Tuomas Kirstilä

Tietoverkon käyttäjän tietoturvan parantaminen salausmenetelmiä käyttäen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Koulutusohjelman nimi

Insinöörityö

2.5.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Tuomas Kirstilä Tietoverkon käyttäjän tietoturvan parantaminen salausmenetelmiä käyttäen 48 sivua 2.5.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Kari Järvi

Tässä opinnäytetyössä tutustutaan salausmenetelmien käyttömahdollisuuksiin ja ominaisuuksiin kenen tahansa tietoverkon käyttäjän näkökulmasta. Opinnäytetyön tavoitteena on esitellä ja kokeilla tärkeimpiä ja arkikäyttöön soveltuvimpia salausohjelmistoja tietoverkon käyttäjän tietoturvallisuuden parantamiseksi. Opinnäytetyössä käydään läpi tietoturvan ja salausmenetelmien teoriaa, perehdytään salausohjelmistojen keskeisimpiin ominaisuuksiin sekä tutustutaan käytännönläheisesti ohjelmistojen asennus- ja käyttövaiheisiin erityisesti tietoverkossa tapahtuvaa sähköpostiviestintää silmällä pitäen. Lopuksi pohditaan ja arvioidaan soveltuvin osin ohjelmistojen tarjoamia ominaisuuksia ja hyötyjä. Työ tehtiin Metropolia Ammattikorkeakoululle.

Avainsanat	Tietoturva, salaus, PGP

Author(s) Title Number of Pages Date	Tuomas Kirstilä Improving the desktop computer user's data security by using encryption methods 48 pages 2.5.2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networking
Instructor(s)	Kari Järvi, Principal Lecturer

This thesis explores the theory, properties, installation and using of encryption software that are available for any desktop computer user in today's data networks. The objective of this final project is to investigate and implement some of the most common and important encryption software for everyday use in order to achieve a high level of data security. This thesis was carried out for Metropolia University of Applied Sciences.

In the thesis the data security and encryption systems are handled in the theoretical level as well as in the practical level. The theoretical part consists of the fundamentals and most significant parts of data security and encryption methods whereas the practical part of this study focuses on deploying appropriate encryption software used in e-mail communication in particular. Finally the preferences and usability of software are considered and evaluated.

Keywords	Data security, encryption, PGP

Sisällys

Lyhenteet

AES	Advanced Encryption Standard, lohkosalausjärjestelmä,
Algoritmi	Tarkasti määritelty vaihesarja, jota seuraamalla voidaan ratkaista tietty ongelma.
Internet	Maailmanlaajuinen tietoverkko.
Intranet	Lähiverkko, joka on eristetty tietyn ryhmän käyttöön.
IP	Internet-protokolla. Teknologia, joka mahdollistaa tiedon siirtämisen verkon yli.
Kryptologia	Tieteenala, joka tutkii kryptografiaa eli viestien salaamista sekä kryptoanalyysia, salausten murtamista.
TCP/IP	Transmission Control Protocol/Internet Protocol. Internet-verkoissa käytetty protokollaperhe.

1 Johdanto

Henkilökohtaisten tietokoneiden ja tietoverkkopalveluiden yleistyttyä tietoturvallisuusasiat ovat nousseet osaksi arkipäiväämme. Yksityisten tietojen säilyminen asiaankuulumattomilta turvassa koetaan yleensä erityisen tärkeäksi. Laite- ja käyttäjämäärän nopea kasvu on kuitenkin luonut olosuhteet, joissa tietojen salassa pysyminen ei ole aina itsestäänselvyys. Esimerkiksi sähköpostiviesti voi sisältää henkilökohtaisia tietoja, joita viestin lähettäjä ei missään tapauksessa haluaisi päätyvän muun kuin osoittamansa vastaanottajan tietoon. Valitettavasti tiedot saattavat joutua myös ulkopuoliselle, mikäli kyseistä seikkaa ei ole erityisen tarkasti huomioitu. Usein ainoa ratkaisu tietojen salassa pitämiseen ja tietoturvan parantamiseen on salausmenetelmien käyttö. Moni tietoverkon käyttäjä ei kuitenkaan ole tietoinen niiden käyttömahdollisuuksista, tarkemmista ominaisuuksista puhumattakaan.

Tässä opinnäytetyössä tarkoitukseni onkin selvittää, milloin ja miten tietoverkkojen käyttäjä voisi hyödyntää salausmenetelmiä tietoturvallisuutensa parantamiseksi. Päämääräni ei ole kaiken kattava selvitys mahdollisimman moniin käyttötarpeisiin, vaan keskityn aihepiiriin mielestäni tärkeän sähköpostiviestinnän näkökulmasta. Tietoturvan ja salausmenetelmien kokonaisuuden kannalta sivuan toki muitakin salauksiin liittyviä ja huomionarvoisia sovellusalueita etenkin teorian tasolla. Perehdyn aiheeseen ja salausohjelmistojen käyttöön lähtökohtaisesti ketä tahansa yksittäistä tietoverkon käyttäjää silmällä pitäen.

Aluksi tutustun salausmenetelmien taustoihin ja keskeisimpään teoriaan mahdollisimman käytännön läheisesti. Varsinaista salaustiedettä eli kryptologiaa tai tietoturvallisuuden osa-alueita käsittelen siis vain asiayhteyden vaatimalla tavalla. Teoriaosuuden jälkeen paneudun salausmenetelmien käyttöön vapaasti käytettävissä olevan PGP-ohjelmiston avulla. Tutustun ohjelmiston ja sen eri versioiden käyttöönottoon ja ominaisuuksiin erityisesti sähköpostiviestinnän ja siihen liittyvien tiedoston salauksen, digitaalisen allekirjoituksen ja avaintenhallinnan kannalta. Arvioin soveltuvin osin ohjelmiston käytettävyyttä, hyötyjä ja mahdollisia haittoja. Tarkoitukseni ei toisaalta ole yksityiskohtaisen asennus- ja käyttöönottodokumentaation laatiminen. Lopuksi pohdin ja esitän teorian sekä työn aikana kertyvien käytännön havaintojen pohjalta näkemyksiäni tietoturvan parantamisen mahdollisuuksista salausmenetelmien avulla.

2 Tietoturva ja salausmenetelmät

2.1 Taustaa ja historiaa

Salaus ja tietoturva ovat tietotekniikassa yleisesti käytettyjä termejä. Niiden varsinaiset merkitykset, sekä termien väliset yhteydet ja eroavuudet eivät silti välttämättä ole itsestäänselvyyksiä edes aihepiiriä tunteville ihmisille. Monesti termit rinnastetaan toisiinsa ja niiden ymmärretään tarkoittavan samaa tai lähes samaa asiaa. Se ei kuitenkaan pidä paikkansa, vaikka ne läheisesti liittyvätkin toisiinsa. Aluksi onkin syytä tutustua termeihin tarkemmin.

Tietoturva on tavoitetila, jossa tiedot, järjestelmät ja palvelut ovat suojattuja erilaisia uhkia vastaan sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla. Tietoturvan tavoitteet luokitellaan tilanteesta ja aiheyhteydestä riippuen hieman eri tavoin. Yleisesti tietoturva jaetaan seuraaviin osa-alueisiin: luottamuksellisuus, eheys, kiistämättömyys ja todennus. Lisäksi näistä johdettavia, mutta usein myös omina osa-alueinaan pidettäviä, ovat saatavuus ja pääsynvalvonta. Salausmenetelmillä voidaan ratkaista luottamuksellisuuden, eheyden ja kiistämättömyyden periaatteet. Salausmenetelmät muodostavat siis tärkeän, vaikkakin pienen osa tietoturvan kokonaisuudesta. [2, s.20.]

Salakirjoituksia tutkiva tieteenala on kryptologia, jonka kehityskaari on pitkä osaksi nykyisten tietoverkkojen tietoturvaa. Historiassa salaus yhdistetään usein sodankäyntiin, jossa sen rooli onkin ollut tärkeä kautta aikojen. Salakirjoituksen juuret ulottuvatkin muinaisen Egyptin, Mesopotamian ja antiikin Rooman aikakausiin. Tekniikan kehittymistä edistivät merkittävästi myös arabit luodessaan salakirjoitukseen liittyviä menetelmiä n. 800-luvulla. Yhä edelleen osa aihepiirin käytössä olevasta termistöstä on peräisin kyseiseltä aikakaudelta. Salakirjoituksen käytön tarpeeseen ovat aikanaan vaikuttaneet esimerkiksi lukutaito tai -taidottomuus sekä vieraat kielet – kirjoitettu teksti tai tuntematon kieli saattoivat jo sellaisinaan olla riittäviä salauksia. Myöhempiä, tämän päivän salausmenetelmien syntyyn olennaisesti vaikuttaneita vaiheita ja tekniikoita ovat olleet erityisesti radio, toisen maailman sodan aikana ja sen jälkeen kehitetty sotatekniikka, sekä viime vuosikymmenten aikana tietoverkot palveluineen.

2.2 Tietoturvan osa-alueet

Luottamuksellisuus (engl. confidentiality) tarkoittaa, että tieto on vain siihen oikeutettujen henkilöiden saatavilla. Tämä voidaan varmistaa salauksen avulla, jolloin tieto ei ole ulkopuolisten luettavissa, ja tunnistamalla vastapuoli, jolloin tiedetään kenelle tietoa luovutetaan. Salausmenetelmillä voidaan siis turvata tiedon säilytyksessä tai siirrossa sen luottamuksellisuus.

Eheys (engl. integrity) varmistaa tietojen pysymisen suojassa oikeudettomilta muutoksilta. Se pyritään saavuttamaan tiivisteiden käytön avulla tiedon muuttumisen havaitsemiseksi, sekä pääsynhallinnalla tiedon alkuperän selvittämiseksi. Näin ollen myös eheyden tavoitteeseen voidaan vaikuttaa salausmenetelmillä, koska tiivisteillä voidaan huomata tiedoissa tapahtuneet muutokset ja toisaalta salauksella varmistaa tiivisteiden turvassa pysyminen. Kuitenkaan pelkkä salaus ei takaa eheyttä, koska salatutkin tiedot voivat muuttua tahattomasti esimerkiksi siirron yhteydessä tai niitä voidaan muokata tahallisesti. Tällöin eheys menetetään, vaikka luottamuksellisuus edelleen säilyykin eli tietosisältö pysyy ulkopuolisilta salattuna.

Saatavuus eli käytettävyys (engl. availability) on nimensä mukaisesti tiedon olemista tarvittaessa saatavilla. Siihen siis vaikuttavat lähinnä tekniset laitteet ja järjestelmät, niiden toimivuus, varmuus ja varajärjestelyt. Salausmenetelmien merkitys on tämän periaatteen toteutumisessa olematon ja oikeastaan sillä on vain käänteinen merkitys; esimerkiksi salasanan unohtaminen estää saatavuuden.

Pääsynvalvonnalla (engl. access control) varmistetaan tietyn käyttäjän tai ohjelman eli subjektin pääsy ainoastaan sille määritettyihin kohteisiin eli objekteihin. Normaalisti se on käyttöjärjestelmän ja sovelluksen tehtävä, mutta myös salausta voidaan hyödyntää pääsynvalvonnan turvaamisessa.

Kiistämättömyys (engl. nonrepudiation) vaalii tietoon kohdistuvien toimenpiteiden oikeaksi osoittamisen periaatetta. Tiedon hakeminen, lukeminen, luonti jne. voidaan yksiselitteisesti osoittaa tapahtuneen tietyn käyttäjän toimesta. Kiistämättömyyden periaatteen sovelluskohteita ovat yksittäisten käyttöjärjestelmien lisäksi esimerkiksi teletunniste- ja potilastietojärjestelmät. Myös sähköisessä allekirjoituksessa kiistämättömyydellä on keskeinen rooli. Salaustekniikoiden avulla voidaan estää sähköisen allekirjoituksen väärentäminen.

Todennuksella (engl. authentication) varmistetaan tietoon liittyvien osapuolten henkilöllisyys (ihmiset) tai aitous (sovellukset). Tämä onkin tietoturvan kriittisin osa-alue, koska siihen liittyvät ongelmat mitätöivät yleensä myös muiden osa-alueiden merkityksen. Lisäksi se on vaikein osa-alue toteuttaa. Salausmenetelmillä todennukseen voidaan vaikuttaa digitaalisen allekirjoituksen kautta. Yleisesti todennusmenetelmiä ja -tapoja on lukuisia. Henkilöiden kohdalla todennus voi perustua kolmeen tekijään:

- Mitä henkilöllä on hallussaan (esim. avain, kulkukortti).
- Mitä henkilö tietää (esim. salasana, henkilötunnus).
- Yksilölliseen ominaisuuteen (esim. sormenjälki, ääni, kasvonpiirteet).

Yksinään mikään tekijöistä ei yleensä tarjoa riittävän vahvaa ja luotettavaa todennusta, joten tarvittaessa kyseisiä keinoja yhdistetään. Esimerkiksi verkkopankin todennustapa voi perustua kahden tai useamman tekijän yhdistelmään; henkilön hallussa olevaan listaan ja henkilön tietämään asiaan, kuten seuraava salasana. Vastaavasti pankkikortissa todennus pohjautuu kortin siruun ja siihen liittyvään tunnuslukuun. Perinteisiä todennusmenetelmiä ovat esimerkiksi allekirjoitus tai henkilötunnus, jotka eivät tosin ole erityisen vahvoja menetelmiä. [4, s. 38.]

Pelkästään edellä mainitut esimerkit kuvaavat hyvin sitä, kuinka haasteellista todennuksen suorittaminen voi olla. Salausmenetelmillä todennukseen voidaan tuoda lisäominaisuuksia, vaikka ne eivät siihen liittyviä periaatteellisia ongelmakohtia poistakaan. Tällaisia ratkaisuja ovat muun muassa haaste-vaste -menetelmä, HST-kortti sekä varmenteet. [4, s. 40.]

3 Salausmenetelmien teoriaa

3.1 Kryptologia, kryptografia ja kryptoanalyysi

Kryptologialla tarkoitetaan salakirjoitusoppia eli tiedettä, joka tutkii ja kehittää tiedon salaamisen (kryptografia) sekä salauksen purkamisen (kryptoanalyysi) toteuttavia algoritmeja. Kryptologia on yli 2000 vuotta vanha tieteenala, jonka tarkoitusta voidaankin yksinkertaisimmillaan havainnollistaa sen syntyajoilta peräisin olevilla alkeellisilla salausmenetelmillä. Sellainen on esimerkiksi Caesarin menetelmä, jossa teksti salataan

korvaamalla alkuperäiset merkit aakkosissa ennalta sovitun merkkimäärän päässä olevilla merkeillä.

Kryptologiaan perustuvia järjestelmiä toteutetaan *Kerckhoffin periaatteen* mukaisesti. Sen mukaan salaus on varma, vaikka kaikki salaus- ja purkumenetelmien yksityiskohdat olisivat julkisia ja tunnettuja salaista avainta lukuunottamatta. Nykyaikaiset salausmenetelmät perustuvat kehittyneiden salausalgoritmien (DES, AES, IDEA, Blowfish jne.) sekä pitkien salausavaimien käyttöön. [5, s. 65.]

Kryptografian tavoite on siis sanoman tai sen lähettäjän ja vastaanottajan salaaminen tai autentikointi eli oikeaksi todistaminen. Kryptografisen eli salatun järjestelmän pitäisi olla varma. Teoriassa täysin varma salausjärjestelmä on rajattomallakin laskentakapasiteetilla murtamaton. Käytännössä se ei välttämättä toteudu parhaimmassakaan tapauksessa, mutta normaalisti rajallisella laskentakapasiteetilla salauksen murtaminen voi kuitenkin olla erittäin vaikeaa ja aikaa vievää. [5, s. 65.]

Kryptoanalyysi tutkii matemaattisesti ja kielellisesti salausten purkamista ja turvallisuutta. Yksinkertaisimmillaan se voi perustua kielellisten tekijöiden, kuten tiettyjen kirjainten esiintymistiheyden tutkimiseen. Muita perinteisiä menetelmiä ovat esimerkiksi ns. brute force eli kaikkien merkkivaihtoehtojen ja yhdistelmien kokeileminen, differentiaalinen analyysi salattavan ja salatun tekstin muutoksia vertailemalla, sekä lineaarinen kryptoanalyysi salaamattoman ja salatun tekstin välisiä riippuvuuksia tutkimalla.

3.2 Salausavaimet ja algoritmit

Aiemmin mainittu Caesarin menetelmä toimii yksinkertaisen salausalgoritmin mukaisesti. Sanoman jokainen kirjain korvataan saman aakkoston, tässä tapauksessa 26 merkkiä sisältävän latinalaisen aakkoston toisella, salausavaimen määrittämällä etäisyydellä olevalla merkillä. Käytetty salausavain on tällöin yhden merkin mittainen. Avaimia on 26 kappaletta, joten salaus on helppo purkaa käymällä läpi kaikki 26 avainvaihtoehtoa. Jos merkkimäärä on vaikkapa 3, salakirjoitetaan teksti TI KLO KOLME muotoon VL NOR NROPH. Matemaattisesti salausalgoritmin toiminta voidaan esittää muodossa: $e(x) = (x + k) \pmod m$. Salaus (e) kirjaimelle (x) muodostetaan siis avaimen (k) avulla käytetyn merkistön sekä koodattavien merkkien lukumäärän (m) mukaan.

Vastaavasti salauksen purku (d) suoritetaan käänteisellä funktiolla: d(x) = (x - k) (mod m).

Hieman Caesarin menetelmää kehittyneempi on Vignérin menetelmä, jossa avainpituutta kasvatetaan yhdistämällä useampi Caesarin menetelmässä käytetty avain. Näin salauksen murtaminen hankaloituu hieman, mutta kovin monimutkaisesta salauksesta ei edelleenkään ole kyse. Esimerkiksi jos käytetään vastaavaa aakkostoa ja kolmen merkin pituista avainta 2, 5, 3, salataan teksti POHJOINEN KAKSI KM muotoon RTKLTLPJQ MFNUN NO.

Näiden niin sanottujen korvaamisalgoritmien lisäksi on muitakin alkeellisen tason salausalgoritmeja. Yksi tällainen on siirtomenetelmä, jossa alkuperäinen sanoma salataan siirtämällä merkit tietyn logiikan mukaisesti. Merkit säilyvät samoina, mutta niiden järjestys näyttää ulkopuoliselle sekavalta. Salattu sanoma TSITLKTSOTIAOSOTRALKYIIA ja sen puretaan siirtotaulukolla muotoon TORSTAI ILTA KLO YKSITOISTA (Kuva 1.).

T	S	I	T	L	K	T	S
O	T	I	A	O	S	O	T
R	A	L	K	Y	I	I	A

Kuva 1. Siirtotaulukko.

Hieman pidemmälle viety siirtomenetelmän muoto voi olla seuraavan kaltainen, jossa avaimen pituus on 10 merkkiä (Kuva 2.).

AVAIN:
Selväkielinen: 1 2 3 4 5 6 7 8 9 10
Salausavain: 5 2 7 1 3 9 6 4 10 8
SALAUS:
Paikka: 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 10
Salaamaton teksti: SALAUS SIIRTO ESIMERKKI
Salattu teksti: UASSLISARIIOETEKMSKRI

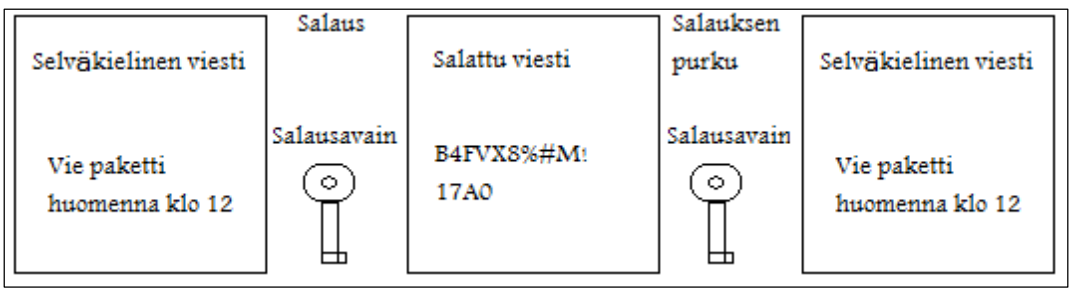
Kuva 2. Salaus siirtomenetelmällä.

Yhteistä edellä kuvatuille esimerkeille on salatun viestin esitys samalla merkistöllä, jolloin ongelmaksi muodostuu kielellisten tekijöiden toistuminen myös salatussa sanomassa ja siten sen helppo arvattavuus. Tällaisia ovat esimerkiksi tietyt sanat, yksittäiset kirjaimet tai muutaman kirjaimen yhdistelmät, jotka esiintyvät käytetyssä kielessä muita yleisemmin. Näitä erottelemalla ja yhdistelemällä eli ns. frekvenssianalyysillä salauksen purkaminen on helppoa. Kyseiset menetelmät ovat siitä huolimatta osaltaan perusta nykypäivänkin algoritmeille. Korvaamiseen ja siirtoon perustuvien tekniikoiden kehittäminen sekä erilaisten niihin pohjautuvien yhdistelmien luominen ja avainpituuksien kasvattaminen ovat luonnollisesti olleet keskeisiä tekijöitä algoritmien kehityksessä.

Uudenaikaisemmista algoritmeista esimerkiksi DES seuraajineen perustuu edellä kuvattuihin alkeellisiin salausmenetelmiin ja niiden yhdistelemiin sekoitus- ja hajautusmenetelmin tehostettuna.

3.3 Symmetriset ja epäsymmetriset salausmenetelmät

Salausmenetelmät tai -järjestelmät jaetaan yleisesti symmetrisiin eli salaisen avaimen menetelmiin ja epäsymmetrisiin eli julkisen avaimen menetelmiin. Perinteisesti käytetyt salausmenetelmät ovat symmetrisiä. Symmetrisessä menetelmässä sekä viestin salaus että salauksen purku suoritetaan samalla avaimella. Salausavainta käyttäen viestistä muodostetaan ulkopuoliselle lukukelvoton merkkijono, joka takaa viestin salassa pysymisen suhteellisen varmasti. Viestin vastaanottaja purkaa merkit jälleen selväkieliseksi viestiksi käyttäen samaa avainta (Kuva 3.) Symmetrisen salauksen suurin ongelma on saman avaimen käyttö viestin lähettäjällä ja vastaanottajalla, jolloin avaimen paljastumisen riski on suuri.



Kuva 3. Symmetrinen salaus.

Epäsymmetrisessä salausmenetelmässä viestin salaukseen ja salauksen purkamiseen käytetään julkisen ja salaisen avaimen sisältävää avainparia (Kuva 4.). Menetelmää kutsutaan myös julkisen avaimen salausmenetelmäksi. Viestin salaamiseen käytetään vastaanottajan julkista avainta, jonka jälkeen viestin avaaminen onnistuu ainoastaan vastaanottajan salaisella avaimella. Epäsymmetrisen salauksen huono puoli on menetelmän hitaus ja resurssivaatimukset – suurempien tietomäärien salaaminen vie aikaa ja tiedostojen koko kasvaa.

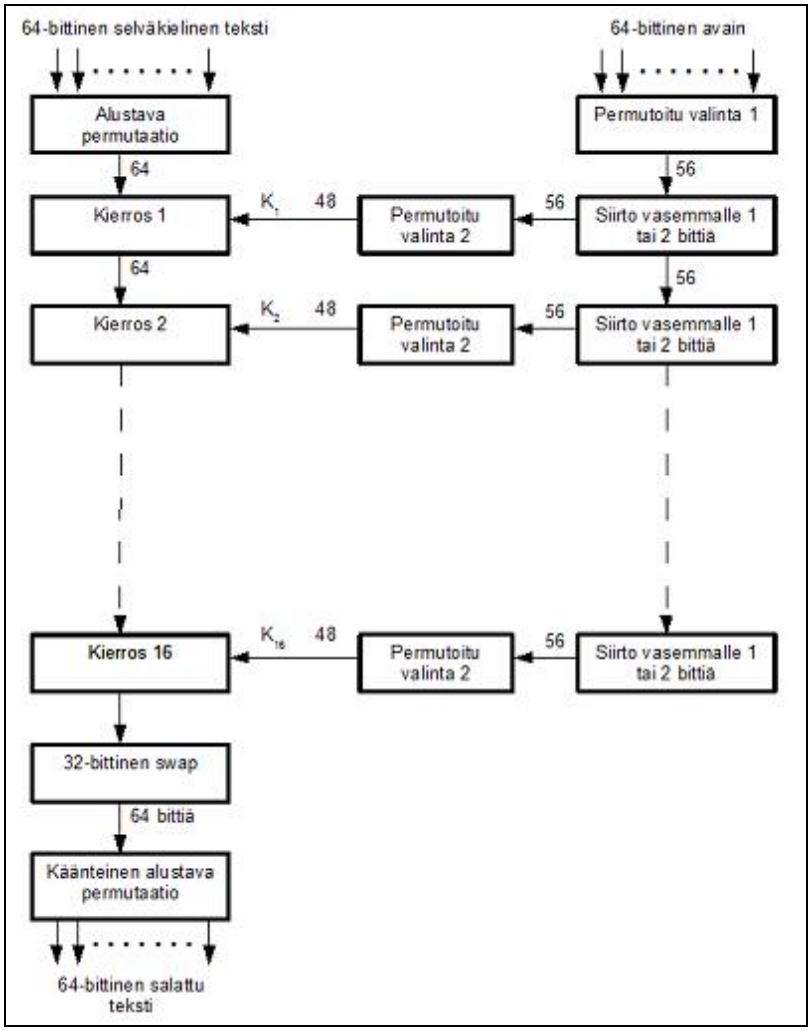
Kuva 4. Epäsymmetrinen salaus.

Menetelmät voidaan myös yhdistää, jolloin vältytään yksittäisen menetelmän heikkouksilta. Yhdistäminen tapahtuu siten, että viesti salataan kertakäyttöisellä symmetrisellä avaimella, joka edelleen salataan vastaanottajan julkisella avaimella. Näin muodostuneen salatun viestin lisäksi vastaanottajalle toimitetaan kyseinen salattu kertakäyttöavain. Vastaanottaja avaa kertakäyttöavaimen salaisella avaimellaan ja sen jälkeen sitä käyttäen salatun viestin. Windows-käyttöjärjestelmän Encrypted File System (EFS) perustuu symmetrisen avaimen ja epäsymmetrisen avaimen käyttöön. Tiedostot salataan ja palautetaan symmetrisellä avaimella, joka on salattu käyttäjän julkisella avaimella.

3.3.1 Symmetriset salausalgoritmit

Tunnetuimpiin ja käytetyimpiin symmetrisiin salausalgoritmeihin kuuluu lohkosalausalgoritmi DES (Data Encryption Standard), joka on kehitetty vuonna 1977. Se on pohjimmiltaan muutettu ja yksinkertaistettu versio IBM:n kehittämästä LUCIFER-salausjärjestelmästä. DES käyttää 56-bittistä avainta, jonka lisäksi 8-bittiä on varattu pariteettitarkistukseen. Samaa avainta käytetään salaukseen ja sen purkamiseen eli kyseessä on symmetrinen salausmenetelmä.

DES-algoritmissa salaus suoritetaan 64-bittinen lohko kerrallaan. Ensin 64-bittiselle selvätekstille suoritetaan alustava permutaatio, jossa käsiteltävät bitit järjestetään uudelleen. Tätä seuraa 16-kierroksinen vaihe, jonka jokaisella kierroksella toistetaan samoja siirto- ja permutaatiofunktioita. Kullakin kierroksella tuotetaan 56-bittinen aliavain (K1-K16). Näiden tuotos on lohkon sisältämän 64-bittisen selväkielisen tekstin ja salausavaimen muodostama esituloste, jolle suoritetaan lopuksi vielä alustavan permutaation käänteinen funktio eli käänteinen permutaatio, joka tuottaa 64-bittisen salatun tektin (Kuva 5.).

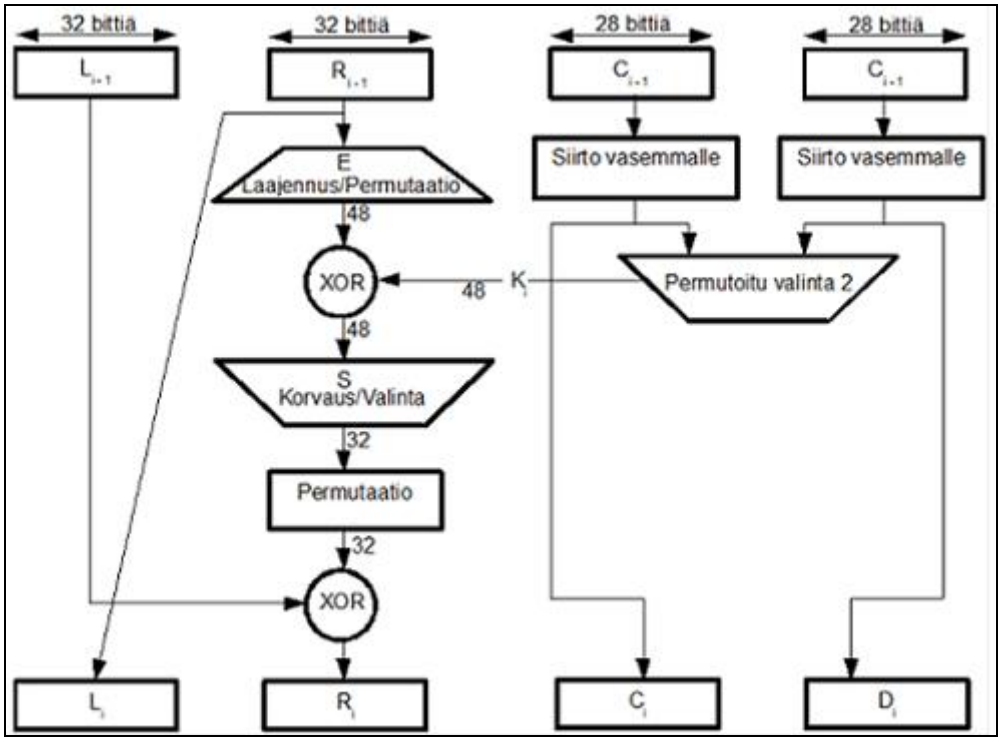


Kuva 5. DES-algoritmin toiminnan yleiskuvaus [7.].

Yksittäisen kierroksen vaiheisiin on hyvä tutustua tarkemminkin. Salattava 64-bitin lohko jaetaan siis aluksi 32-bittiseen vasempaan (L_0) ja oikeaan (R_0) lohkoon. Myös 56-bittinen avain jaetaan kahtia, 28-bittiseen vasempaan ja oikeaan osaan, joista permutoinnin eli avainosien sisältämien bittien siirto-operaatioiden seurauksena muodostuu

ns. permutoitu valinta 2 ja edelleen kierroskohtainen avain (K_i). Ensimmäisellä kierroksella oikean lohkon (R_0) sisältö syötetään funktiolle (F) kierroskohtaisen (K_1) avaimen kanssa. Funktion tulokselle sekä vasemman lohkon (L_1) sisällölle suoritetaan XOR-operaatio (poissulkeva tai-operaatio), josta muodostuu seuraavan kierroksen oikea lohko (R_1), eli $R_1 = L_0 \oplus F(R_0,K_1)$. Edeltävän kierroksen oikeasta lohkosta (R_0) tulee puolestaan seuraavan kierroksen vasen lohko (L_1) ja kierros alkaa alusta saman kaavan toistuessa jokaisella kierroksella. 16 kierroksen jälkeen vasen ja oikea lohko yhdistetään jälleen ja yksi kokonainen lohko on näin käsitelty.

DES:n toimintaan liittyvistä yksityiskohdista on lisäksi hyvä tietää funktion (F) toimintaperiaate hieman tarkemmin. Funktio sisältää kolme osaa; laajennuksen, S-laatikon ja permutoinnin. Laajennus (E) pidentää sisään tulevan 32-bittisen oikean lohkon 48 bitin mittaiseksi käyttämällä osaa lohkon biteistä kahteen kertaan. Tälle 48-bittiselle lohkolle ja kierrosavaimelle tehdään XOR-operaatio, jonka tulos viedään S-laatikkoon, jossa bittiyhdistelmä nimensä mukaisesti (S, substitute) korvataan toisella. Tämä on salauksen kannalta tärkeä vaihe, koska ilman sitä bittien riippuvuus olisi helppoa arvata differentiaalisen kryptoanalyysin avulla. S-laatikon käsittelyn jälkeen käytössä on jälleen 32 bittiä. Niille tehdään vielä permutointi, jonka jälkeen funktio on suoritettu (Kuva 6.).



Kuva 6. DES-algoritmin yksittäisen kierroksen vaiheet [7.].

Muutama vuosikymmen sitten kehitetty DES on yhä laajasti käytössä oleva salausalgoritmi, jossa ei ole suuria heikkouksia, vaikka lyhyt avain onkin vähentänyt sen käytettävyyttä ja se on murrettu alle vuorokaudessa. Siitä on kuitenkin kehitetty tehokkaampia versiota kuten 3DES. 3DES salaa tiedon käyttäen kolmea avainta. Koska DES:n avaimen pituus on 56 bittiä, saadaan 3DES:ssä avaimen pituudeksi 168 bittiä. 3DES-salauksessa luodaan ensin kolme 56-bittistä avainta. Ensimmäinen salaus tehdään avaimella yksi, sitten salaus puretaan avaimella kaksi ja lopuksi salataan avaimella kolme. Näin saadaan aikaan vahva salaus. DES-algoritmin merkittävä sovelluskohde on esimerkiksi pankkien tiedonsiirtoyhteyksien tietoturvamenetelmä PATU [6].

DES:n tapaan symmetrisiä lohkosalaukseen perustuvia salausmenetelmiä ovat esimerkiksi sitä kehittyneemmät AES, IDEA ja Blowfish sekä jonosalaukseen perustuvat RC4 ja SEAL. Lohkosalauksella tarkoitetaan siis menetelmää, jossa salattava teksti syötetään lohko kerrallaan salausalgoritmin läpi. Jonosalauksessa puolestaan salattava teksti syötetään algoritmille merkki kerrallaan.

Advanced Encryption Standard (AES) on DES:n seuraaja, jonka kehityksessä tavoitteena oli julkinen ja kaikille saatavilla oleva tehokas lohkosalaaja. Salausavain voi olla joko 128-, 192- tai 256-bittinen. Tiedon salaus tapahtuu sarjana muutoskierroksia, joissa algoritmiin syötettyä salaamatonta dataa muokataan tiettyjen vaiheiden kautta, kunnes haluttu kierrosmäärä tulee täyteen. Kierrosten lukumäärä riippuu salausavaimen pituudesta: 128-bittisellä avaimella suoritetaan 10, 192-bittisellä avaimella 12 ja 256-bittisellä avaimella 14 muutoskierrosta. Jokaiselle muutoskierrokselle lasketaan oma kierrosavain niin sanotun *Rijndaelin avainjärjestyksen* mukaan. [12.]

Muita tunnetuimpia salausmenetelmiä ovat muun muassa Rivest Cipher 4 (RC4) jonosalaus, jossa avaimen pituus voi olla jopa 2048-bittinen. Se on tunnetusti erittäin nopea ja vahva salausalgoritmi, jonka heikkous on saman avaimen käyttö kahden eri viestin salaamisessa. IDEA (International Data Encryption algorithm) on 128-bittistä avainta käyttävä salausmenetelmä, jota pidetään erittäin turvallisena, mutta hitaana. IDEA on PGP-ohjelman oletussalain. Blowfish-menetelmässä avaimen pituus voi olla 32 ja 448 bitin välillä. Lohkon koko on 64 bittiä ja salauskierrosten lukumäärä on 16.

3.3.2 Epäsymmetriset salausalgoritmit

Yleisin asymmetrinen salausalgoritmi on RSA, jonka kehittivät Ron Rivest, Adi Shamir ja Len Adleman vuonna 1977. Julkinen ja salainen avain muodostetaan suurista alkuluvuista yksisuuntaisella modulaarifunktiolla. Turvallisuus perustuu siihen, että kyseinen funktio on erittäin vaikea ja aikaa vievä laskea toisinpäin johtuen suurten lukujen tekijöihin jakamisen vaikeudesta. Algoritmissa avaimen pituus vaihtelee ja sen pituus ei ole suoraan verrannollinen symmetrisessä salauksessa käytettäviin pituuksiin, esimerkiksi 512-bittinen RSA on erittäin heikko.

Diffie-Hellman on Whitfield Diffien ja Martin Hellmanin avaimenvaihtoon kehitetty algoritmi, jonka tarkoituksena on taata turvallinen symmetrisen avaimen jakelu. Se perustuu matemaattiseen funktioon, jonka avulla voidaan generoida yhteinen salaisuus ja tätä kautta salattu avain tiedon salausta varten. Algoritmi tarjoaa siis vain avaimen jakelun, mutta ei salausta tai digitaalista allekirjoitusta. Digital Signature Algorithm (DSA) on algoritmi, jota käytetään vain todentamiseen, sillä ei voi salata tietoa.

3.4 Avainturvallisuus

Salausmenetelmien turvallisuuden kannalta tärkein yksittäinen tekijä on avainten hallinta. Se on yleensä koko järjestelmän haavoittuvin osa, koska kadonneen tai muuten paljastuneen avaimen myötä salaus menettää useimmiten merkityksensä. Näin ollen esimerkiksi salasanan, josta avain luodaan, laadulla ja säilytyksellä on keskeinen rooli. Tämän lisäksi salausmenetelmiin liittyvä avaintenvaihto tuo omat ongelmansa ja riskinsä, joten osapuolten välinen turvallinen avaintenvaihto täytyy myös ratkaista. Salausratkaisuissa avaintenvaihto on yleensä välttämätöntä, koska vaihtumaton ja säännöllisesti toistettu avain paljastuu ennemmin tai myöhemmin.

Arkielämän jokapäiväisiä ja useimmissa tapauksissa riittävän hyviä kanavia avaintenvaihtoon ovat poikkeavat ja yleisesti suojatut menetelmät. Viestinnän osapuolten ollessa tietoverkon käyttäjiä, voidaan siis käyttää tavallisesta liikennöinnistä poikkeavaa menetelmää silloin, kun salausavaimet vaihdetaan. Salasana voidaan lähettää esimerkiksi tietoverkon sijaan salatun GSM-verkon kautta tekstiviestinä, jolloin ulkopuolisen salakuuntelun mahdollisuus vähenee huomattavasti. Avain voidaan myös hajauttaa useaan eri kanavaan; vaikka osa tekstiviestinä, osa tavallisena kirjeenä, osa puhelimit-

se, osa kuriirin kautta. Tämä on erittäin hidas ja työläs, mutta melkoisella varmuudella turvallinen menetelmä. [4, s. 111.]

3.4.1 Diffie-Hellman-protokolla

Tietoverkon sisällä tapahtuvaan avainten vaihtoon on kehitetty tarkoituksenmukaisia ratkaisuja. Näistä ensimmäinen on 1970-luvulla alkunsa saanut Diffie-Hellman-avaintenvaihtoprotokolla, jonka keskeisimmät toimintaperiaatteet ovat seuraavat. Osapuoli 1 ja osapuoli 2 sopivat yhteisen alkuluvun Y ja geneerisen alkion g, jotka eivät ole salaisia eli ne voidaan vaihtaa huoletta avoimen kanavan läpi. Osapuoli 1 valitsee oman salaisen kokonaisluvun S1, ja laskee oman julkisen luvun P1 kaavalla: $P1 = g^{S1} \bmod Y$, jonka hän lähettää osapuolelle 2. Osapuoli 2 valitsee oman salaisen luvun S2, josta hän laskee vastaavasti oman julkisen luvun P2 kaavalla: $P2 = g^{S2} \bmod Y$, ja lähettää sen osapuolelle 1. Näin molemmilla osapuolilla on toistensa julkiset luvut. Mahdollinen salakuuntelija on myös saanut julkiset luvut P1 ja P2 yhteisten lukujen lisäksi lisäksi, mutta salaisista luvuista hänellä ei ole tietoa.

Osapuoli 1 laskee seuraavaksi avaimen $K = P2^{S1} \bmod Y$. Samalla tavoin osapuoli 2 muodostaa osapuolen 1 julkisen luvun ja oman salaisen luvun avulla avaimen $K = P1^{S2} \bmod Y$. Lopputuloksena molemmilla on siis sama avain K, jota ei kuitenkaan ole lähetetty avoimen kanavan yli. Salakuuntelijalla voi olla hallussaan muut luvut, mutta avainta K hänellä ei ole. Periaatteessa taitavan salakuuntelijan olisi silti helppo laskea K. Diffie-Hellman protokollan jakojäännökseen eli moduloon perustuvan laskennan käänteinen suoritus eli diskreetti logaritmi on kuitenkin tämän päivän menetelmin hyvin hankalaa.

Edeltävä esimerkki voidaan esittää vielä oikeilla luvuilla. Osapuolet 1 ja 2 sopivat yhteisestä alkuluvusta Y = 23 sekä primitiivisestä alkiosta g = 5. Osapuolen 1 salainen kokonaisluku S1 = 6 ja osapuolen 2 salainen kokonaisluku S2 = 15.

Osapuolen 1 julkinen luku on tällöin $P1 = g^{S1} \bmod Y$ eli $5^6 \bmod 23 = 15625 \bmod 23 = 8$. Osapuolella 2 vastaavasti $P2 = g^{S2} \bmod Y$ eli $5^{15} \bmod 23 = 30517578125 \bmod 23 = 19$. Osapuoli 1 lähettää siis osapuolelle 2 luvun 8 ja osapuoli 2 osapuolelle 1 luvun 19.

Osapuoli 1 laskee salaisen avaimen $K = P2^{S1} \bmod Y$ eli $19^6 \bmod 23 = 47045881 \bmod 23 = 2$. Osapuoli 2 laskee myös avaimen $K = P1^{S2} \bmod Y$ eli $8^{15} \bmod 23 =$

35184372088832 mod 23 = 2. Kumpikin osapuoli saa siis saman tuloksen eli avain K = 2. Oikeissa toteutuksissa luvut ovat tietysti paljon suurempia satunnaislukuja, joita osapuolet eivät itse valitse.

Diffie-Hellman menetelmän suurin ongelma tietoturvan kannalta on niin sanottu man-in-the-middle -hyökkäys, eli nimensä mukaisesti avaimenvaihtotapahtuman keskellä tiedonsiirtoon puuttuva henkilö, joka sieppaakin toisen osapuolen lähettämän luvun ja välittää toiselle osapuolelle oman lukunsa. Näin nousee esiin Diffie-Hellman avainten-vaihtoprotokollan keskeinen ongelma, eli osapuolia ei voida todentaa ja varmistua siitä että luku on todella peräisin luotetulta osapuolelta. [4, s. 117.]

3.4.2 Tiivisteet

Tiivisteillä voidaan toteuttaa tietoturvan eheyden periaatetta, eli varmistua siitä, että tallennettu tai siirretty tieto on säilynyt muuttumattomana. Tiiviste (hash) on yksisuuntainen funktio, joka rakentaa sille syötetystä bittijoukosta kuten tiedostosta tai sähköpostiviestistä pituudeltaan vakion bittijonon eli tiivistearvon. Kyseisestä arvosta ei voida päätellä alkuperäistä syötettä. Yleisesti käytössä oleva tiivistefunktio on SHA1 (Secure Hash Algorithm 1) jota käytetään PGP:ssä ja SSH:ssa. Tiiviste on myös bittijoukon sormenjälki (fingerprint) eli se yksilöi sille syötetyn bittijoukon. [4, s. 122.]

3.5 Salausmenetelmien sovelluksia

Salausmenetelmien hyödyntämiseksi on onneksi kehitetty käytännön sovelluksia, jotka automatisoivat avainten hallintaan ja salaukseen liittyvät toimenpiteet. Seuraavaksi on listattu niistä muutamia yksittäisen käyttäjän kannalta keskeisimpiä tietojen käsittelyyn, säilytykseen, siirtoon ja viestintään liittyen. Kustakin sovellusalueesta on olemassa sekä kaupallisia että avoimeen lähdekoodiin perustuvia ohjelmistoratkaisuja.

3.5.1 Digitaalinen allekirjoitus

Digitaalisella allekirjoituksella voidaan varmistaa viestin tai asiakirjan eheys, eli sen muuttumattomuus. Tästä on hyötyä sekä lähettäjän tai tekijän että vastaanottajan tai kohderyhmän kannalta. Samalla virheellisen tai väärennetyn tiedon julkaisu toisen henkilön nimissä estyy eikä alkuperäistä sanomaa voi ylipäätään kukaan ulkopuolinen

muuttaa. Eheyden lisäksi toteutuu siis kiistämättömyyden periaate eli todistus asiakirjan lähettäjästä tai tekijästä samalla tavoin kuin sinetti paperidokumentissa. Pelkästään näistä seikoista voidaan päätellä, että digitaalisen allekirjoituksen tulisi olla pikemminkin sääntö kuin poikkeus viestien ja dokumenttien vaihdoissa ja julkaisuissa. Digitaalista allekirjoitusta voidaan käytännössä hyödyntää esimerkiksi PGP-ohjelmiston avulla.

3.5.2 Varmenteet eli sertifikaatit

Varmenteet ovat todistuksia tiedon esittäjän identiteetistä tai tiedon oikeasta alkuperästä, koska niiden avulla salaukseen käytettävän julkisen avaimen voidaan todistaa kuuluvan tietylle taholle. Varmenne on aina luotettavan tahon eli sertifikaatin varmentajan (CA, Certificate Authority) digitaalisella allekirjoituksella oikeaksi ja aidoksi todistama. Varmenne sisältää julkisen avaimen lisäksi yleensä ainakin sen haltijan nimitiedot, myöntämispäivämäärän ja voimassaoloajan sekä sarjanumeron. Varmenteet voidaan luokitella käyttötarkoitusten mukaan. Esimerkkejä ovat henkilövarmenne joka yhdistää henkilön julkisen avaimen ja sen haltijan, sekä palvelinvarmenne, jonka avulla käyttäjä voi varmistua käyttämänsä palvelimen ja palvelun aitoudesta.

3.5.3 SSH ja SFTP

SSH (Secure Shell) kehitettiin suojaamattoman Telnet-yhteyden korvaajaksi. Se muodostaa salatun pääteyhteyden kahden tietokoneen välille. Käyttäjän tunnistus ja siirrettävä tieto salataan julkisen avaimen menetelmällä. Salattu tiedonsiirtoprotokolla eli SFTP (Secure File Transfer Protocol) on tavallisen suojaamattoman FTP-yhteyden salattu muoto ja SSH-protokollan laajennus.

3.5.4 SSL

SSL (Secure Sockets Layer) -protokollan avulla muodostetaan salattu yhteys web-selaimen ja web-palvelimen välille arkaluontoisten tietojen välittämiseksi. SSL koostuu kahdesta komponentista, tietuekerroksesta ja kättelykerroksesta. Se perustuu julkisen avaimen menetelmään. Palvelimelle lähetetään kertakäyttöinen avain joka on salattu palvelimen julkisella avaimella. Palvelin purkaa salauksen salaisella avaimellaan. Tällöin saadaan kertakäyttöinen avain, joka on käytössä yhden työaseman ja palvelimen välisen istunnon ajan.

3.5.5 S/MIME

Sähköpostiviestien välitykseen käytetyn MIME (Multipurpose Internet Mail Extension) -protokollan salausta tukeva versio eli S/MIME (Secure Multipurpose Internet Mail Extension) perustuu julkisen avaimen salausmenetelmään ja X.509-varmenteiden käyttöön. MIME määrittelee viestien ominaisuudet eri viestijärjestelmien välille sopiviksi.

3.5.6 Kiintolevyn salaus

Tietokoneen tai pelkästään siihen tallennetun tiedon päätyessä vääriin käsiin, ovat yksittäiset suojatut tai salatut tiedot vaarassa paljastua. Tällöin ei siis välttämättä ole hyötyä edes siitä, että yksittäiset tiedostot kuten tärkeät sähköpostiviestit on salattu. Tärkeää olisi myös salata koko kiintolevy tai mahdollinen muu massamuisti, jolloin tietosisältöön on ulkopuolisen jo erittäin hankala päästä käsiksi. Esimerkiksi Windows-ympäristössä kokonaisen kiintolevyn, ulkoisen massamuistin tai vaikkapa muistitikun salaaminen on mahdollista BitLocker-salausohjelmistolla, joka käyttää salaukseen vahvaa 128-bittistä AES-algoritmia.

3.5.7 PGP

PGP (Pretty Good Privacy) tarjoaa nimensä mukaisesti varsin hyvää yksityisyyttä. Sillä voidaan varmistaa tiedon luottamuksellisuus. Se on epäsymmetrisen eli julkisen avaimen että symmetrisen eli salaisen avaimen menetelmät yhdistävä ohjelmisto, joka soveltuu erityisesti sähköpostiviestien salaamiseen. Sitä voidaan käyttää myös muiden tiedostojen salaukseen, ja digitaaliseen allekirjoitukseen eli vastata todentamisesta. Lisäksi se soveltuu avainten hallintaan. Salausmenetelmien hyödyntäjille se onkin ehkä merkittävin ja monipuolisin yksittäinen ohjelmisto niin henkilökohtaiseen käyttöön kuin vaativampienkin yritys- tai viranomaistahojen tarpeisiin. PGP:n monikäyttöisyyden vuoksi perehdynkin tarkemmin juuri siihen perustuviin ohjelmistoihin ja niiden ominaisuuksiin.

4 Turvallinen sähköpostiviestintä ja tietojen säilytys OpenPGP-salausohjelmiston avulla

4.1 Sähköpostin salauksen tarpeellisuus

Yksittäisen tietoverkon käyttäjän kannalta ehkä merkittävin salausmenetelmien käytön osa-alue on sähköpostiviestintä ja siihen liittyvien asiakirjojen säilytys. Internetissä kulkee vähintään satoja miljoonia sähköpostiviestejä päivittäin, mutta viestintä kokonaisuudessaan tai siihen liittyvät asiakirjat eivät yleensä ole salausmenetelmin suojattuja, toisin kuin esimerkiksi yksittäiset web-pohjaiset pankki-, kauppa- tai viranomaispalvelut.

Sähköpostia voidaan oikeastaan verrata perinteiseen postikorttiin – sillä ei ole kirjeen tapaan sisältöä suojaavaa kuorta, vaan viesti voi olla pääosan kulkureitistään avoin niin sähköisten jakelijoiden kuin kenties muidenkin sivullisten silmäiltäväksi. Tämäkin voi tuntua vähäpätöiseltä asialta, etenkin jos miettii sähköpostiviestien määrää; äkkiseltään voisi kuvitella todennäköisyyden melko pieneksi, että miljoonien viestien joukosta joku tarkkailisi juuri omien viestien sisältöä tai lähettäjä- ja vastaanottajatietoja. Nykyisen teknologian myötä on kuitenkin jopa varsin systemaattinen ja laaja-alainen tietojen keruu teknisesti mahdollinen. Yksi esimerkki tällaisesta on Yhdysvaltojen ja kumppanien perustama ECHELON-signaalientiedustelujärjestelmä, joka pystyy valvomaan maailmanlaajuista tietoliikennettä, muiden muassa puheluita ja sähköpostiviestejä.

Pelkästään näitä taustoja vasten kannattaa tietoturvaa ja yksityisyyttä arvostavan, tai liike- tai muussa toiminnassaan salaista viestintää tarvitsevan tietoverkon käyttäjän, ainakin pyrkiä mahdollisimman turvalliseen viestinnän tasoon, lähettää viestit postikortin sijaan suljetussa kirjekuoressa. Asia tulee siis viestinnän osapuolten huomioida useimmiten joko täysin erillisin sähköpostiratkaisuin, kuten yhteisen, salattuun yhteyskanavaan sidotun viestipalvelimen avulla, tai mahdollisesti muulla tavoin keskenään sovituin menetelmin ja käytännöin. On kuitenkin saatavilla monissa tapauksissa sulavammin arkisiin työvälineisiin ja -menetelmiin sekä sähköpostiohjelmistoihin sopivia salausratkaisuja, joita voidaan käyttää hankalampien erityisratkaisujen sijaan. Siitä huolimatta asiaa ei ole aina nykypäivänäkään huomioitu edes yritystasolla, tavallisista käyttäjistä puhumattakaan. Viime kädessä jokaisen tulee tietysti itse määrittää omiin tarpeisiin sopiva ja riittävä salauksen taso suhteessa mahdollisimman hyvään tietoturvaan.

Joka tapauksessa salausmenetelmiä voitaisiin käyttää huomattavasti nykyistä yleisemminkin, kunhan tilanteeseen sopiva ohjelmisto ja halua sen käyttöön löytyy. Ohjelmistoratkaisuista parhaasta ja monipuolisimmasta päästä ovat PGP:hen perustuvat ohjelmistot, joiden avulla voidaan salata sähköpostiviestit ja tiedostot sekä digitaalisesti allekirjoittaa viestit tai muut niihin liittyvät dokumentit. Voidaanpa joitain versioita käyttää internet-puheluidenkin salaukseen.

4.2 PGP-salausohjelmistot

PGP on Phil Zimmermanin kehittämä salausohjelmisto, jonka ensimmäinen versio julkaistiin 1991. PGP yhdisti eri salaustekniikat yhteen helppokäyttöiseen ohjelmistoon, jonka ensimmäiset versiot olivat lisäksi ilmaisia käyttää. Sen jälkeen alkuperäisen PGP:n versiot ovat muuttuneet kaupallisiksi tai osittain kaupallisiksi. PGP:n kehitystä ovat alusta alkaen leimanneet siihen liittyneet patenttikiistat ja käyttörajoitteet. Osa versioista on ollut käytettävissä vain Yhdysvalloissa, osa sen ulkopuolella. Sittemmin on kuitenkin ilmestynyt muitakin PGP:hen perustuvia ja sen kanssa yhteensopivia ohjelmistoja, joten nykyisin tarjolla on lukuisia PGP-ohjelmistoja ja niiden eri versioita. Alkuperäinen PGP on nykyisin kaupallinen ohjelmisto, mutta avoimen OpenPGP-standardin mukaiset ohjelmistot kuten GnuPG (GPG, GNU Privacy Guard) ovat käyttäjälle ilmaisia. Ohjelmistojen ominaisuudet vaihtelevat ohjelmistopaketista ja versiosta riippuen. Nykyisissä PGP-ohjelmistoissa käytössä olevia salausalgoritmeja ovat esimerkiksi SHA1 allekirjoituksiin, AES, 3DES ja IDEA salaukseen, RSA salausavainten luomiseen ja Diffie-Hellman salausavainten salaamiseen. Tässä työssä käytän PGP-yhteensopivan GnuPG:n Linux-versiota sekä sen Gpg4win-nimistä Windows-versiota, koska ne ovat ilmaisia vaihtoehtoja Windows- ja Linux-ympäristöihin.

4.3 PGP-peruskäsitteet

4.3.1 Julkinen, salainen ja istuntoavain

Julkisen ja salaisen avaimen peruskäsitteet kuvattiin jo aiemmin. Suurten lukujen vuoksi julkisen avaimen menetelmien laskutoimitukset ovat raskaita ja hitaita verrattuna pienempiä yksiköitä käsitteleviin salaisen avaimen menetelmiin. Sen vuoksi käytännön julkisen avaimen menetelmät – kuten PGP – käyttävät astetta kehittyneempää istuntoavaimeen perustuvaa menetelmää. Satunnainen, versiosta riippuen esimerkiksi 128-

bittinen IDEA-istuntoavain luodaan erikseen joka kerta, kun PGP:n julkisen avaimen menetelmään perustuvaa viestin salausta käytetään. Se onkin ensimmäinen vaihe viestin salauksessa PGP:llä. Tämän jälkeen PGP käyttää esimerkiksi AES- tai vanhemmissa versioissa IDEA-algoritmia itse viestin salaukseen istuntoavaimen avulla. Seuraavassa vaiheessa istuntoavain salataan vastaanottajan julkisella avaimella RSA-algortmia käyttäen. Lopuksi salattu viesti ja salattu istuntoavain kääritään yhteen viestin lähetystä varten. (Garfinkel, s.12)

4.3.2 Avainsertifikaatit

PGP säilyttää julkiset avaimet avainsertifikaatissa, joka sisältää julkisen avaimen, avaimen luojan tunnistetiedot kuten nimen ja sähköpostiosoitteen, avaimen luontipäivämäärän. Siinä voi myös olla avaimen todenperäisyyden osoittavien henkilöiden digitaaliset allekirjoitukset.

4.3.3 Avainrenkaat

Avainsertifikaatit eli julkiset avaimet kerätään avainrenkaaksi kutsuttuun tiedostoon. Se on erillisiä tiedostoja tehokkaampi vaihtoehto, koska avainten haku on nopeampaa. Asia korostuu luonnollisesti silloin, kun avaimia on kymmeniä tai satoja. Yleensä PGP-ohjelmiston käyttäjällä on kaksi avainrengastiedostoa. Toinen sisältää käyttäjän salaiset avaimet, ja toisessa on käyttäjän tallentamat julkiset avaimet esimerkiksi ystäviltä tai muilta yhteydenpidon osapuolilta. Jos osapuolia on paljon, voi olla järkevää käyttää kahta tai useampaa julkisen avaimen avainrengasta.

4.3.4 Salalauseet

Kun julkisen ja salaisen parin muodostama avainpari luodaan, PGP:lle syötetään salalause. PGP:n salalauseella on useampi tehtävä, joista tärkein on salaisen avaimen avainrenkaassa olevan salaisen avaimen purku. Salalause siis turvaa PGP:llä salatun viestin, koska ainoastaan salalauseen tunteva voi käyttää salaista avainta. Salalause voi olla eri jokaiselle salaiselle avaimelle jos niitä on useampia, tai kaikki voivat käyttää samaa salalausetta. Kun vastaanotettu viesti puretaan, PGP pyytää salalausetta, jolla se purkaa viestin salaukseen käytettyyn julkiseen avaimeen liittyvän salaisen avaimen, jota sen jälkeen voidaan käyttää salatun viestin purkamiseen. Myös viestin digitaali-

seen allekirjoitukseen tarvitaan salalausetta. PGP purkaa sillä taas yksityisen avaimen jolla viesti voidaan allekirjoittaa. Edelleen, kun PGP:llä halutaan salata tiedosto, tarvitaan sitä varten salalause. Se voi olla sama kuin salaisen avaimen suojana käytetty mutta yhtä lailla se voi olla eri.

Salalausetta voidaan verrata muihin tietokonejärjestelmien pääsynvalvonnassa käytettyihin salasanoihin, koska se valvoo pääsyä joihinkin PGP-sovelluksen toimintoihin. Mutta merkittäviä erojakin on. PGP ei vertaa salalausetta kiintolevylle tallennettuun salalauseeseen, vaan käyttää sitä vain salaukseen tai salauksen purkamiseen. Lisäksi salalauseen pituutta ei ole rajoitettu toisin kuin salasanojen yleensä, joten sen arvaaminen tai murtaminen on huomattavasti vaikeampaa.

Salalauseen merkitys salaisen avaimen suojana on hyvin helppoa käsittää, kun kuvitellaan tilanne, jossa henkilön tietokone varastetaan. Jos salainen avain ei ole salattu, tietokoneen haltuunsa saanut ulkopuolinen pystyy lukemaan kaikki salatut viestit ja lähettämään allekirjoitettuja viestejä. Lähes vastaava tilanne esiintyy paljon yleisemminkin, kun samalla tietokoneella on useampi käyttäjä. Ilman omia salalauseita pystyisi jälleen kuka tahansa lukemaan toisen salattuja viestejä tai allekirjoittamaan viestejä. (Garfinkel, s.16)

4.3.5 PGP:n digitaalinen allekirjoitus

Koko asiakirjan salaus ei välttämättä ole aina tarpeen. Tällöinkin saatetaan haluta varmistaa asiakirjan säilyminen muuttumattomana, eli estää sisällön ja alkuperätietojen muokkaus ulkopuolisilta. Yhtä lailla halutaan evätä vilpillisten viestien lähetys omissa tai yrityksen nimissä. Ja usein täytyy myös todistaa asiakirjan aitous ja alkuperäinen tekijä, ilman että kaikkien siihen tutustuvien tulisi sen alkuperä erikseen kysyä ja varmistaa. Ilman digitaalista allekirjoitusta aitoutta ei voitaisi mitenkään todistaa. Se on siis sähköisen asiakirjan sinetti. Kuitenkaan pelkkä digitaalisen allekirjoituksen olemassa olo ei takaa mitään. Se voi olla väärennetty siinä missä perinteinenkin allekirjoitus. Digitaalisen allekirjoituksen aitous voidaan kuitenkin tarkistaa matemaattisesti.

Digitaalisen allekirjoituksen käytännön sovelluskohteita ovat esimerkiksi sähköpostiviestin sisällön ja lähettäjän todennus, sähköpostin tai uutisryhmäviestin väärennöksen esto, hinnastojen tai hintatietojen aitous, tiedotteiden, sääntöjen, todistusten tai muiden virallisten asiakirjojen oikeaksi todistaminen. Oikeastaan sen pitäisikin sisältyä jokai-

seen asiakirjaan ja sähköpostiviestiin. Sen käyttöä ovat kuitenkin rajoittaneet hankalat ohjelmistot sekä allekirjoituksissa käytettyjen algoritmien patenttiasiat.

PGP luo digitaalisen allekirjoituksen käsittelemällä viestin tai asiakirjan ensin tiiviste- eli hash-funktiolla tuottaen 128-bittisen luvun. Tämä matemaattinen funktio suodattaa siis koko asiakirjan yhdeksi suureksi luvuksi. Kyseinen luku allekirjoitetaan sen jälkeen kirjoittajan yksityisellä avaimella, jonka tuloksena syntyy PGP-allekirjoituslohko asiakirjan loppuun osoittamaan tekijän ja kirjoituksen aitouden. Viestin tai asiakirjan vastaanottajan PGP ajaa saman tiivistefunktion viestin sisältöosuudelle. Sen jälkeen PGP varmistaa viestin perässä olevan allekirjoituslohkon lähettäjän julkisella avaimella. Lopuksi PGP tarkistaa viestisisällön muuttumattomuuden vertaamalla lähetetystä ja vastaanotetusta viestistä lasketut tiivisteet. Jos ne ovat samat, tiedosto ei ole muuttunut allekirjoituksen jälkeen. Jos niissä on eroa, PGP ilmoittaa tiedoston muuttuneen. Näin ollen mikä hyvänsä tahallinen tai tahaton, suuri tai pieni muutos asiakirjan sisältöön vaikuttaa digitaaliseen allekirjoitukseen. Se ei kuitenkaan kerro, mikä tai kuinka suuri osa sisällöstä on muuttunut. PGP:n digitaalista allekirjoitusta on miltei mahdoton väärentää sen paremmin toisesta dokumentista kopioidun allekirjoituksen kuin asiakirjasisällön allekirjoitusvaiheen muutoksillakaan.

4.3.6 Avainsertifikaattien allekirjoitukset

Yksi julkisen avaimen salausmenetelmien – muiden muassa PGP:n – ongelma on itse julkisten avainten jakelutavat. Lähettäjällä pitää olla vastaanottajan julkinen avain lähettääkseen tälle salatun viestin. Niin ikään vastaanottajalla pitää olla lähettäjän julkinen avain todentaakseen viestin lähettäjän allekirjoituksen. Näin ollen olisi kätevää, jos kaikkien julkiset avaimet olisivat jossakin saatavilla osoitekirjan tai puhelinluettelon tapaan. Viestin lähettäjä voisi poimia vastaanottajan julkisen avaimen luettelosta hänelle viestiä lähettäessään. Tähän onkin olemassa ratkaisu, PGP-avainpalvelin, joka toimii siis avainluettelona. PGP-avainpalvelimet eivät kuitenkaan ratkaise avaimen aitouteen liittyvää ongelmaa. Ei pystytä varmistamaan, että luettelossa esiintyvä julkinen avain todella kuuluu henkilölle, jolle sen oletetaan kuuluvan. Jos joku onnistuukin vaihtamaan toisen henkilön avaimen tilalle omansa, voi hän myös onnistua purkamaan ja lukemaan alkuperäiselle henkilölle osoitetun salatun viestin. Edelleen hän voi salata viestin uudelleen alunperin tarkoitetun vastaanottajan julkisella avaimella ja näin viestin todelliset lähettäjä ja vastaanottaja osapuolet eivät tiedä välissä olleesta kolmannesta osapuolesta mitään. PGP ei varsinaisesti ratkaise kyseistä avaintenjaon ongelmaa, mutta hel-

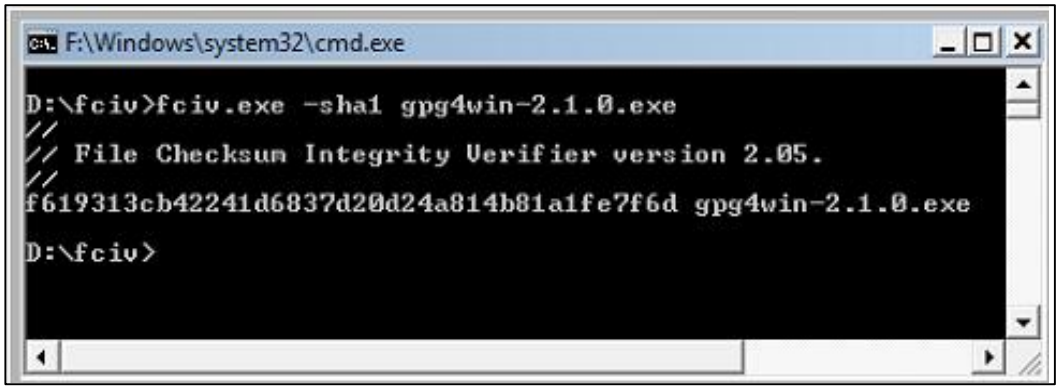
pottaa kuitenkin tilannetta sallimalla ihmisten allekirjoittaa toistensa avainsertifikaatteja. Allekirjoittaja totuudenmukaisesti vahvistaa avaimen aitouden ja sen kuulumisen tietylle henkilölle. Niistä PGP muodostaa niin sanotun web-luottamusverkoston, joka siis rakentuu vahvistettujen julkisten avainten kirjastosta. Se ei välttämättä ole yhtä kätevä kuin yksittäinen keskitetty julkisten avainten rekisteri, mutta toisaalta useampien käyttäjien keskinäisiä avainvahvistuksia on vaikea olla hyväksymättä.

4.4 GnuPG

GnuPG on siis avoimen lähdekoodin OpenPGP-standardiin perustuva PGP-ohjelmisto. Sen virallinen Windows-ympäristöön kehitetty versio on Gpg4win, jonka luontia on tukenut muun muassa Saksan liittovaltion tietoturvatoimisto. Gpg4win-ohjelmistossa on PGP-standardin lisäksi tuki S/MIME (X.509) -standardille. GnuPG itsessään on Linux-ympäristöihin toteutettu täysi vastine PGP-ohjelmistolle. GnuPG-ohjelmistot on tarkoitettu tiedostojen ja sähköpostiviestien salaukseen, avaintenhallintaan sekä digitaalisten allekirjoitusten muodostamiseen. Ne eivät käytä patentoituja algoritmeja, ovat useimpien alkuperäisten PGP-versioiden kanssa yhteensopivia, tukevat avainpalvelinten käyttöä ja tarjoavat jopa joitakin tietoturvan parannuksia sekä toiminnallisia laajennuksia alkuperäiseen PGP-ohjelmistoon nähden. GnuPG:ssä käytetään muun muassa DSA-, RSA-, AES-, 3DES-, Blowfish-, MD5- ja SHA-1 -algoritmeja.

4.5 Gpg4win Windows-ohjelman käyttöönotto ja ominaisuudet

GnuPG:n Windows-ympäristöön kehitetty ohjelmisto on nimeltään Gpg4win. Sen asennuspaketti voidaan ladata ohjelmiston omalta web-sivustolta (http://www.gpg4win.org). Ennen ohjelmistopaketin asennusta on hyvä varmistaa ladatun tiedoston aitous. Mikäli aiempaa GnuPG-versiota ei ole asennettu, tulee laskea tiedoston tiiviste eli tarkistussumma SHA-1-algoritmin avulla. Tämän jälkeen eheys varmistetaan vertaamalla saatua arvoa ohjelmiston lataussivustolla ilmoitettuun tiedoston SHA-1-tarkistussummaan. Jos ne täsmäävät, voidaan tiedoston alkuperään luottaa ja ohjelmiston asennus käynnistää. Windows-ympräistössä tarkistussumman voi laskea esimerkiksi Microsoftin File Checksum Integrity Verifier -ohjelmalla (Kuva 7.).



Kuva 7. SHA-1-tarkistussumman laskenta Windows-ympäristössä.

Gpg4win-ohjelmiston version 2.1.0 täydelliseen asennuspakettiin kuuluvat: GnuPG salausohjelmisto, Kleopatra-avaintenhallintaohjelmisto, GNU-yksityisyysavustaja ja vaihtoehtoinen avaintenhallinnan laajennus, GnuPG Outlook -laajennus sähköpostiviestien salaukseen Microsoft Outlook 2003- ja 2007 -ohjelmistoilla, GnuPG:n shell-laajennus komentorivikäyttöön tai Windows Explorer -laajennus sekä Claws-sähköpostiohjelmisto GnuPG käyttöön. Gpg4win-ohjelman käytön kannalta olennaisinta on se, että varsinaiseen sähköpostikäyttöön vaaditaan myös sen kanssa yhteensopiva sähköpostiohjelma.

Gpg4win perustuu muiden salausohjelmistojen tapaan avainten käyttöön. Tarkemmin ottaen sen toiminta pohjautuu julkisen avaimen salausmenetelmän periaatteeseen, jossa salainen avain on ehdottoman salainen ja julkinen avain mahdollisimman julkinen. Salainen avain purkaa viestin salauksen, julkinen avain suorittaa salauksen. Siinä missä salaisen avaimen menetelmä perustuu yhteiseen salaisuuteen, vaikkapa salaiseen postilaatikkoon johon kummallakin viestinnän osapuolella on sama avain, julkisen avaimen menetelmässä laatikkoon voi kuka tahansa pudottaa viestin siihen liittyvällä julkisella avaimella, mutta auki laatikon saa ainoastaan sen yksityisen avaimen haltija. Vastaavasti sähköpostiviestin salaus tapahtuu vastaanottajan julkisella avaimella, jonka jälkeen viestin saa avatuksi vain ja ainoastaan kyseinen vastaanottaja salaisella avaimellaan. Eli mikä parasta, salaista avainta tai mitään muutakaan salaista ei koskaan tarvitse vaihtaa osapuolten kesken. Salainen avain on vain ja ainoastaan omassa avainrenkaassa ja muistissa. Muun muassa tätä tarkoitusta palvelee Gpg4Win-ohjelmisto.

Yksityinen avain on siis keskeinen komponentti epäsymmetrisessä eli julkisen avaimen salausmenetelmässä, joten avaimen turvallisuus on erityisen tärkeässä roolissa koko salausjärjestelmää koskien. Teknisesti avain on vain yksittäinen tiedosto sen haltijan tietokoneella. Tiedosto on suojattu pääsyoikeuksilla, joten muut käyttäjät eivät pysty lukemaan sitä tai kirjoittamaan siihen. Todellisen suojan avaintiedostolle tuo kuitenkin toinen taso eli salalause. Pääsyoikeudet eivät välttämättä pidättele järjestelmänvalvojia, viruksia tai haittaohjelmia, mutta salalause on tai sen pitäisi olla vain haltijansa muistissa oleva salainen lause, jota tarvitaan avaimen käyttöön. Helposti muistettavakin salalause on pelkkää yksittäistä sanaa niin paljon vaikeampi kokeilemalla murtaa, että se tarjoaa miltei täysin varman suojan. Toisaalta oikeaa kieliopillista lausetta lyhyempikin salalause voi olla erittäin vahva, jos se sisältää useita erilaisia merkkejä, kuten isoja ja pieniä kirjaimia, numeroita, erikoismerkkejä ja välilyöntejä. Ennen muuta on ehdottomasti vältettävä helposti arvattavia salalauseita. Sellaisia ovat esimerkiksi käyttäjätunnuksissa tai muuten jo käytössä olevat salasanat, julkiseen henkilötietoon kuten nimeen, osoitteeseen, syntymäaikaan tai muuhun vastaavaan tietoon liittyvät sanat ja lauseet, sanakirjan sanat, missä tahansa kielessä yleisesti esiintyvät sanat tai sanonnat sekä yksittäiset lyhyet sanat.

Julkisen avaimen menetelmä takaa siis melko varmasti sen, että salatun viestin voi avata ainoastaan sille osoitettu vastaanottaja. Siitä huolimatta se ei sellaisenaan todista viestin lähettäjästä mitään, joten tarvitaan myös todennus viestin lähettäjän henkilöllisyydestä. Niinpä jonkun pitää todistaa, että salaisen viestin lähettäjä todella on oikea. Molemmat toimenpiteet voidaan suorittaa Gpg4win-ohjelmistolla joko OpenPGP- tai S/MIME.menetelmällä. Kummatkin perustuvat julkisen avaimen menetelmään ja niiden tehtävä on tiedon salaus ja allekirjoitus. Vaikka menetelmissä on joitain merkittäviäkin eroja, ei kumpikaan tarjoa erityistä etua tai paremmuutta toiseen verrattuna. OpenPGP ja S/MIME ovat siis vaihtoehtoiset menetelmät, jotka molemmat täyttävät samat tehtävät ja turvallisuustavoitteet. Ne eivät ole yhteensopivat keskenään, mutta Gpg4win tarjoaa mahdollisuuden käyttää niitä rinnakkain.

Siinä missä oikean elämän henkilötodistuksen myöntää tietty viranomainen, joka edelleen on riippuvainen seuraavista viranomaisista ja viime kädessä lainsäätäjistä, toimii Gpg4win-ohjelmiston S/MIME vastaavankaltaisen luottamushierarkian mukaisesti. S/MIME-avaimen pitää olla valtuutetun tahon todistama ennen kuin sitä voidaan käyttää. Tämän tahon myöntämä X.509-standardin mukaisen varmenteen täytyy olla sitä

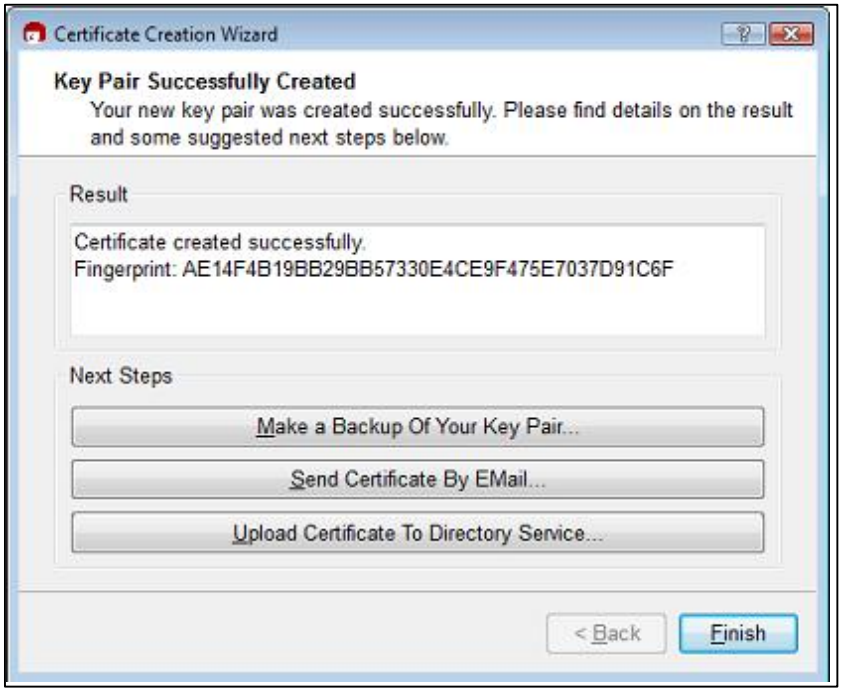
ylemmän tason organisaation valtuuttama ja niin edelleen, ylimmän tahon ollessa juurisertifikaatti.

Periaate eroaa siis aiemmin mainitusta OpenPGP:n web-luottamusverkostosta, joka puolestaan rakentuu internetin ja salausavainten käyttäjien välisten luottamussuhteiden pohjalta. Näin ollen OpenPGP on helpommin otettavissa käyttöön, koska sitä varten ei tarvita virallisen korkeamman tahon valtuutusta. Kumpaa tahansa menetelmää käyttääkin, on muistettava, että lähettäjän todentaminen on vähintäänkin yhtä tärkeää kuin itse viestin salaus.

4.5.1 OpenPGP-avainten luominen Gpg4win-ohjelmalla

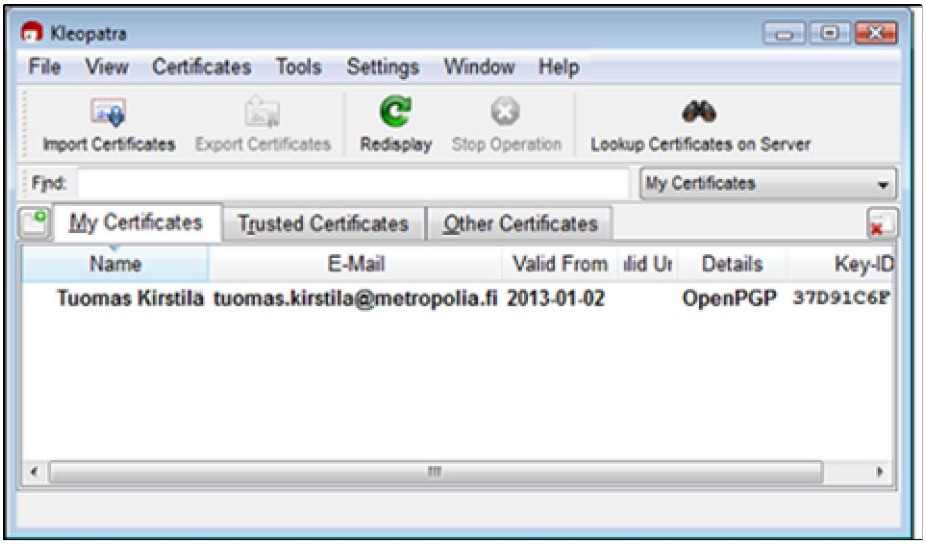
Gpg4win-ohjelmisto tarjoaa siis vaihtoehtoiset OpenPGP- ja S/MIME-pohjaiset metodit viestien salaukseen ja lähettäjän todentamiseen. Tämän työn käytännön testeissä käytän OpenPGP:tä, koska sen käyttöönotto ja kokeilu onnistuvat ilman virallisia varmenteita. Varmenteet eli oma julkinen ja salainen avain luodaan Gpg4win-täysasennuspakettiin kuuluvalla Kleopatra-varmenteenhallintaohjelmalla.

Uusi varmenne luodaan valitsemalla ensin varmenteen muoto OpenPGP- ja S/MIME-avainparin väliltä, joten tässä tapauksessa valitaan siis OpenPGP. Tämän jälkeen syötetään varmenteen haltijan nimi- ja sähköpostiosoitetiedot. Halutessaan voi myös määrittää tarkempia avaimen ominaisuuksia, kuten käytetty salausalgoritmi ja avainpituus sekä varmenteen käyttötarkoitus. Oletuksena nämä ovat 2048-bittinen RSA ja salaus, allekirjoitus sekä varmennus. Sitten syötetään oma salalause, jonka jälkeen avainten-parin luonti kestää hetken. Lopputuloksena tuotetaan ilmoituksen lisäksi varmenteen sormenjälki (engl. fingerprint), joka on yksilöllinen 40-bittinen heksadesimaaliljärjestelmän luku. Sen tarkoitus on sekä tunnistaa varmenteen yksilöllisyys että toimia kyseisen haltijan sormenjälkitunnisteena (Kuva 8.).



Kuva 8. Avainparin luomisen tuloksena näkyy sen haltijan sormenjälki.

Lopuksi tuore varmenne näkyy omien varmenteiden listalla (Kuva 9.).



Kuva 9. Omien varmenteiden näkymä.

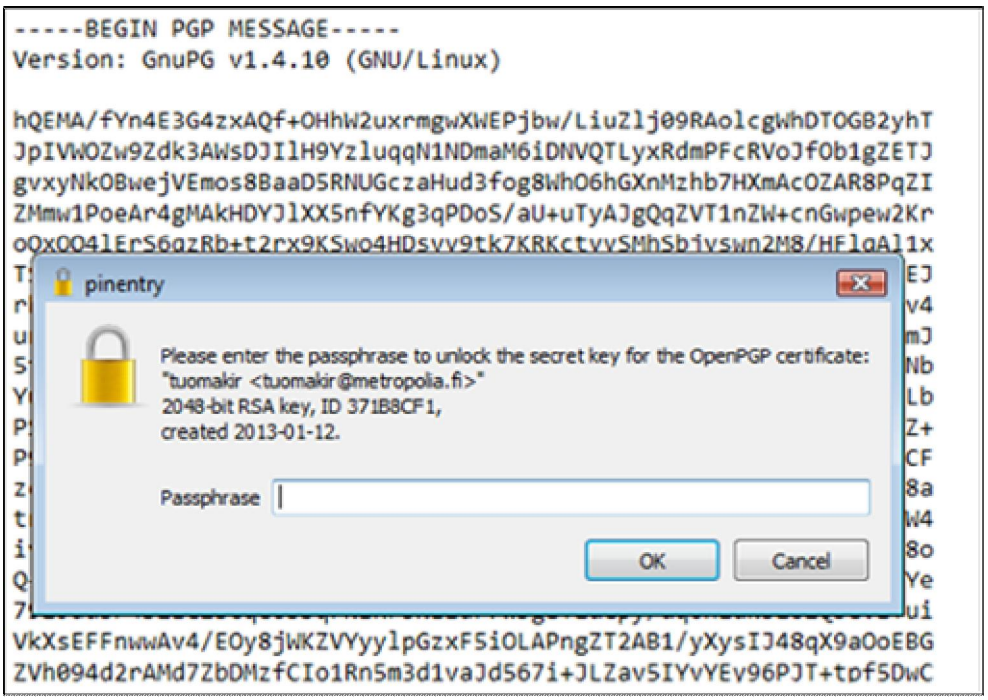
4.5.2 Julkisen avaimen jakelu sekä viestin salaus ja salauksen purkaminen

Salaisten viestien vaihtamiseksi oma julkinen avain pitää toimittaa viestintäkumppaneille, joiden vastaavasti pitää lähettää omat julkiset avaimensa. Avaimen toimituskanavia ovat esimerkiksi sähköposti, OpenPGP-sertifikaattipalvelin tai omat kotisivut. Avaimen pitää vain olla helposti jaeltavassa muodossa. Gpg4win-ohjelmistossa OpenPGP-avain voidaan viedä Kleopatra-avaintenhallintaohjelmalla .asc-päätteiseksi tiedostoksi, joka sisältää avaimen ASCII-muotoisena tekstinä. Tiedosto aukeaa millä tahansa tekstinmuokkausohjelmalla jolloin sen otsikkotiedot osoittavat sen julkiseksi avaimeksi (Kuva 10.).

Kuva 10. Julkinen avain.

Kyseinen .asc-tiedosto eli julkinen avain voidaan sen jälkeen lähettää sellaisenaan sähköpostin liitetiedostona vastaanottajalle, tai sen sisältö voidaan kopioida tekstieditorin kautta viestin sisällöksi. Näistä jälkimmäinen on varmempi tapa ja toimii aina. Liitetiedoston lähetys tai vastaanotto ei välttämättä toimi kaikissa sähköpostipalveluissa, mutta on toisaalta kätevämpi tapa.

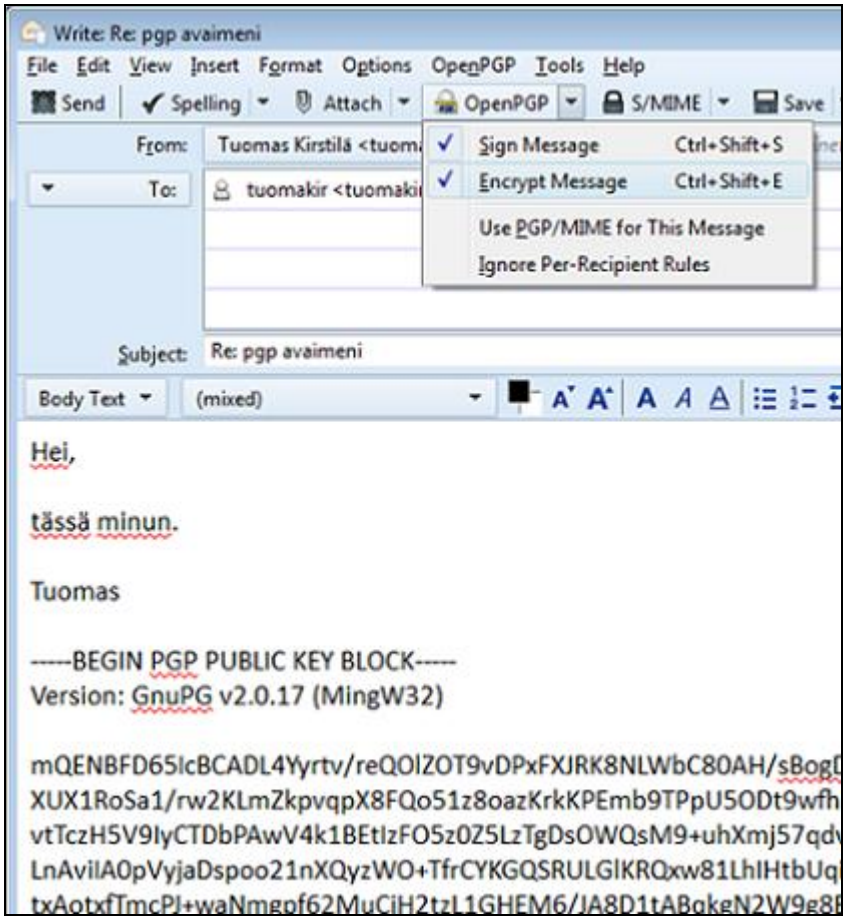
Ennen avaimen lähettämistä henkilölle, jonka kanssa salattu viestintä on tarkoitus aloittaa, voi Gpg4win-ohjelmalla harjoitella viestinvaihtoon liittyviä toimenpiteitä. Sen mahdollistaa ohjelmistoa varten kehitetty sähköpostirobotti, jolle oma julkinen avain lähetetään sähköpostitse. Robotti lähettää vastausviestin, jonka se on salannut juuri vastaanottamallaan julkisella avaimella (Kuva 11.).



Kuva 11. Harjoitusrobotin lähettämä salattu viesti.

Robotin lähettämän viestin pystyy avaamaan ainoastaan vastaanottaja yksityisellä avaimellaan. Tässä tapauksessa siis oma yksityinen avain avataan ensin siihen liittyvän salalauseen avulla, jonka jälkeen OpenPGP purkaa salauksen ja robotin lähettämä viesti paljastuu. Vastausviestin lisäksi robotti on lisännyt oman julkisen avaimensa viestiin. Se voidaan tallentaa mihin tahansa tekstimuotoiseen tiedostoon, josta se tuodaan Kleopatra-avaintenhallintaan. Näin avaintenhallintaan on tallennettu kyseisen vastaanottajan julkinen avain. Sen avulla voi lähettää robotille vastausviestin, jonka salaus hoituu juuri tallennetulla robotin julkisen avaimella. Näin avainten luonnin ja hallinnan sekä salatun viestin lähettämisen ja vastaanoton perusperiaatteet ovat tulleet tutuiksi, ja salattu viestiliikenne voidaan aloittaa myös todellisuudessa.

Gpg4win lisää sen kanssa yhteensopivaan sähköpostiohjelmaan OpenPG-ominaisuuden. Tämä tulee esiin viestin lähetysvaiheessa, jossa valitaan viestin salaus ja niin haluttaessa myös viestin allekirjoitus (Kuva 12.). Tämän jälkeen OpenPGP pyytää vielä valitsemaan vastaanottajan julkisen avaimen, jolla viesti salataan. Tässä tapauksessa syötetään myös salalause oman salaisen avaimen käyttämiseksi viestin allekirjoitukseen.



Kuva 12. Oman julkisen avaimen lähetys salattuna ja allekirjoitettuna viestinä.

Sen jälkeen salattu viesti allekirjoituksineen on muodostettu (Kuva 13.).

Kuva 13. Salattu viesti.

Purettu viesti näyttää samalta lähettäjällä sisältäen saateviestin ja sen alla lähettäjän julkisen avaimen. Viesti on lisäksi allekirjoitettu lähettäjän todentamiseksi (Kuva 14.).

Kuva 14. Viesti vastaanotettu ja salaus purettu.

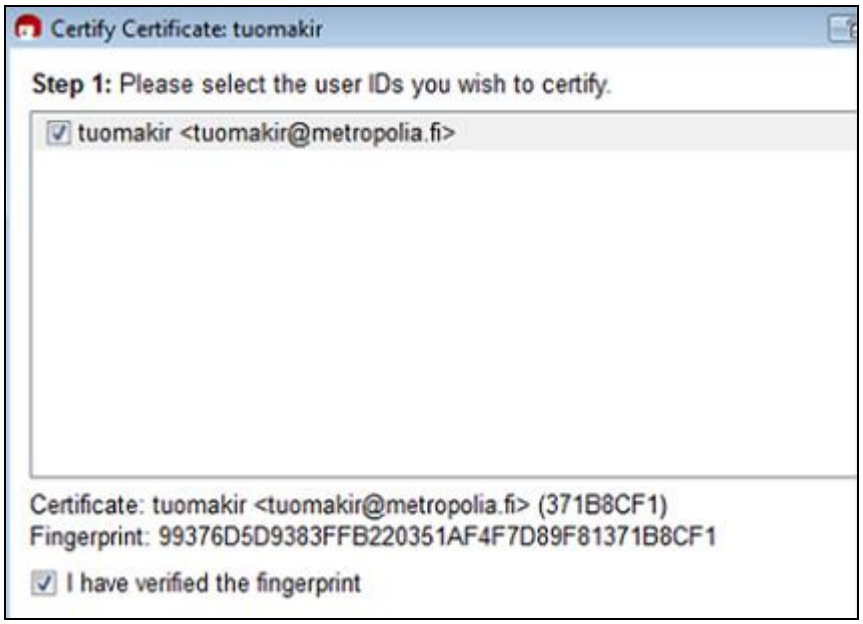
4.5.3 Varmenteiden todentaminen ja viestin digitaalinen allekirjoitus

Vaikka itse viesti olisikin salattu, on myös tärkeää saada varmistus lähettäjän aitoudesta. Muutoin salattukin viesti menettää merkityksensä. Gpg4win-ohjelmistossa tämä voidaan varmistaa Kleopatra-avaintenhallinnalla tutkimalla halutun osapuolen varmennetta ja siinä olevaa sormenjälkeä (engl. fingerprint) (Kuva 15.).

Kuva 15. Varmenteen allekirjoitus.

Jokaisella varmenteella on siis yksilöllinen tunniste, sormenjälki, joka yksilöi varmenteen ja sen omistajan. Viime kädessä se vaatii kuitenkin sormenjäljen varmistamista omistajaltaan, eli kyseisen tiedon vaihtamista muuta kautta, jolloin saatuja tietoja voidaan verrata keskenään ja varmistua sormenjäljen olevan aito. Kun tästä on saatu varmistus, voidaan kyseisen henkilön varmenne vahvistaa Kleopatralla ja allekirjoittaa oman salaisen avaimen avulla (Kuva 16.). Samassa yhteydessä vahvistettu varmenne voidaan toimittaa myös julkiseen OpenPGP-varmennepalveluun kaikkien saataville. Mitä useamman vahvistuksen jokin varmenne saa, sitä luotettavampana sitä voidaan pitää. Muodostuu niin sanottu luottamusverkko. Tällöin kuitenkin korostuu entisestään lähtökohta, jossa varmenteen vahvistaminen suoritetaan vasta sen jälkeen, kun sen aitoudesta on todella saatu varmuus. Muussa tapauksessa luottamusverkolle voi muodostua käänteinen merkitys.

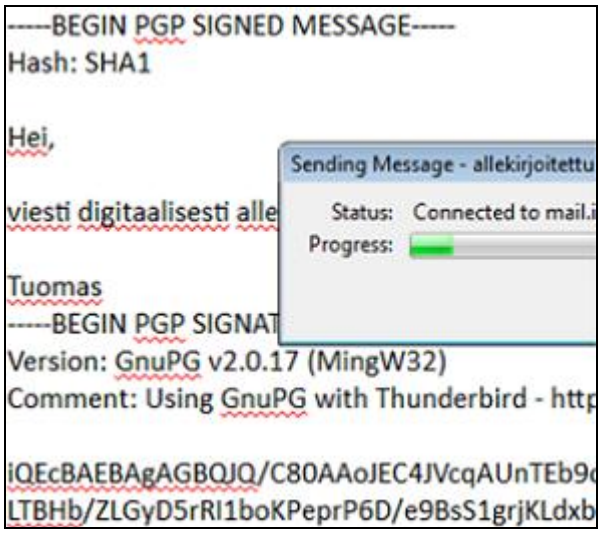
Kumppanuusverkostoon perustuvan varmenteiden vahvistamisen sijaan tai lisäksi saman asian voi ajaa kaupallinen tai viranomaisiin perustuva tietoturvallisuustaho. Luottamus ei tällöin perustu yksittäisten henkilöiden välisiin suoriin luottamussuhteisiin, vaan keskitettyyn varmenteita hallitsevaan ja luotettavana pidettyyn tahoon.



Kuva 16. Varmenteen vahvistaminen.

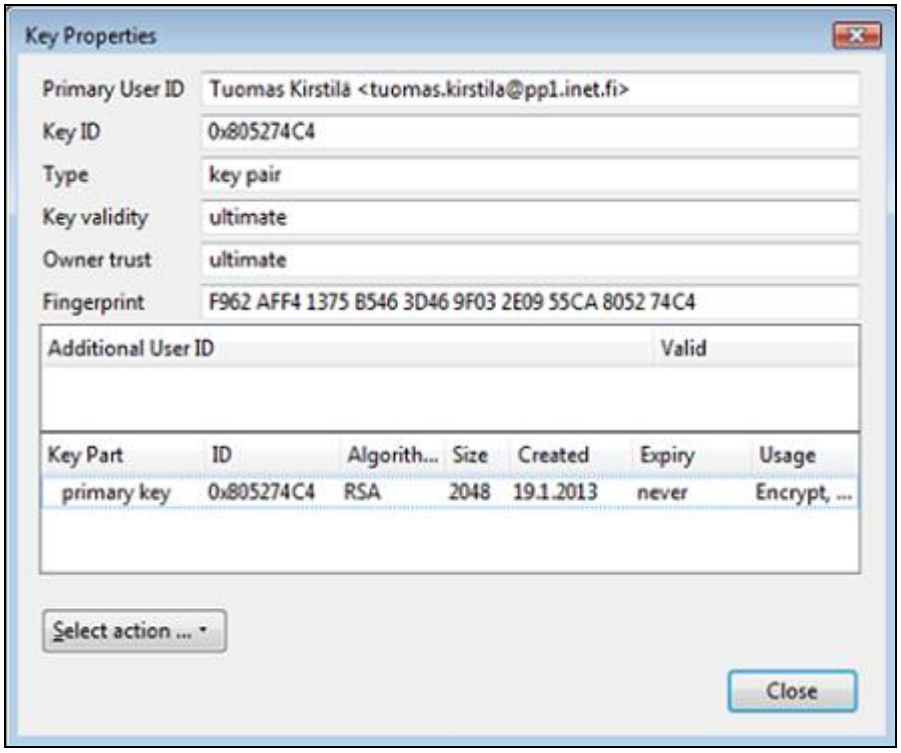
Gpg4win mahdollistaa siis sähköpostiviestin digitaalisen allekirjoituksen. Allekirjoitusta voidaan käyttää yhdessä salauksen kanssa, mutta se ei ole suoranaisesti riippuvainen salauksesta. Sitä voidaan käyttää silloinkin, kuin itse viestiä ei syystä tai toisesta ole

salattu, esimerkiksi silloin kun lähettäjällä ei ole vastaanottajan julkista avainta. Pelkkä allekirjoituskin on vastaanottajalle osoitus viestin lähettäjän ja asiakirjan alkuperästä ja eheydestä. Viestin vastaanottajan pitää kuitenkin jotain kautta saada lähettäjän julkinen OpenPGP-varmenne allekirjoituksen tarkistamiseksi. Viestin digitaalinen allekirjoitus valitaan viestin lähetysvaiheessa ja syötetään salalause omaa yksityistä avainta varten, joka muodostaa viestiin allekirjoituksen (Kuva 17.).



Kuva 17. Viestin digitaalinen allekirjoitus.

Vastaanottaja tarkistaa allekirjoituksen lähettäjän julkisella avaimella. Mikäli viestin eheys on säilynyt, allekirjoitus näkyy onnistuneesti. Jos viesti on tiedonsiirrossa muuttunut, tarkistus epäonnistuu. Se ei välttämättä merkitse viestin sisältöön kohdistunutta tarkoitusperäistä muokkausta ulkopuolisen toimesta, vaan voi johtua puhtaasti internetin luonteen mukaisesta siirron häiriötilanteesta. Joka tapauksessa se on signaali ottaa yhteyttä lähettäjään ja pyytää viesti uudelleen. Gpg4win-yhteensopivalla sähköpostiohjelmalla tarkistus voidaan suorittaa Kleopatraan tallennettujen julkisten avainten kanssa joko automaattisesti ohjelman toimesta tai manuaalisesti kunkin viestin kohdalla erikseen. Lisäksi voidaan tarkistaa allekirjoitukseen käytetyn varmenteen tiedot ja varmistaa että sormenjälki täsmää lähettäjän ilmoittamaan (Kuva 18).



Kuva 18. Lähettäjän julkisen varmenteen tiedot.

4.5.4 Sähköpostin liitetiedoston salaus

Liitetiedoston salaus ei suuresti eroa pelkän salatun viestin lähettämisestä. Niinpä viesti ja sen liitetiedosto voidaan kummatkin salata ja allekirjoittaa yhdessä ilman erillisiä toimenpiteitä. Viesti liitetiedostoineen salataan edelleen vastaanottajan julkisella avaimella. Salausvaiheessa valitaan lisäksi viestin salaustapa (Kuva 19.). Suositeltava on PGP/MIME-standardi, jolloin viestin liitteet ja teksti salataan yhdessä ja myös viestin erilaiset esitysmuodot kuten HTML ovat tuettuja. Toinen vaihtoehto on perinteinen ja toistaiseksi varmemmin eri sähköpostijärjestelmien välillä toimiva inline PGP, jossa viesti ja liite salataan erikseen. Mikäli käytössä oleva sähköpostiohjelmisto ei ole suoraan Gpg4win-yhteensopiva, voidaan liitetiedosto salata myös erikseen.

Kuva 19. Sähköpostiviestin salaaminen liitetiedostoineen.

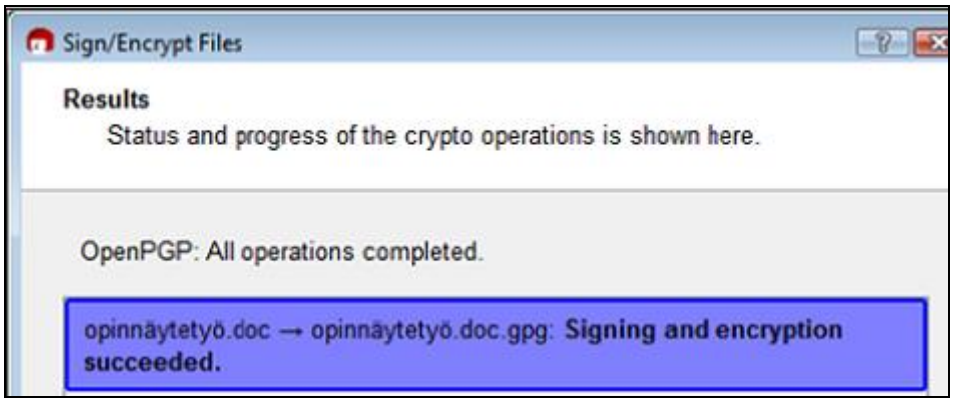
4.5.5 Tiedostojen salaus ja allekirjoitus

Sähköpostiviestien lisäksi Gpg4win-ohjelmalla voi salata mitä tahansa yksittäisiä tiedostoja viestin salauksesta tutulla periaatteella. Tiedosto salataan julkisella avaimella, minkä jälkeen vain salaisen avaimen haltija pystyy lukemaan sen. Näin estetään valtuuttamattomia henkilöitä näkemästä tiedostoa. Tiedosto allekirjoitetaan salaisella avaimella, jolla estetään siihen kohdistuvat muutokset muiden kuin tiedoston luojan ja omistajan toimesta. Allekirjoitus tarkistetaan tekijän julkisella avaimella.

Tiedoston salaus suoritetaan Kleopatra-ohjelmalla 64-bittisessä Windows käyttöjärjestelmässä (Kuva 20.). Valittu tiedosto voidaan salata ja samalla allekirjoittaa, tai suorittaa vain jompikumpi toimenpide. Näiden lisäksi tiedosto voidaan arkistoida. Tämän jälkeen valitaan oma julkinen avain tiedoston salaamiseksi ja edelleen allekirjoitetaan tiedosto omalla salaisella avaimella.

Kuva 20. Tiedoston salaus ja allekirjoitus.

Onnistunut prosessi tuottaa .gpg-päätteisen tiedoston (Kuva 21.).



Kuva 21. Salaus ja allekirjoitus valmis.

Tiedoston salauksen purku ja allekirjoituksen tarkistaminen ovat käänteiset toimenpiteet, jotka voidaan suorittaa Kleopatra-ohjelmalla (Kuva 22.)

Kuva 22. Salatun tiedoston avaaminen ja allekirjoituksen tarkistaminen.

Vertailun vuoksi yksittäinen tiedosto tai hakemisto voidaan salata myös Windows-käyttöjärjestelmän moniin versioihin sisältyvällä EFS-tiedostojärjestelmä (Encrypting File System) salausominaisuudella. Jos esimerkiksi sähköpostiviestintään liittyviä tiedostoja säilytetään paikallisella kiintolevyllä, voi se olla OpenPGP:lle vaihtoehtoinen tai lisäratkaisu tiedostojen salaamiseksi. Windows-järjestelmissä tähän voidaan yhdistää myös eri käyttäjien kesken esimerkiksi Aktiivihakemistoon perustuva ratkaisu, jolloin tiedostoja voidaan salata toisen käyttäjän julkisella varmenteella ja näin toimittaa tiedosto salattuna toiselle osapuolelle hieman PGP:n tapaan. Sekä OpenPGP:hen että EFS:ään perustuvassa tiedostonsalauksessa on tärkeää, että julkisen avaimen varmenteista ja niihin liittyvistä salaisista avaimista otetaan myös varmuuskopiot siltä varalta, että alkuperäinen varmenne syystä tai toisesta katoaa tai vaurioituu.

4.5.6 Yksityisen avaimen hallinta

Julkisten OpenPGP avaimien hallinta, niiden tuonti ja vienti tulivat tutuiksi jo salatun sähköpostiviestinnän aloitusvaiheessa. Toisinaan myös yksityinen avain joudutaan siirtämään toiseen tietokoneeseen tai sen varmuuskopio on joka tapauksessa hyvä olla olemassa ja aika ajoin päivittääkin. Avain viedään Kleopatra-avaintenhallintaohjelmalla binäärimuotoiseksi tiedostoksi, joka sisältää salatun varmenteen yksityinen avain mukaanlukien. Kyseinen binääritiedosto on .gpg-päätteinen, ja sitä ei voida avata tai muokata millään tekstinmuokkausohjelmalla. Avain voidaan niin halutessa tallentaa myös ASCII-muotoon, jolloin sen sisältö nähdään tekstieditorilla julkisen avaimen tapaan yksityisen PGP-avaimen otsikkotiedoin, jonka alla varsinainen avainosa on sekalaisena

merkistömassana. Tallennettua yksityisen avaimen sisältävää tiedostoa tulee säilyttää ja käsitellä erityisellä huolellisuudella.

4.6 GnuPG Linux-ympäristössä

GnuPG:tä voidaan käyttää yhtä lailla Linux-ympäristössä, johon kyseinen OpenPGP-standardiin perustuva ohjelmisto on alunperin kehitettykin. Niinpä on hyvä tutustua pääpiirteittäin myös siltä osin sähköpostisalauksen käyttöönottoon. Tämän hetken yleisimmistä Linux-järjestelmistä ja jakeluversioista esimerkiksi Ubuntussa GnuPG on yleensä mukana käyttöjärjestelmän perusasennuspaketissa gpg-ohjelmanimellä, ja tarvittaessa se voidaan asentaa aptitude-paketinhallintaohjelmalla.

Ohjelmiston käyttö aloitetaan Linux -ympäristössäkin avainparin luomisella (Kuva 23.). Avainparin luonti tuottaa myös avaintunnisteen, joka voidaan asettaa bashrc-tiedostoon, jolloin GnuPG:tä käyttävät sovellukset automaattisesti käyttävät kyseistä avainta. Samassa yhteydessä asennetaan yksityisiä avaimia hallitseva gpg-agent eli GnuPG-agenttiohjelmisto ja käynnistetään se taustaprosessiksi (engl. daemon).

Kuva 23. OpenPGP-avaimen luominen Linux-ympäristössä.

Tämän jälkeen julkisen avaimen binäärimuotoinen avaintiedosto voidaan enkoodata tekstimuotoiseksi ASCII-tiedostoksi, jota on helppoa jakaa tai kopioida ystäville ja muille viestinnän osapuolille suoraan tai tarkoitusta palvelevien sivustojen kautta (Kuva 24.). Näin on saatu perusasetukset valmiiksi salatun viestinnän aloittamiseksi. Vastaa-

valla tavalla ja samassa yhteydessä julkinen avain voidaan gpg-ohjelman avulla siirtää myös julkiselle avainpalvelimelle, josta kuka tahansa voi ladata sen salatun viestin lähettämiseksi. Toimenpidettä kannattaa kuitenkin aluksi harkita, varsinkin jos on vähänkään epävarmuutta sen hetkisen avaimen pitkän tähtäimen käyttötarkoituksesta. Jakeluun lähetetty avain voi levitä melko nopeasti avainpalvelinverkossa, mikä sinänsä on hyvä asia, mutta voi toisaalta aiheuttaa ylimääräistä vaivaa siinä tapauksessa, ettei nimenomainen avain ole sittenkään lopullinen. Vanhentuneen avaintiedon poistaminen saattaa olla varsin aikaa vievää, etenkin jos avain on ehtinyt leviämään laajemmalti [16.].

```
tuomakir@utesti:~$ gpg --output julkinenavain.asc --export -a $GPGKEY
tuomakir@utesti:~$ cat julkinenavain.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQENBFEO23YBCAC4VEBw6X7MWYLdtNPjkUDfKzTJm4whiNpkG+kkV6nw0q9IErUJ
wbwoxbaZHR4SFg7Kq4vvEWJDbSgZD8GCjKEn+sDpKRyR5M9v5uHNKLAdgzo+TKxA
pLcNiwcybNCGfpAkYMnfo4DXfy40Nws/iQ/Uix6RAQYS35XSOUxF5y6034C3fRQW
ivu4pfpfqbyBzWBTN2XYDhDiExF2v7azqnf4i12nDpD/HrA4m62vvMGXMUg+CbdX
uFz5dgSImh6OGshsWX24ZL7OjLLKOJDuvXzZI8v5HLUryz+Awtu9odnQGm4M2Lrs
Bl+N2fgiIUvp1yJkMM7CqxzfJeQgrFNsycKXABEBAAG0IXR1b21ha2lyIDx0dW9t
YWtpckBtZXRyb3BvbGlhLmZpPokBOAQTAQIAIgUCUQ7bdgIbAwYLCQgHAwIGFQgC
CQoLBBYCAwECHgECF4AACgkQPK4XZIHACq9/7AgAqBZA4uE+SnB8b2VwvA4uyFSN
```

Kuva 24. Julkisen avaimen ASCII-version luonti ja sen tarkistaminen.

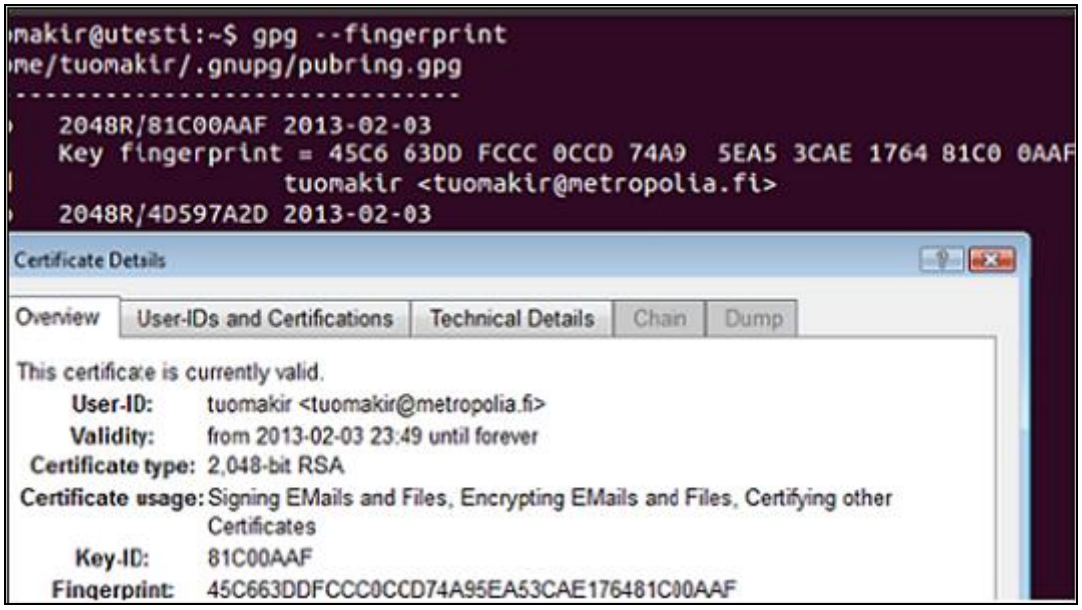
4.6.1 Salatut sähköpostiviestit Linux-ympäristössä

Sähköpostiviestejä voidaan Linux- tai Unix-ympäristössä käsitellä käyttöjärjestelmän shell- eli komentorivitasolla esimerkiksi Mutt-asiakasohjelmalla. Myös graafisia ohjelmia voidaan käyttää varsinkin Linux-työpöytäympäristöissä, jolloin niiden käyttö ja määritykset tapahtuvat hyvin pitkälti Windows-ympäristön tapaan. Vertailun ja Linux-ympäristön alkuperäisen luonteen vuoksi käsittelenkin tässä yhteydessä komentorivipohjaista sähköpostiviestinnän salausta.

Sähköpostiasiakasohjelmiston lisäksi tarvitaan SMTP (Simple Mail Transfer Protocol) -ohjelmisto sähköpostiviestien toimittamiseksi eteenpäin välittäjän tai vastaanottajan SMTP-palvelimelle. Itse käytin tarkoitukseen kevyttä avoimen lähdekoodin Msmtp–ohjelmistoa. Sähköpostin asiakasohjelmiston eli MUA:n (Mail User Agent) – tässä tapauksessa Mutt-ohjelmiston – asetustiedostot puolestaan määritetään kutsumaan msmtp-ohjelmaa viestin lähetysvaiheessa. Lisäksi Mutt-asetuksiin määritetään asetuk-

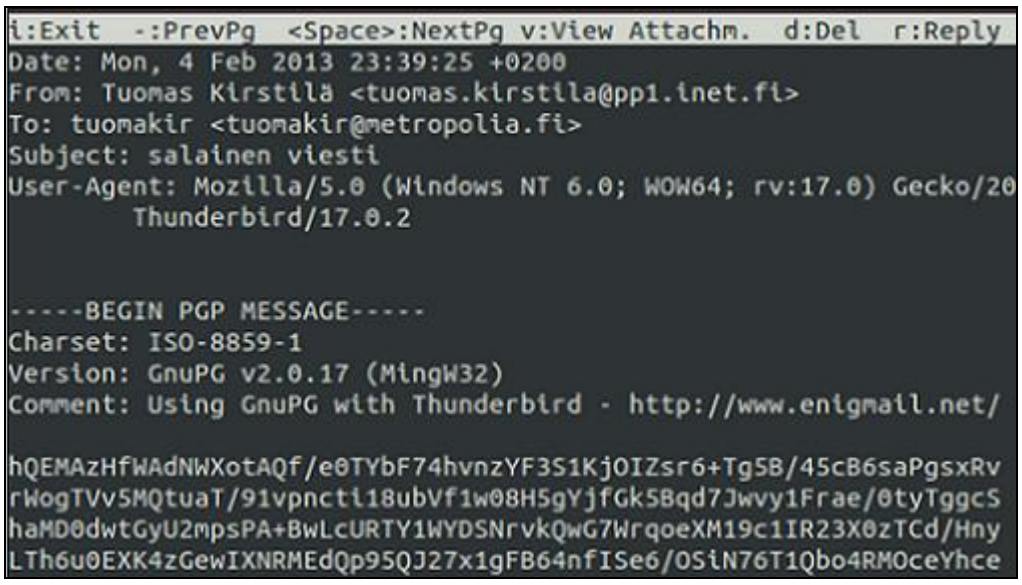
set saapuvan sähköpostin lukemiseen esimerkiksi IMAP (Internet Message Access Protocol) -protokollalla.

Salattu viestintä alkaa tutun kaavan mukaan. Lähetetään Linuxin GnuPG:llä luotu julkinen avain vastaanottajalle, tässä tapauksessa vastaanottajalle Windows-ympäristön sähköpostiasiakasohjelmistoon. Vastaanottaja tallentaa julkisen avaimen Kleopatra-avaintenhallinnalla. Samalla on hyvä varmistaa, että lähettäjän ilmoittama sormenjälki täsmää vastaanottajan näkemään (Kuva 25.).



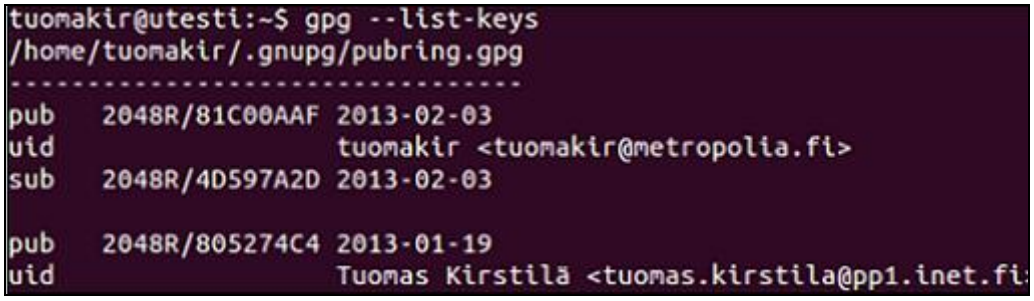
Kuva 25. Julkisen avaimen sormenjäljen tarkistaminen.

Tämän jälkeen julkisen avaimen haltija voi lähettää vastauksensa, jonka vastaanottaja saa salattuna (Kuva 26.).



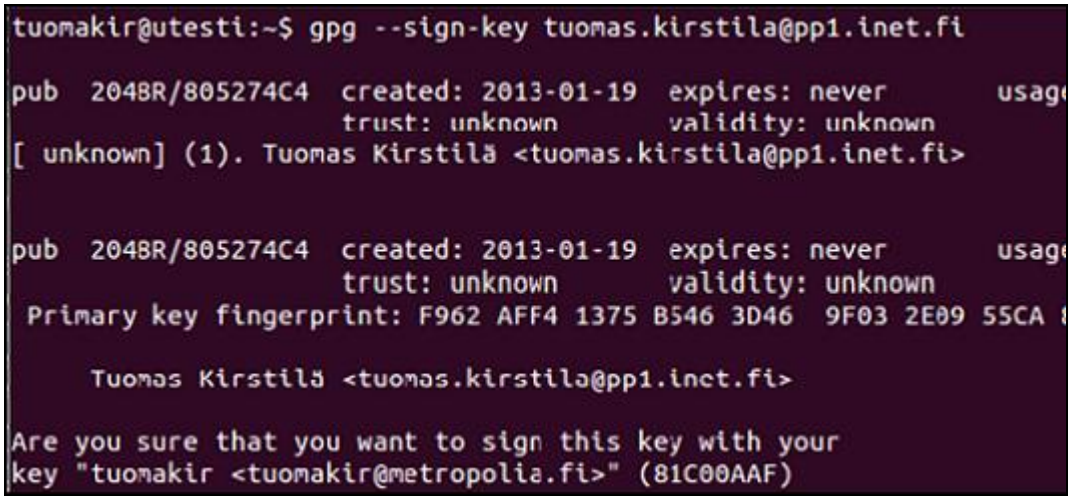
Kuva 26. Salatun viestin vastaanotto Linux-ympäristössä.

Salattu viesti puretaan GnuPG-ohjelmalla. Mikäli lähettäjän julkinen avain löytyy omasta julkisten avainten avainrenkaasta, nähdään myös viestin digitaalinen allekirjoitus. Tallennetut julkiset avaimet voidaan listata GnuPG:ssä kuvan mukaisesti (Kuva 27.).



Kuva 27. Julkisen avainrenkaan sisältö.

Allekirjoitus ei näy kuitenkaan luotettavana ennen toisen osapuolen julkisen avaimen allekirjoittamista ja varmentamista omalla salaisella avaimella. Avaimen oikeellisuuden ja luotettavuuden pitää vain olla varmistettu tapaamisen yhteydessä tai muun yhteydenpitokanavan kautta vaihtamalla siihen liittyvä sormenjälkitieto tai sen muodostavan heksadesimaaliluvun kahdeksan viimeisen numeron GnuPG-avaintunniste. Sen jälkeen kyseisen osapuolen julkinen avain voidaan allekirjoittaa (Kuva 28.).



Kuva 28. Toisen osapuolen julkisen avaimen varmentaminen GnuPG:llä.

Lopulta viestin salaus puretaan (Kuva 29.).

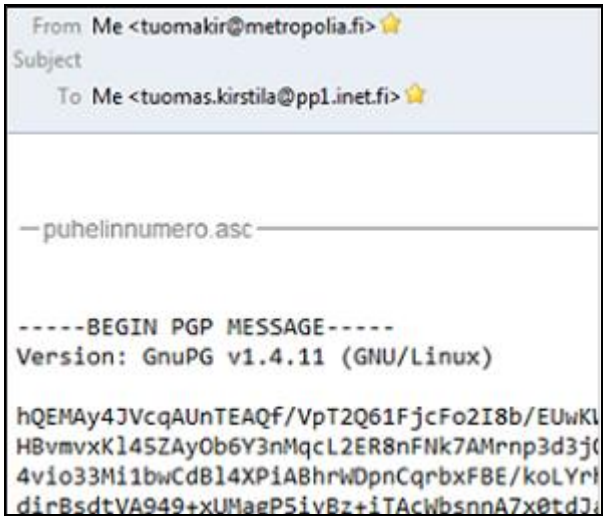
Kuva 29. Salatun viestin avaaminen GnuPG:llä.

Viestin tai tiedoston salaus avainrenkaaseen tallennetulla vastaanottajan julkisella avaimella ja sen allekirjoitus omalla salaisella avaimella tapahtuvat GnuPG:ssä kuvan osoittamalla tavalla (Kuva 30.).

```
tuomakir@utesti:~$ gpg -a -se -r Tuomas puhelinnumero

You need a passphrase to unlock the secret key for
user: "tuomakir <tuomakir@metropolia.fi>"
2048-bit RSA key, ID 81C00AAF, created 2013-02-03

tuomakir@utesti:~$ cat puhelinnumero.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

hQEMAy4JVcqAUnTEAQf/VpT2Q61FjcFo2I8b/EUwKWtSLSUAMKfSio
HBvmvxKl45ZAyOb6Y3nMqcL2ER8nFNk7AMrnp3d3jQ4SVwP5JqR/0w
4vio33Mi1bwCdBl4XPiABhrWDpnCqrbxFBE/koLYrhy8f3O0f95aAi
dirBsdtVA949+xUMagP5iyBz+iTAcWbsnnA7x0tdJaAJ0zD9sl+TiJ
```

Kuva 30. Tiedoston salaus ja allekirjoitus GnuPG:llä.

Salattu viesti ei eroa vastaanottajan päässä alkuperäisestä, vaan näyttää edelleen täsmälleen samalta.



Kuva 31. Salattu viesti saapunut vastaanottajalle.

Vastaanottaja purkaa viestin salaisella avaimellaan. Hän saa vakuudeksi myös viestin allekirjoitustiedot, jonka aiemmin vaihdettu sormenjäljen avaintunnistekin vahvistaa (Kuva 32.). Paljastunut viesti osoittaa sen, ettei salatusta viestistä pysty sitä mitenkään johtamaan tai päinvastoin. Näin salattujen viestien ja tiedostojen vaihto on todella osoittanut toimivuutensa, käyttökelpoisuutensa ja monipuolisuutensa.

Kuva 32. Purettu viesti allekirjoituksineen.

4.7 Avainten varmistaminen ja käytöstä poistaminen

Julkinen avain lähetetään usein eteenpäin heti sen luomisen jälkeen, joten monesti siitä on olemassa kopio paikallisen levyn lisäksi esimerkiksi sähköpostipalvelimella. Sen sijaan yksityisestä avaimesta ei välttämättä varmuuskopiota ole, jos ei sitä erikseen luoda. Se voi olla tarpeen esimerkiksi laiterikon, tai muuten vain toiseen tallennusmediaan tai tietokoneeseen siirryttäessä. OpenPGP:ssä yksityisestä avaimesta otetaan kopio Kleopatra-avaintenhallintaohjelmalla. Ohjelmalla varmuuskopioksi viety varmenne sisältää käytännössä koko avainparin eli julkisen ja salaisen avaimen. Varmuuskopion säilytyksessä tulee luonnollisesti olla erittäin tarkka.

Joskus voi olla tarpeen poistaa tai mitätöidä käytössä oleva avain. Asia konkretisoituu esimerkiksi salaiseen avaimeen liittyvän salasanan unohtuessa tai salaisen avaimen joutuessa muutoin vääriin käsiin. GnuPG:llä ja OpenPGP:llä on mahdollista luoda tiedosto, jolla esimerkiksi avainpalvelimelle ladattu avain voidaan mitätöidä. Lähtökohtaisesti on kuitenkin hyvä pitää mielessä, että erityisesti avainpalvelimelle tai muuten laajasti jaellun avaimen poistaminen käytöstä ei ole välttämättä aivan yksinkertaista.

4.8 PGP:n turvallisuus

Ennen PGP-sovellusten vakavamielistä käyttöönottoa kenties suurin yksittäinen huolenaihe on sen itsessään turvallisuus. Voiko salaukseen todella luottaa? Siihen vaikuttavat tietysti monet yksittäiset tekijät PGP:n versioista ja avainten salasanoista lähtien.

Mutta puhtaasti PGP:n salausteknisestä näkökulmasta katsottuna on ainakin hyvin laaja ja yksimielinen käsitys menetelmän luotettavuudesta. PGP:n käyttämät salausalgoritmit eivät ole olleet ainakaan toistaiseksi tunnetuin keinoin murrettavissa. Pidetään myös varmana, ettei ohjelmaan ole piilotettu sen käyttäjän turvallisuutta uhkaavaa takaporttiakaan, jonka kautta kenties tekniikkaa kehittävä tai jokin täysin tuntematon taho pystyisi salauksen kiertämään. Ja vaikka PGP:n käyttämät salaus- ja purkumenetelmät ovat tunnettuja, on itse salaus ehdottoman turvallinen niin pitkään kuin salainen avain pysyy salassa. Lisäksi viimeisimpänä muttei vähäisimpänä, on menetelmän pitkäaikainen ja suuren käyttäjäkunnan osoittama suosio. Vuosien aikana tuhansien, jopa miljoonien PGP-käyttäjien keskuudesta ei ole noussut esille ainakaan merkittävää menetelmän luotettavuutta epäilevää käyttäjäkuntaa eikä menetelmää ole muutenkaan pystytty osoittamaan epäluotettavaksi tai haavoittuvaksi. Näihin menetelmän turvallisuutta koskeviin tietoihin ja olettamuksiin voi siis tavallinenkin käyttäjä epäilemättä uskoa ainakin nykytilanteen valossa.

5 Pohdinta ja yhteenveto

Työn lähtökohta oli kartoittaa tietoturvan parantamisen mahdollisuuksia käytännön salausmenetelmin ketä tahansa tietokoneen ja tietoverkon käyttäjää silmällä pitäen. Vaikka aihe on ollut tavalla tai toisella esillä koko henkilökohtaisten tietokoneiden elinkaaren eli viime vuosikymmenten ajan, voi sitä nykyisin pitää entistäkin tärkeämpänä. Yhä suurempi osa tiedoistamme tallennetaan sähköisesti alati laajenevaan tietoverkkoon. Verkkoympäristössä tapahtuvasta viestinnästä ja tietojen tallentamisesta on tullut arkipäivää lähes jokaiselle, vaikka välttämättä kaikkia asiaan liittyviä tekijöitä tai seurauksia ei aina tarkemmin pohdita. Suuri osa tiedoista voi tietysti olla tietosuojan kannalta tai arkaluontoisuudeltaan lähes merkityksetöntä, mutta joukossa on varmasti myös tärkeää, henkilökohtaista tai jopa identiteetin paljastavaa ja siten väärinkäyttäjille arvokasta tietoa. Ne saattavat päätyä ihmisten tietämättömyyttä tai huolimattomuutta mihin tahansa, aiheuttaen pahimmillaan suurtakin harmia tai vahinkoa omistajalleen tai niistä muulla tavoin riippuvaiselle taholle. Onneksi yksittäinenkin tietoverkon käyttäjä voi itse vaikuttaa tietoturvansa ja tietosuojansa tasoon – oman verkkokäyttäytymisen lisäksi varsinkin sähköpostiviestinnän ja tietojen säilytyksen osalta. Ei vaadi edes kovin merkittäviä toimenpiteitä tietojensa väärinkäytösten riskiä pienentääkseen ja oman tietoturvansa tasoa parantaakseen.

Työ osoitti, että salausmenetelmien käyttö näiden tietoturvapyrkimysten saavuttamiseksi kannattaa, jos punnitaan vaadittavia toimenpiteitä sekä toisaalta tunnettujen ja arvioitujen riskien mahdollisuutta ja esiintyvyyttä. Oletettavaa tietysti olisi, että mahdollisimman hyvä tietoturva olisi kaikissa tietotekniikan sovelluksissa ja palveluissa poikkeuksetta lähtökohta. Valitettavasti näin ei joka tilanteessa ole, vaan toisinaan osa käyttäjistä ja jopa ohjelmiston tai palvelun toimittajista etenee käytettävyyden ehdoilla. Salausmenetelmien osalta tämä tarkoittaa, ettei niiden toimiminen ja riittävän tietoturvatason saavuttaminen ole läheskään aina ohjelmistojen perusominaisuuksiin kuuluva automaatio, vaan vaatii yleensä sekä hieman perehtyneisyyttä aihepiiriin että ylimääräisiä työvaiheita. Asia tuli hyvin tässäkin työssä esille.

Aiheen teoria ja salausohjelmistojen ominaisuudet sekä niiden käyttöön liittyvät toimenpiteet muodostavat melko laajan kokonaisuuden pelkästään peruskäyttöäkin ajatellen. Se loikin haasteensa riittävän yhdenmukaisen ja tiiviin sekä silti mahdollisimman monipuolisen ja hyödyllisen selvitystyön tekemiselle. Päätinkin rajata käsiteltävää aihealuetta melko voimakkaasti niin teoria- kuin käytännönosuudesta käsitellen kuitenkin molemmista olennaisimmat. Salausmenetelmien sovellusalueista pidin yksittäisen käyttäjän tietoturvan kannalta keskeisimpänä sähköpostiviestintää, jonka koin myös parhaiten kuvaavan salausmenetelmien soveltamista käytännössä. Lisäksi monipuolinen avoimen lähdekoodin PGP-ohjelmisto soveltui erityisesti sähköpostiviestinnän salaukseen tärkeitä lisäominaisuuksia unohtamatta. Kokonaisuudessaan työ muodostaa mielestäni yleistietopaketin salausmenetelmien käyttöönottamiseksi, alkaen asiaan liittyvien peruskäsitteiden ymmärtämisestä, edeten sovellusten käyttöönoton ja peruskäytön vaiheisiin. Onnistuin mielestäni laatimaan sisällön työn lähtökohtia vastaavaksi. Eli se vastaa yksittäisen tietoverkon käyttäjän tietoturvan parantamisen mahdollisuuksiin liittyviin kysymyksiin - etenkin tietoturvan keskeisimpiin kuuluvien osa-alueiden; luottamuksellisuuden, eheyden ja todennuksen osalta.

Henkilökohtaisesti työ oli ennen kaikkea mainio tapa perehtyä projektiluonteisesti itseäni kiinnostavaan tietotekniikan osa-alueeseen monipuolisesti teorian, ohjelmistojen käyttöönoton ja käytön sekä dokumentoinninkin muodoissa. Ennakkoon ehkä haasteellisimmalta tuntunut, mielekkään asiakokonaisuuden muodostaminen onnistui mielestäni melko hyvin siitäkin huolimatta, ettei kyse ollut tietyn, tuotantoympäristöön sijoitettavan järjestelmän tai vastaavan raameiltaan hyvin selkeän projektin läpiviemisestä. Toisaalta puhtaasti oman mielenkiinnon pohjalta muodostettu ja osin kuvitteellinenkin kokonaisuus myös jollakin tavalla sopii tietoturvan luonteeseen, koska menetelmien tuot-

tamaa todellista tehoa tai hyötyä ei välttämättä muutenkaan voida täysin yksiselitteisesti tai systemaattisesti osoittaa, mitata tai vertailla. Voidaan vain pyrkiä vallitsevissa ja tunnetuissa olosuhteissa mahdollisimman korkeaan tietoturvan tasoon, joka tuskin koskaan toteutuu aivan täydellisesti.

Toivon tämän työn tarjonneen lukijalleen joitain virikkeitä ja näkökulmia salausmenetelmien käyttöönottoon. Uskon sen ainakin osoittaneen salausmenetelmien käytön merkityksellisyyden myös tavallisen tietoverkon käyttäjän tietoturvallisuuden kannalta. Tekijälleen työ avasi kaiken kaikkiaan laajan näkymän tietoturvan ja salausmenetelmien monipuoliseen ja kiehtovaan maailmaan. Se on antanut vähintään hyvät yleistiedot salausmenetelmiin liittyvistä tekniikoista edesauttaen niiden syvällisemmänkin tason ymmärtämystä ja hyödyntämistä jatkoa ja laajempia kokonaisuuksia silmällä pitäen. Olisi siis mielenkiintoista työskennellä salausmenetelmien parissa jatkossakin ja kenties hieman erilaiseen lähtökohtaan ja sovellusalueeseen liittyen.

Lähteet

1 Baker, M. Mel, H.X. 2001. Cryptography Decrypted. Addison-Wesley.

2 ECHELON. 2012. Verkkodokumentti. <http://en.wikipedia.org/wiki/ECHELON>. Luettu 01.01.2013.

3 Gollmann, D. 2010. Computer Security (Third Edition). Wiley.

4 Järvinen, P. 2003. Salausmenetelmät. Porvoo: WS Bookwell.

5 Kerttula, E. 2000. Tietoverkkojen Tietoturva. Helsinki: Oy Edita Ab.

6 PATU Pankkien asiakasyhteyksien tietoturva. 1998. Verkkodokumentti. Suomen Pankkiyhdistys. <http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/PATU_v1_22.pdf>. Luettu 16.12.2012.

7 Stallings, W. 2011. Cryptography and Network Security (Fifth Edition). Pearson.

8 The GNU Privacy Handbook. 2012. Verkkodokumentti. The Free Software Foundation. <http://www.gnupg.org/gph/en/manual.pdf>. Luettu 28.12.2012.

9 The Gpg4win Compendium - Secure e-mail and file encryption using GnuPG for Windows. 2012. Verkkodokumentti. Gpg4win Initiative. <http://www.gpg4win.org/documentation.html> Luettu 29.12.2012.

10 Tiedonsalaaminen. 2012. Verkkodokumentti. Jyväskylän Yliopisto. <http://appro.mit.jyu.fi/doc/tiedonsalaus/>. Luettu 20.10.2012

11 Tiedostojen suojaaminen Bitlocker-asemansalauksen avulla. 2012. Verkkodokumentti. Microsoft. <http://windows.microsoft.com/fi-FI/windows7/Help-protect-your-files-using-BitLocker-Drive-Encryption>. Luettu 28.10.2012.

12 Announcing the Advanced Encryption Standard. 2001. National Institute of Standards and Technology. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Luettu 30.12.2012.

13 Mime Security with OpenPGP. 2001. RFC – Network Working Group. <http://community.roxen.com/developers/idocs/rfc/rfc3156.html>. Luettu 01.02.2013.

14 Enigmail Configuration Manual. 2013. Verkkodokumentti. The Enigmail Project. <http://www.enigmail.net/documentation/>. Luettu 01.02.2013.

15 The Encrypting File System. 2013. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc700811.aspx>. Luettu 03.02.2013.

16 GnuPrivacyGuardHowto. 2012. Verkkodokumentti. Ubuntu documentation. <https://help.ubuntu.com/community/GnuPrivacyGuardHowto>. Luettu 04.02.2013.