luvun puoliväliä eli paljon ennen DES:n standardiksi tuloa. On lapsellista kuvitella, että NSA:n teoreetikot olisivat olleet toimettomina sen jälkeen; on melko varmaa, että he ovat kehittäneet uudempia DES:n ratkaisutekniikoita. Tästä ei kuitenkaan ole näyttöä, ainoastaan huhuja.

Winn Schwartau kirjoittaa, että NSA on rakentanut massiivisen DES:n ratkaisukoneen jo 1980-luvun puolivälissä. Todennäköisesti on myös olemassa joukko algoritmeja, joilla voidaan pienentää DES:n avainten kokeiluun perustuvan ratkaisun kompleksisuutta useilla kertaluokilla. DES:n sisäisiin toimintoihin perustuvilla algoritmeilla voidaan osittaisratkaisujen perusteella hylätä mahdottomina avainjoukkoja ja täten pienentää merkittävästikin kokeilutyötä. Tilastollisia algoritmeja käyttäen voidaan pienentää vielä lisää DES:n avainten tehollista kokoa. Muita algoritmeja voidaan käyttää todennäköisten avainten, esimerkiksi tulostuskelpoiset ASCII-merkit yms, kokeiluun. Huhutaan, että NSA kykenee ratkaisemaan "täys-DES:n" 3-15 minuutissa riippuen etukäteen mahdollisen prosessoinnin määrästä. Tällaisten ratkaisujärjestelmien hinta on suuruusluokkaa 50.000 $. DES:n ratkaisumahdollisuuksia koskevat huhut samoin kuin niiden jatkuva lisääntyminen merkitsevät käytännössä sitä, että varsinkaan korkeimman tason turvallisuutta vaativissa sovelluksissa edes "täys-DES:a" ei voida pitää riittävän turvallisena.

Markkinoilla on saatavissa DES-tuotteita, joissa käytetään standardoitua lyhempää avainta. On selvää, että tällaisten tuotteiden turvallisuus voi olla ratkaisevasti "täys-DES:a" alempi. Niissä esiintyy usein myös tilastollisia säännönmukaisuuksia, joilla voidaan monissa tapauksissa helpottaa ratkaisua huomattavasti. Todettakoon, että USA yleensä sallii nykyään yleensä myös "täys-DES":n viennin rajoituksitta.

Eräs mahdollisuus parantaa "täys-DES:lla" saavutettavaa turvallisuutta on käyttää Bihamin suunnittelemaa, avaimesta riippuvien S-lohkojen sovellusta. Se lisää algoritmin kestävyyttä kaikkien avainten kokeiluun perustuvaa ratkaisua vastaan sekä tekee myös differentiaalisen ja lineaarisen kryptoanalyysin vaikeammaksi. Tällä tavalla modifioitu DES on ratkaistavuuden kannalta vähintään tavallisen DES:n tasoinen ja samalla selvästi erilainen kuin tavallinen DES. Tämä piirre pakottaa ratkaisua yrittävät kehittämään tälle "uudelle algoritmityypille" soveltuvat ratkaisumenetelmät.

6.5 RSA:n turvallisuudesta tänään

RSA:n turvallisuus perustuu täydellisesti suurten lukujen tekijöihin jaon vaikeuteen. Ei ole kuitenkaan koskaan todistettu matemaattisesti, että on tarpeellista jakaa n tekijöihin, jotta selväkielisanoma m voitaisiin määrittää salakielisanoman c ja julkisen avaimen e perusteella. Voidaan olettaa, että jossain vaiheessa saatetaan keksiä täysin uusi tapa ratkaista RSA. Tällä hetkellä ei ole tietoa mainitusta ratkaisutavasta.

Todennäköisin tapa yrittää ratkaista RSA-salaus on yhä yritys jakaa moduuli n tekijöihin. Tämän ratkaisutavan mahdollisuuksista esiintyy eri lähteissä hyvin erilaisia tietoja. Eräänä melko luotettavana kriteerinä voitaneen pitää USA:n vientirajoituksiin liittyviä kannanottoja. Tällä hetkellä USA:sta saadaan yleensä viedä RSA-tuotteita, joiden moduuli n on enintään 512 bittiä. Tämä voidaan tulkita niin, että USA:n tiedusteluorganisaatiot kykenevät ratkaisemaan lähes viiveettä RSA-tuotteiden salaukset 512-bittiseen moduuliin asti. Tällä perusteella varsinkin korkeaa salausturvallisuutta vaativissa sovelluksissa tulisi käyttää vähintään 1024 bittistä RSA:a.

6.6 A5 :n turvallisuudesta

Tähän algoritmiin liittyy runsaasti outoa politiikkaa. Alunperin ajateltiin, että GSM'n salaustekniikka saattaisi estää puhelimien viennin joihinkin maihin. Nyt jotkut viranomaiset ovat esittäneet, että vientiongelmia ei pitäisi syntyä, kun otetaan huomioon A5:n taso, joka on niin heikko, että viranomaisongelmiin ei ole aihetta. Eräs huhu kertoo, että NATO'n tiedusteluorganisaatioilla oli 1980-luvun puolivälissä kissanhännänvetoa siitä pitäisikö GSM'ssa käyttää vahvaa vai heikkoa salausta. Saksalaiset halusivat vahvaa salausta, koska he olivat lähellä entistä Neuvostoliittoa. Muut maat kumosivat kuitenkin heidän vaateensa ja A5 onkin ranskalaisten kehittämä.

Perusratkaisutapa vaatii 2^{40} kokeilua. Tässä ratkaisussa arvataan kahden ensimmäisen rekisterin sisällöt ja määritetään sen jälkeen kolmannen sisältö algoritmin tuottaman bittijono perusteella. Tuotettu bittijono voidaan määrittää tunnetun tai valitun selväkielen ratkaisumenetelmällä. Tämän ratkaisutavan tehon riittävyydestä kiistellään. Samalla kuitenkin nähdään, että kehitteillä oleva avainten kokeilulaite tulee ratkaisemaan tämän kiistan pian.

A5:n taustalla olevat perusideat ovat hyviä. Tältä osin A5 on hyvin tehokas. Se läpäisee kaikki tunnetut tilastolliset testit. Sen ainoa heikkous on, että sen rekisterit ovat niin lyhyitä, että kaikkien avainten riittävän nopea kokeilu on mahdollista.

A5:n muunnokset, joissa käytetään pidempiä rekistereitä ja monimutkaisempia takaisinkytkentöjä ovat todennäköisesti turvallisia.

7 Tietoturvallisuuden kansainvälisestä kehityksestä

7.1 Vienti- ja tuontirajoitukset

7.1.1 Yleistä

Salaustuotteisiin kohdistuu eri maissa viranomaistoiminnoista ja niiden mahdollistamisesta johtuvia vienti-, tuonti- ja käyttörajoituksia. Viraomaistoiminnoista johtuvien rajoitusten tärkeimpänä syynä on epäilemättä se, että erityisesti korkeatasoisen salaustekniikan käyttö rajoittaa ja hidastaa merkittävästi viranomaisten ja niihin verrattavien organisaatioiden teletoimintaan ja tietotekniikkaan kohdistamia tiedustelutoimia. Salaustekniikka voi usein jopa estää täysin mainitun tiedustelun.

Vientirajoituksista keskeisimmässä asemassa kansainvälisesti tarkasteltuna ovat USA:n vientirajoitukset.

Omalta osaltaan rajoituksia tuovat myös patentit. Niillä turvataan ensisijaisesti tuotteiden kehittäjien ja valmistajien taloudellisia etuja.

7.1.2 USA

USA pitää salaustuotteita aseina, jotka uhkaavat muun muassa kansallista turvallisuutta sekä vaikeuttavat rikosten tutkintaa. Näistä syistä salaustuotteiden vientiä koskevat samat rajoitukset kuin aseiden vientiä. USA:n edustajat sanovat jatkuvasti, että salaustuotteet "väärissä käsissä" voivat olla uhka kansalliselle turvallisuudelle sekä este rikosten tutkinnalle. "Väärillä käsillä" USA:n edustajat sanovat tarkoittavansa rikollisten lisäksi myös "vihamielisiä" julkishallinnon organisaatioita eri puolilla maailmaa. Eri yhteyksissä on lisäksi käynyt ilmi, että samaan "vihamielisten tahojen" joukkoon voivat joskus myös kuulua USA:n talouden kannalta eri tavoin vaaralliset teollisuus- ja liikeyritykset eri puolilla maailmaa.

USA:ssa julkaistiin vuoden 1995 alkupuolella vientirajoitusten muutossuunnitelmia lähinnä salausteknisten tuotteiden valmistajien vaatimuksesta heidän kilpailumahdollisuuksiensa parantamiseksi kansainvälisillä vientimarkkinoilla. Näiden suunnitelmien sekä niihin liittyneen jatkokäsittelyn tulosten tärkeimmät kohdat USA:sta tuotavien salaustuotteiden käyttäjien kannalta ovat:

* USA pitää tärkeänä vahvojen salausteknisten ratkaisujen saamista "sähköistyvän maailman" käyttöön.

* Vienti sallitaan rajoituksitta vain tuotteille, jotka eivät estä tiedusteluorganisaatioiden (CIA, ...) ja poliisin telekuuntelua ja tietojärjestelmiin kohdistuvia tutkimuksia.
* DES-tuotteiden (vast), joissa käytetään enintään 40 bittistä avainta vientiä ei rajoiteta. Tämä kohta on muutettu vuoden 1997 alussa 56 bittiin.
* RSA-tuotteiden, joissa käytetään enintään 512 bittistä moduulia vientiä ei rajoiteta.
* Salaustuotteille, joissa käytetään KEY ESCROW-tekniikan mukaista avainten hallintaa, myönnetään vientilisenssit. KEY ESCROW-tekniikka antaa viranomaisille mahdollisuudet myös vahvoilla salausmenetelmillä salattujen tietojen tulkintaan ilman kohdeorganisaation myötävaikutusta ja kohdeorganisaation tietämättä..
* USA "TARJOAA" KEY-ESCROW-TEKNIIKKAA VAPAAEHTOISENA TEKNILLISENÄ MAHDOLLISUUTENA

7.2 EU

EU:n komission alaisena toimivan, EU:n tietoturvallisuuden kehittämisestä vastaavan SOG-IS -ryhmän (Senior Officials Group-Information Security) puheenjohtaja on esittänyt seuraavat yhdeksän tietoturvallisuuden kehittämisperiaatetta:

* Luotettavan turvallisuuden tarjoaminen sisältäen hajautettujen tietojärjestelmien teknisen käytön edellyttämän luotettavien kolmansien osapuolten järjestelmän (=TTP-järjestelmä) sekä luotettavan asiantuntija-avun tarjoamisen evaluointiin.
* Vapaaehtoinen käyttö, joka tarkoittaa muun muassa sitä, että käyttäjiä ei sidota julkishallinnon organisaatioiden määrittelemiin tai tarjoamiin teknillisiin ratkaisuihin. Käytännössä tämä merkitsee myös sitä, että EU:n periaatteissa ei kannateta USA:n voimakkaasti ajamaa KEY ESCROW -avaintenhallinnan järjestelmää, joka antaisi viranomaisille mahdollisuudet salatun tietoliikenteen sekä salattujen tiedostojen tulkintaan ja tutkimiseen kohdeorganisaation tietämättä.
* Markkinavetoisuus, jolla tarkoitetaan sitä, että salaustekniikkaan perustuvat turvallisuuspalvelut ja tuotteet tulee kehittää ainoastaan liike-elämän ja teollisuuden kaupallisten tarpeiden pohjalta. Niitä ei saa keinotekoisesti ohjata tai pakottaa julkishallinnon organisaatioiden valtuuksilla tai rajoituksilla.
* Avoimmuus & ei-rajoitettu, jolla tarkoitetaan, että salaustekniikkaan perustuvien turvallisuusratkaisujen kehittämistä ei tule rajoittaa millään tavalla (ks. myös edellinen kohta).
* Kansainvälinen perspektiivi, jonka mukaan laajamittaiseen käyttöön otettavien tietoturvallisuusratkaisujen tulisi olla käytettävissä yli kansallisten rajojen.
* Otettava huomioon kansalliset velvoitteet. Tämän kohdan mukaan eri maissa voi olla omaan lainsäädäntöön tai omaan kansalliseen turvallisuuteen perustuvia näkökohtia, jotka on otettava huomioon päätettäessä kansallisista ratkaisuista (esimerkiksi USA:n KEY ESCROW-järjestelmä).

* Tekninen tehokkuus ja mahdollisesti myös järkevyys. Tämän vaatimuksen toteuttamisella pyritään auttamaan alan erikoistekniikkaan perehtymättömiä käyttäjiä sekä huolehtimaan kansallisista vaatimuksista (ks. myös edellinen kohta) mahdollisesti johtuvien viranomaisten vaatimusten toteutumisesta.
* Laillinen tehokkuus ja ehkä myös hyväksyttävyys (ks. edelliset kohdat / viranomaisten kansallinen toiminta).
* Ratkaisujen on mahdollistettava tulevaisuuden haasteet.

EU:ssa valmistellaan tällä hetkellä TTP-järjestelmän lisäksi muun muassa tietoteknisten järjestelmien ja niiden elementtien sertifiointi- ja sertifikaattien hyväksymisjärjestelmää. Mainittua järjestelmää tultaneen laajentamaan jatkossa kattamaan myös tietojärjestelmiin perustuvat palvelut. Tähän laajennusajatukseen liittyy myös sertifioinnin perusteina tällä hetkellä olevien normistojen kehittäminen. Näyttää siltä, että EU-maissa tällä hetkellä käytössä olevat ITSEC- ja ITSEM-normistot tullaan korvaamaan ehkä jo 2-3 vuoden kuluessa kansainvälisen kehitystyön tuloksena syntymässä olevalla COMMON CRITERIA-normistolla.

7.3 Kehitys Suomessa

Suomi on osallistunut ja osallistuu jatkuvasti sekä EU:ssa että OECD:ssa käynnissä oleviin tietoturvallisuuden kehityshankkeisiin.

Suomessa on jo tällä hetkellä eräiden organisaatioiden käytössä TTP-ratkaisuja. Uusia ratkaisuja kehitetään parhaillaan useissa organisaatioissa.

Valtiovarainministeriön hallinnon kehittämisosaston alaisissa työryhmissä määritellään ja kehitetään sähköistä asiakirjaa ja tähän liittyen myös TTP-ratkaisua. Periaatteet ovat pääpiirtein samat kuin edellä esitetyt EU:n suuntaviivat. Tässä työssä ollaan myös kiinteässä yhteydessä lainsäädäntöä kehittäviin tahoihin. Valtiovarainministeriön johdolla tehtävän työn eräänä keskeisenä tavoitteena on kehittää ratkaisut, jotka mahdollistavat eri organisaatioiden sisäisten järjestelmien yhdistämisen valtakunnalliseksi järjestelmäksi sekä edelleen kansallisen järjestelmän liittymisen osaksi kansainvälistä järjestelmää.

7.4 OECD

7.4.1 Yleistä

OECD:ssa valmistellaan parhaillaan uuden tietoturvallisuuspolitiikan käyttöönottoa vuonna 1997 alkavalle 5-vuotiskaudelle. Politiikkaa kehitettäessä näytti loppuvaiheisiin asti siltä, että tällä politiikalla tulisi olemaan huomattava rooli kansainvälisessä tietoteknisessä infrastruktuurissa (GII = Global Information Infrastructure). Lähinnä viranomaisten mahdollisuuksista päästä käsiksi salattuihin tietoihin ja / tai salaisiin salausavaimiin ratkaisemattomiksi jääneet erimielisyydet eri OECD-maiden välillä aiheuttivat sen, että politiikka jäi melko yleiselle tasolle.

7.4.2 Lähtökohta

Uuden politiikan luonnin merkittävänä lähtökohtana oli USA:n vuonna 1995 monessa yhteydessä esittämät vaatimukset "vahvan salaustekniikan" käytön rajoittamiseksi kansainvälisin sopimuksin. Vaihtoehtona salaustekniikan tason rajoituksille USA on esittänyt "KEY ESCROW" avainten hallintajärjestelmää, joka antaisi viranomaisille mahdollisuudet avainten hallintajärjestelmän kautta salatun tietoliikenteen sekä salattujen tiedostojen tulkintaan ja tutkimiseen kohdeorganisaation tietämättä.

USA perustelee lähtökohtaansa kansainvälisen rikollisuuden torjunnalla. Todellisuudessa vähintään yhtä merkittävä peruste on USA:n tiedusteluorganisaatioiden halu säilyttää mahdollisuutensa kansainvälisten tieto- ja tietoliikennejärjestelmien tiedusteluun, yritysvakoilu mukaan luettuna. Samanlainen halu on selvästi myös eräillä muilla, "vahvan salaustekniikan" käytön rajoituksia kannattavilla mailla.

Lukumääräisesti suurin osa OECD-maista (mm. pohjoismaat ja EU:n komission SOG-IS -ryhmän puheenjohtaja) eivät kannata "vahvan salaustekniikan" käytön rajoittamista. Nämä maat pitävät välttämättömänä vahvan salaustekniikan käyttöä "tietoteknistyvän maailman" tietoturvallisuuden keskeisenä osana.

7.4.3 Suositus jäsenmaille

Vähän yli vuoden aikana käytyjen useiden neuvottelujen tuloksena on saatu aikaan luonnos, joka jaettaneen jäsenmaille OECD:n uutena salaustekniikan käyttöpolitiikkana vuoden 1997 aikana. Luonnoksessa suositellaan, että jäsenmaat:

* luovat uudet tai parantavat olevia politiikkoja, menettelytapoja, käytäntöjä ja proseduureja vastaamaan ja ottamaan huomioon politiikkaluonnoksen liitteessä määritellyt salauspolitiikan käyttöperiaatteet
* neuvottelevat, koordinoivat ja toimivat yhdessä kansallisella ja kansainvälisellä tasolla politiikan suuntaviivojen toteuttamiseksi
* toimivat käytännöllisten ja toiminnallisten ratkaisujen hyväksi kansainvälisen salauspolitiikan alueella käyttäen suuntaviivoja perustana kansainväliseen salauspolitiikkaan liittyvissä erityissopimuksissa
* levittävät tietoa suuntaviivoista sekä julkiselle että yksityiselle sektorille edistämään tietoisuutta salaustekniikkaan liittyvistä asioista ja periaatteista
* poistavat tai välttävät luomasta salaustekniikan käyttöpolitiikan nimissä tarpeettomia esteitä kansainväliselle kaupalle sekä tieto- ja tietoliikenneverkkojen kehitykselle
* määrittelevät selkeästi sekä saattavat julkiseen tietoisuuteen kaikki kansalliset kontrollit, joita julkishallinto toteuttaa salaustekniikan käyttöön liittyen
* tarkastelevat suuntaviivoja vähintään joka viides vuosi tarkoituksena parantaa kansainvälistä yhteistyötä salaustekniikan käyttöpolitiikkaan liittyen

7.4.4 Mitä saatiin todellisuudessa sovituksi

* Koko OECD:a kattavaan sopimukseen ei päästy, jotkut jäsenmaat säätelevät kansallisin määräyksin voimakkaasti salaustekniikan käyttöä (mm. USA, Ranska ja Englanti), monet jäsenmaat (mm. pohjoismaat) eivät näe tällaisia rajoituksia tarpeellisiksi eivätkä hyväksy niitä.
* Kansallisten rajoitusten ja määräysten huomioon ottaminen "kansallisella tasolla" hyväksyttiin laajasti.
* Kansallista säädöksistä riippuen eri kansallisilla tasoilla käytetään "vapaasti valittavissa olevaa" (mm. pohjoismaat) ja "säädöksin rajoitettua" salaustekniikkaa (mm. USA, Englanti ja Ranska)
* Tulos merkitsee käytännössä, että "kädenvääntö" USA:n (ja sen kannattajien) sekä vapaan käytön kannattajien välillä jatkuu.

Ristiriidat merkitsevät käytännössä sitä, että OECD:n monet jäsenmaat kehittävät omia infrastruktuurejaan ilman merkittävää kansainvälistä yhteistyötä. Myös EU:ssa tehtävällä kehitystyöllä on tässä tilanteessa huomattavasti suurempi merkitys kuin OECD:n politiikkaa kehitettäessä näytti. On selvää, että OECD:ssa vallitseva tilanne tulee lähivuosina aiheuttamaan vaikeuksia ja hidastamaan kansainvälisten tieto- ja tietoliikennejärjestelmien tietoturvallisuuden kehitystä.

LÄHTEET:

Julkaistut:

[1] BRUCE SCHNEIER, "Applied Cryptography", second edition, John Wiley & Sons, Inc, New York, 1996 (ISBN 0-471-11709-9).
[2] ALFRED J. MENEZES, PAUL C. van OORSCHOT, SCOTT A. VANSTONE, "Handbook of Applied Cryptography", CRC Press, New York, 1997
(ISBN 0-8493-8523-7).
[3] GREGORY B. WHITE, ERIC A. FISCH, UDO W. POOCH, "Computer and Network Security", CRC Press, New York, 1996 (ISBN 0-8493-7179-1)
[4] ISO-standardi ISO/IEC 7498-2, Part 2: Security Architecture (1988)
[5] ISO-standardi ISO/IEC 9798-4 (1995)
[6] Liikenneministeriön valmiusohje 4/95, Valtion Painatuskeskus, ISSN 1238-2159, ISBN 951-723-923-8

Julkaisemattomat:

1. OECD:n vuosien 1997-2002 tietoturvallisuuspolitiikan valmisteluasiakirjat vv. 1995-1997
2. EU:n tietoturvallisuuden sertifiointia koskevan järjestelmän kehittämistyöryhmän dokumentaatio vv. 1995-1997
3. Kirjoittajan luento- ja esitelmämateriaalit vv. 1995-1997