LAUREA AMMATTIKORKEAKOULU Uuden edellä

Salausmenetelmät: Symmetrinen, epäsymmetrinen ja tiivistealgoritmit

Kaarnalehto, Mika

2011 Laurea

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Salausmenetelmät: Symmetrinen, epäsymmetrinen ja tiivistealgoritmit

Kaarnalehto, Mika
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2011

Laurea ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Tietojärjestelmien kehittäminen

Mika Kaarnalehto

Salausmenetelmät: Symmetrinen, epäsymmetrinen ja tiivistealgoritmit

Vuosi 2011 Sivumäärä 34

Opinnäytetyönä on tehty itseopiskelumateriaali, josta opiskelija voi omatoimisesti opetella salauksen historiasta, nykypäivästä ja keskeisistä menetelmistä. Työn tavoitteena on tuottaa harjoitustehtäviä salausmenetelmiin perehtymistä varten tietojenkäsittelyn ja turvan opiskelijoille.

Salaisuuksia henkilöiden kesken on ollut pitkään, mutta keinot niiden säilyttämiseen ja lähettämiseen ovat vaihdelleet. Menetelmät ja tekniikat, joita vain sotilaat ja diplomaatit käyttivät, ovat tänään osa jokapäiväistä elämää. Kryptologia on salaisuuksiin ja niiden purkamiseen erikoistunut tieteenlaji.

Ensimmäisiä salakirjoituksen kuvauksia löytyy 400-luvun eKr kirjoituksista. Ensimmäinen sotilaalliseen kryptografiaan käytetty laite on spartalainen scytale, joka on peräisin samoilta ajoilta kuin ensimmäiset salakirjoituksen kuvaukset. 1900- luvulla tekniikan kehittyminen mahdollisti myös salauksessa käytettävien menetelmien uudistamista. Toinen maailmansota on yksi merkittävistä yksittäisistä tekijöistä salaustekniikan kehittymisessä eteenpäin. Tietotekniikka alkoi liittyä yhä kiinteämmin salaukseen. Internet ja langaton matkaviestintä aiheuttivat vallankumouksen lopullisesti 1990-luvun puolivälissä.

Salausmenetelmillä pyritään varmistamaan tietojen luottamuksellisuus, eheys ja kiistämättömyys. Kaikki salaukset ovat murrettavissa. On kyse vain siitä, paljonko aikaa ja tietokonetehoa tarvitaan. Salaustekniikat pohjautuvat joko tietokoneella tapahtuvaan bittien sekoittamiseen (symmetriset salaukset) tai matemaattiseen laskentaan (epäsymmetriset salaukset).

Työssä on kerätty olemassa olevaa teoreettista tietoa salausmenetelmistä useista eri lähteistä ja tehty niiden pohjalta tiivistetty itseopiskelumateriaali. Opiskelumateriaalituotos tulee olemaan sähköisessä muodossa, mikä mahdollistaa materiaalin helpon jakamisen kursseilla. Materiaalissa on myös tehtäviä, joissa pääsee käytännössä testaamaan oppimaansa ja näkemään salauksen mahdollisuudet.

Asiasanat salausmenetelmät, kryptologia, symmetrinen, epäsymmetrinen, tiivistefunktio

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Mika Kaarnalehto

Cryptography: symmetric, asymmetric, and hash functions

Year 2011 Pages 34

The thesis is a self-learning material that students can independently use to learn the history and the modern day cryptography and the main methods. The goal is to provide exercises to familiarize Business Information Technology and Security Management students with the encryption methods.

There have always been secrets between persons, but the means to preserve and transmit them have varied. Methods and techniques which only soldiers and diplomats have used, are today a part of everyday life. Cryptology is the encryption and the decryption of a specialized type of science.

The first cipher descriptions can be found in the 4th century BC writings. The first device used for military cryptography is a Spartan scytale, which dates back to the same era as the first cipher description. In the 20th century technological development also made encryption methods used for regeneration possible. The Second World War is one of the significant individual factors in the development of encryption technology. Information technology began to be more closely associated with encryption. The Internet and wireless mobile communications brought caused a revolution in the mid 1990s.

Cryptographic methods are to ensure data confidentiality, integrity and non-repudiation. All levels of encryption can be broken. It is just a matter of how much time and computer power is needed. Encryption techniques are based either on mixing computer bits (symmetric encryption) or a mathematical calculation (asymmetric encryption).

This thesis has gathered known theoretical information about encryption methods from many different sources. The self-learning material which was made is based on the gathered information. The self-learning material will be in electronic form, which will make distribution very easy in classes. The material also includes exercises in which students can test their learning and see the opportunities of encryption in action.

Key words cryptography, cryptology, symmetric, asymmetric, hash functions

Sisällys

1 Johdanto

Opinnäytetyönä on tehty itseopiskelumateriaali, josta opiskelija voi omatoimisesti opetella salauksen historiasta, nykypäivästä ja keskeisistä menetelmistä. Opiskelumateriaalituotos tulee olemaan sähköisessä muodossa, mikä mahdollistaa materiaalin helpon jakamisen kursseilla. Materiaalissa on myös tehtäviä, missä pääsee käytännössä testaamaan oppimaansa ja näkemään käytännössä salauksen mahdollisuudet.

Työn tavoitteena on tuottaa harjoitustehtäviä salausmenetelmiin perehtymistä varten tietojenkäsittelyn ja turvan opiskelijoille. Salausmenetelmät on esitelty yksinkertaisella ja selkeällä tavalla, ettei oppiakseen salausmenetelmistä tarvitse olla tietojenkäsittelyn asiantuntija. Opetuspaketti tulee Laurea ammattikorkeakoulun käyttöön eri koulutusohjelmissa, joissa käsitellään turvallisuuteen tai salaukseen liittyviä asioista.

Käytän opinnäytetyössäni menetelmänä konstruktiivista tutkimusta. Työssä on kerätty olemassa olevaa teoreettista tietoa salausmenetelmistä useista eri lähteistä ja tehty niiden pohjalta tiivistetty itseopiskelumateriaali.

Opinnäytetyössä käsitellään ensimmäisenä käytettävä Konstruktiivinen tutkimusmenetelmä; minkälaisissa tapauksissa sitä voidaan käyttää lähestymistapana. Työssä seuraavana käydään läpi erilaisia oppimistyylejä ja minkä takia on päädytty tekemään itseopiskelumateriaali. Teoriaosassa aloitetaan salausmenetelmien historiasta ja miten menetelmät ovat muuttuneet teknologian kehittyessä. Tarkemmin paneudutaan symmetrisen ja epäsymmetrisen salauksen sekä tiivistealgoritmien käyttöön sähköpostiviestinnässä. Viimeiseksi käydään läpi, minkälaisessa muodossa itseopiskelumateriaalin on.

2 Konstruktiivinen tutkimusmenetelmä

Opinnäytetyöni perustuu konstruktiiviseen tutkimusmenetelmään. Konstruktiivinen tutkimus soveltuu käytettäväksi kun luodaan jonkinlainen konkreettinen tuotos, suunnitelma, mittari tai malli, jonka päämääränä on ongelman ratkaisu. Konstruktiivinen tutkimus muistuttaa lähestymistapana innovaatioiden tuottamista, vaikka läheskään kaikki kehittämistyön tuloksena syntyneet uudet tuotokset eivät ole innovaatioita vaan kehitystyön tuloksena syntyneitä rakenteita, joita arvioidaan niiden käytännön hyödyn perusteella. Konstruktiivisessa tutkimuksessa on oleellista sitoa käytännön ongelma ja sen ratkaisu teoreettiseen tietoon. On myös tärkeää, että ratkaisu osoittautuu toimivaksi myös kohdeorganisaation ulkopuolella. Konstruktiivinen tutkimus voidaan jakaa kuuteen vaiheeseen (Ojasalo, Moilanen & Ritalahti 2009, 65–67.):

1. Ongelman etsiminen
2. Teoreettisen ja käytännöllisen tiedon hankinta tutkimuksen ja kehittämisen kohteesta
3. Ratkaisun konstruktio
4. Ratkaisun toimivuuden testaaminen
5. Ratkaisussa käytettyjen teoriakytkentöjen näyttäminen ja ratkaisun uutuusarvon osoittaminen
6. Ratkaisun soveltamisalueen laajuuden tarkastelu

Opinnäytetyössäni ongelmana on salausmenetelmiin liittyvien harjoitustehtävien puuttuminen, jotka tekevät syvällisemmän opiskelun mahdolliseksi. Harjoitustehtävien lisäksi työhön kuuluu teoriapaketti, jossa käydään harjoitustehtäviin liittyvät menetelmät läpi.

Teoreettista tietoa on paljon, mutta se on hajautettuna useaan eri lähteeseen. Aloitin lähestymisen ongelmaan keräämällä ja tutustumalla lähteisiin oppimisesta, opetusmateriaalin tuottamisesta ja salausmenetelmistä. Harjoittelin myös käytännössä tiedon salaamisessa käytettäviä menetelmiä, saaden näin käytännöllistä tietoa, mikä auttoi huomattavasti konstruktiovaiheessa.

Konstruktiovaiheessa päädyin tekemään internetpohjaisen itseopiskelupaketin, koska verkossa oleva materiaali on helposti käytettävissä ja saatavissa mistä vain. Syntynyt materiaali ei ole innovaatio vaan kehitystyön tuloksena syntynyt tuotos, jota arvioidaan sen käytännön hyödyn perusteella. Testaaminen ja käytännön hyödyn varmistaminen sekä jatkokehittäminen jäävät myöhempään ajankohtaan.

3 Salausmenetelmät itseopiskelumateriaalina

Tehdessäni koulutusmateriaalia salausmenetelmistä opinnäytetyönä, mietin parasta mahdollista vaihtoehtoa opiskelijan oppimisen kannalta. Ammattikorkeakoulun monimuoto-opiskelu mahdollistaa useita erilaisia opetusmenetelmiä, joita olisi voinut käyttää. Päädyin tekemään itseopiskelumateriaalin, koska itseopiskelu soveltuu parhaiten suurimmalle osalle opiskelijoista, joka selviää oppimistyylimääritelmistä seuraavassa osiossa. Käyn seuraavaksi läpi erilaisia oppimistyylejä, sekä opiskelijan vireystilan vaikutusta oppimiseen.

”Termeillä monimuoto-opetus ja monimuoto-opiskelu tarkoitetaan lähiopetuksen, etäopetuksen ja itseopiskelun yhdistämiseen perustuvia opetuksen ja opiskelun toteutustapoja” (Kajanto 1993, 164.).

3.1 Oppimistyylit

Olemme kaikki oppijoita - muuten emme osasi kävellä, puhua, laskea, ajaa pyörällä, luoda ihmissuhteita tai lukea sanomalehteä. Oppiminen tapahtuu monella eri tavalla: kokeilemalla, erehtymällä, korjaamalla, leikkimällä, kysymällä, tekemällä, tutkimalla, matkimalla jne. Ongelmia voi tulla, kun oletetaan kaikkien toimivan ja oppivan samalla tavalla ja vauhdilla. On tärkeä muuttaa koulutustilanne itselle sopivaksi oppimistapahtumaksi. (Otala 2001, 47–48.)

Ihmisillä on erilaisia oppimistyylejä, eli vastaanotamme tietoa ja muodostamme tietoa eri tavoin. Oppimistyylin mukaan oppija voi olla aktiivinen osallistuja, käytännön toteuttaja, looginen ajattelija tai harkitseva tarkkailija. (Otala 2001, 61.)

- Aktiivinen osallistuja oppii parhaiten saadessaan haastavia tehtäviä, jos oppimista tuetaan visuaalisin keinoin, esimerkiksi kuvin, videoin ja esimerkein. Aktiivinen innostuu uudesta ja on valmis myös kokeilemaan kaikenlaista. (Otala 2001, 62.)

- Käytännön toteuttaja oppii parhaiten tekemällä ja kehittämällä taitoja. Hän tarvitsee oppiakseen välittömän soveltamismahdollisuuden, eli hän oppii, kun voi saman tien toteuttaa uuden asian. (Otala 2001, 63.)

- Looginen ajattelija oppii parhaiten mallien, käsitteiden ja teorioiden avulla. Hän käyttää oppimisessa lukemista, tutkimista ja päättelemistä. Hänelle soveltuvat kurssit ja jopa koulumuotoinen oppiminen, koska teoriaan pohjautuva oppiminen voidaan helposti siirtää minne vain. (Otala 2001, 64.)

- Harkitseva tarkkailija oppii parhaiten, kun on aikaa ajatella ja pohtia ennen toimintaa. Hän myös vetäytyy mielellään syrjään voidakseen puntaroida tapahtumia ja tarkastella niitä eri näkökulmista. Hän tarvitsee aikaa selvittääkseen asioita perusteellisesti, joten itseopiskeluohjelmat ja kirjat ovat sopivia oppimistapoja. (Otala 2001, 65.)

Jokaisessa erilaisessa oppimistyylin kuvauksessa on havaittavissa niiden soveltuvuus itseopiskelumateriaalin ja siihen liittyvien harjoitusten tuomiin mahdollisuuksiin. Omatoimisessa oppimisessa jokainen voi räätälöidä itselleen sopivan painotuksen alueista, joissa tarvitsee harjoitusta.

Aktiivinen osallistuja ja käytännön toteuttaja oppivat parhaiten haastavien tehtävien kautta, ja kun he saavat käyttää heti opittuja asioita. Työssä olevat salausmenetelmät on esitelty teorian avulla, mutta myös käyttäen hyväksi visuaalisia keinoja, kuten kuvia ja esimerkkejä. Harjoitustehtävät tuovat haasteita ja mahdollistavat teorian testaamisen suoraan käytäntöön.

Looginen ajattelija ja harkitseva tarkkailija oppivat parhaiten käsitteiden ja teorioiden avulla. He tarvitsevat aikaa voidakseen tutkia ja puntaroida oppimaansa, joten itseopiskelumateriaali on ihanteellinen oppimiseen. Teoriaan pohjautuva itse oppiminen sopii molemmille, koska siihen ei ole sidottu aikarajoitteita niin voimakkaasti kuin normaaliin tuntiopetukseen.

3.2 Parhaan vireystilan hyödyntäminen oppimisessa

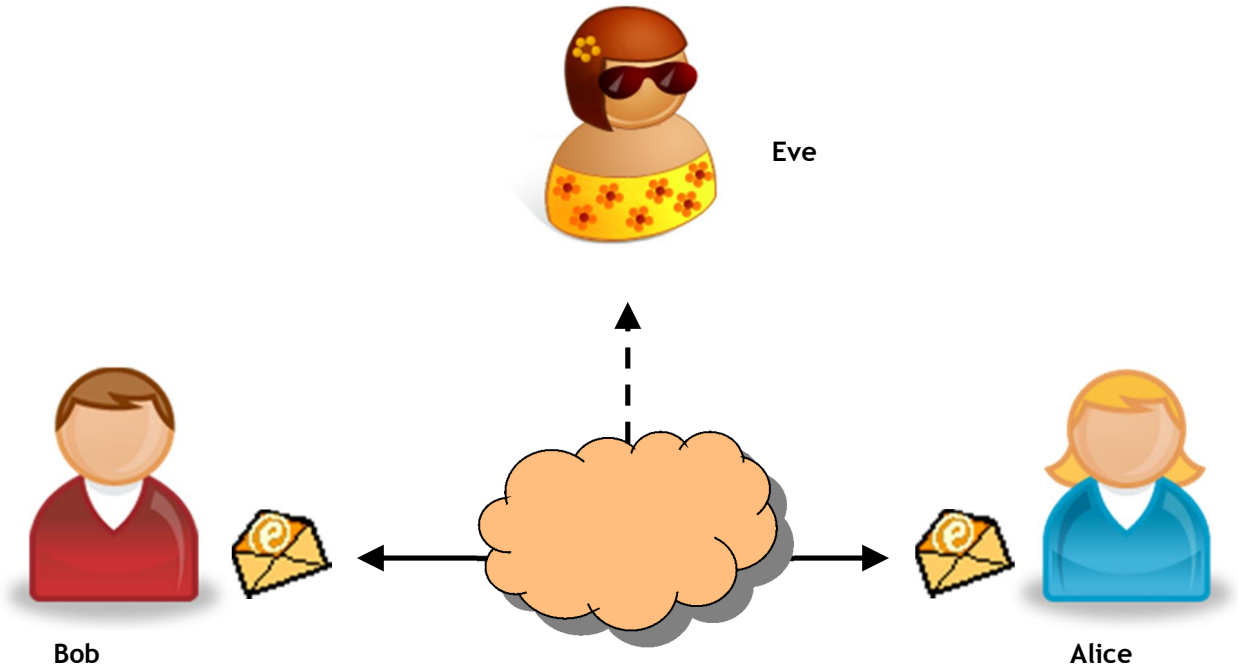
Parhaan oppimisajankohdan tunnistaminen auttaa valitsemaan sellaisen ajankohdan, jolloin oppiminen on mieluisaa eikä turhaan joudu taistelemaan väsymystä vastaan. Vireystilat voidaan jakaa kahteen pääryhmään, jotka ovat aamuvirkut ja yökyöpelit. Aamuvirkut ovat herättyään virkeitä ja valmiita täyteen touhuun. Yökyöpeleillä kestää pitkään, ennen kuin he pääsevät aamulla käyntiin. He alkavat olla tehokkaimmillaan vasta iltapäivällä ja illalla. Itseopiskelumateriaali mahdollistaa sen, että jokainen pystyy valitsemaan ihanteellisen oppimisajankohdan itselleen. (Otala 2001, 67–68.)

4 Teoria salausmenetelmistä

Salaisuuksia ja viestejä henkilöiden kesken on ollut kautta aikojen, mutta keinot niiden säilyttämiseen ja lähettämiseen ovat vaihdelleet. Salausta käytetään viestin koodaamiseksi, niin että ainoastaan viestin vastaanottaja voi muuttaa koodin selkokieliseksi tekstiksi. Menetelmät, joita aikanaan käyttivät vain sotilaat ja diplomaatit, ovat tänään osa jokapäiväistä elämää. (Järvinen 2003, 19–20.)

Kryptologia on salauksiin ja niiden purkamiseen erikoistunut tieteenlaji, joka on saanut nimensä kreikan kielen sanoista kryptos (salainen, piilotettu), sekä sanasta logos (sana). Salakirjoitusta kutsutaan kryptografiaksi ja salausten murtamista kryptoanalyysiksi. (Järvinen 2003, 19.)

Englanninkielisessä kirjallisuudessa käytetään nimityksiä Alice, Bob ja Eve. Ne tulivat tutuiksi 1977 julkaistussa RSA- menetelmän kuvauksessa, jonka jälkeen niistä on tullut kryptologian epävirallisia standardeja. Henkilöt Alice ja Bob lähettävät toisilleen viestejä, Eve (tulee sanasta eavesdropper, salakuuntelija) on kiinnostunut viestien sisällöistä ja hänellä on fyysinen pääsy käytettyyn viestikanavaan. Viestien ja tietojen salaamistarpeet voivat olla erilaisia, mutta periaatteet pysyvät samana. (Järvinen 2003, 45.)



Kuva 1: Bob, Alice ja Eve

4.1 Salauksen historia

Tiedon salaaminen ei ole tullut tarpeelliseksi vasta nykyaikana, vaan sillä on jo pitkät perinteet. Ensimmäisiä salakirjoituksen kuvauksia löytyy Herodotoksen historianteoksesta, jossa hän kertoo 400-luvulla eKr sattuneista Kreikan ja Persian välisistä yhteydenotoista, joita hän piti kamppailuna vapauden ja orjavallan välillä. Persian hallitsija Kserksen alkoi salassa koota kaikkien aikojen suurinta armeijaa, jolla hän kostaisi Ateenalle ja Spartalle kokemansa röyhkeyden, koska maat eivät olleen onnitelleet häntä Persepolis - kaupungin rakentamisen aloit-

tamisesta. Armeijan kokoamisen oli kuitenkin huomannut kreikkalainen Demeratos, joka oli karkotettu omasta kotimaastaan ja asuin Persiassa. Karkotuksestaan huolimatta hän oli uskollinen Kreikalle ja halusi varoittaa spartalaisia uhkaavasta vaarasta. (Singh 1999, 20-21.)

Ongelmana hänellä oli kuinka saada viesti perille vaarantamatta itseään. Hän keksi kaivertaa viestinsä kirjoitustauluun, jonka jälkeen hän valoi sulaa vahaa kirjoituksen päälle näin peittäen kirjoituksen. Kirjoituksen ollessa piilossa se ei herättänyt epäluuloa tienvartijoissa matkalla määränpäähänsä. Salakirjoituksen taito pelasti Kreikan joutumasta Persian hallitsijan vallan alle. Näin syntyi ensimmäinen tiedon salausmenetelmä nimeltään steganografia. Sana tulee Kreikan sanoista steganos (peitetty) ja grafein (kirjoittaa). (Singh 1999, 20–22.)

Viestin salaamiseksi käytettiin yksinkertaisesti kätkemistä. Seuraavan kahden vuosituhannen ajan eri muotoja steganografiasta käytettiin ympäri maailmaa. Esimerkkeinä viestin kätkemiselle on kirjoittaa viesti kaljuun päähän ja odottaa hiusten kasvamista. Saavuttua määränpäähän ajellaan pää uudestaan kaljuksi ja viesti tulee näkyviin. Muinaiset kiinalaiset kirjoittivat viestejä hienolle silkille, joka rutistettiin pieneksi palloksi ja peitettiin vahalla. Sitten viestinviejä nielaisi pallon. Myös näkymättömät musteet luetaan steganografian piiriin. (Singh 1999, 22–23.)

Steganografian pitkäikäisyys osoittaa, että se tarjoaa jonkin verran suojaa. Mutta jos viesti löydetään, kuka tahansa voi tulkita salaisen viestin. Siksi samanaikaisesti steganografian kanssa kehittyi kryptografia. Sen tarkoitus ei ole piilottaa itse viestiä vaan sen merkitys. Menetelmää kutsutaan salakirjoittamiseksi. Kun viesti pitää saadaan käsittämättömäksi, se sekoitetaan käyttäen tiettyä järjestelmää, jonka viestin lähettäjä ja vastaanottaja ovat sopineet etukäteen. Vastaanottajan saadessa viestin vain hän pystyy muuttamaan sen selväkieliseksi. Väärän henkilön löytäessä viestin hän ei pysty lukemaan sitä, koska ei tiedä käytettyä sekoitusjärjestelmää. (Singh 1999, 23–24.)

Ensimmäinen sotilaalliseen kryptografiaan käytetty laite on spartalainen scytale, joka on peräisin 400-luvulta eKr. Scytale on puusauva, jonka ympärille on käärityn nahka- tai pergamenttisuikale. Lähettäjä kirjoitti viestin pitkittäin sauvan suuntaan ja kiersi sitten auki suikaleen, jossa näytti vain olevan sarja merkityksettömiä kirjaimia. Viestin viejä otti suikaleen ja käytti sitä joskus vyönä kirjaimet sisäänpäin käännettyinä, kätkeäkseen viestin. Viestin lukemiseksi vastaanottaja vain otti sauvan, jonka halkaisija oli sama kuin lähettäjän sauvalla, ja kääri suikaleen sen ympärille. (Singh 1999, 26–27.)

Kuva 2: Scytale (Oracle ThinkQuest)

Sekoitusjärjestelmän vaihtoehto on korvausjärjestelmä. Yksi menetelmistä on aakkosten järjestäminen sattumanvaraisiksi pareiksi, jonka jälkeen alkuperäisen viestin kaikki kirjaimet korvataan niiden pareilla. Näin viesti ”aika yksinkertaista” kirjoitettaisiin VGJV PJNGSJULZVGNZV. (Singh 1999, 27-28.)

a	d	h	i	k	å	m	o	r	s	u	ö	y	z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
v	x	b	g	j	c	q	ä	l	n	e	f	p	t

Taulukko 1: Korvaussalakirjoitus

Salakirjoitusta kutsutaan nimellä korvaussalakirjoitus, koska selväkielisen tekstin jokainen kirjain korvataan toisella kirjaimella. Ensimmäinen korvaussalakirjoituksen käyttö löytyy Julius Caesarin Gallian sodasta. Korvauksessa roomalaiset kirjaimet korvattiin kreikkalaisilla, minkä ansiosta viholliset eivät ymmärtäneen viestiä. Caesar käytti salakirjoitusta usein, mutta harva käytetyistä koodeista on säilynyt jälkipolville. Kuitenkin Suetoniuksen 100- luvulla jKr. kirjoittaman teoksen ”Rooman keisarien elämänkertoja” ansiosta meillä on yksityiskohtainen kuvaus eräästä Caesarin käyttämästä korvaussalakirjoituksesta. Caesar vaihtoi yksinkertaisesti viestin jokaisen kirjaimen toiseen kirjaimeen, joka on kolme kirjainta eteenpäin aakkosissa. Kryptografian asiantuntijat puhuvat usein selväkielen aakkosista, eli aakkosista joilla alkuperäinen viesti on kirjoitettu, sekä koodiaakkosista eli kirjaimista jotka on vaihdettu selväkielen kirjainten paikalle. Tätä korvausta kutsutaan usein Caesarin siirtosalakirjoitukseksi tai vain Caesarin salakirjoitukseksi. Korvaussalakirjoitukseksi sanotaan mitä tahansa korvausta, jossa kirjaimet on vaihdettu toisiin kirjaimiin tai symboleihin. (Singh 1999, 28–30.)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	å	ä	ö
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C

Taulukko 2: Ceasarin salakirjoitus

1900-luvulla tilanne alkoi muuttua, kun alettiin laajemmin käyttää radioaaltoja kommunikointiin. Radioaalloilla viestin levitessä kaikille, jotka olivat kuulolla, sen sisältö oli pakko koodata niin turvalliseksi, ettei viestin kuullut ulkopuolinen voinut ymmärtää sitä. Niinpä alettiin kehittää uusia menetelmiä ja tekniikoita viestien salaamiseksi. On puhuttu toisen maailmansodan olleen merkittävin yksittäinen tekijä salaustekniikan kehittymisessä eteenpäin. (Järvinen 2003, 21.)

Toisen maailmansodan kuuluisin salauskone oli saksalaisten käyttämä Enigma, jolla oli merkittävä vaikutus saksalaisen sodan alkumenestykseen, mutta myös sen loppuvaiheen häviöön. Enigma oli kirjoituskonetta muistuttava laite, jonka näppäimistöltä syötetyt merkit kulkivat sähköisesti kolmen roottorin läpi. Aina kun yksi merkki oli koodattu, roottori pyörähti eteenpäin ja tehtyään täyden kierroksen se siirsi seuraavaa roottoria yhdellä askeleella. Käyttöä varten osapuolilla piti olla hallussaan koodikirja, jossa lueteltiin päivittäin vaihtuvat roottorien alkuasetukset neljän viikon ajalle. Turvallisuuden lisäämiseksi koodikirjan ilmoittamia alkuarvoja käytettiin vain kyseisenä päivänä sanomakohtaisten avainten välittämiseen. Niissä lähettäjä määritteli itse seuraavan viestin käyttämät roottorien lähtöarvot, jotka ilmaistiin kolmena kirjaimena. (Järvinen 2003, 21-22.)

Kuva 3:Enigma (MBnet.)

Englannin sotilastiedustelun yksikkö Bletchley Parkissa onnistui kehittämään menetelmiä ja laitteita, jotka mahdollistivat avainten etsintää ja salattujen viestien purkamista. Todellinen Enigman murto onnistui kuitenkin vasta, kun englantilaiset olivat onnistuneet kaappaaman käytössä olleen koodikirjan. Enigman kaltaiset mekaaniset salauskoneet säilyivät joissakin maissa käytössä aina 1990-luvulle asti. (Järvinen 2003, 23-24.)

Suurin muutos alkoi 1970-luvulla, kun kansainvälinen rahaliikenne siirtyi sähköiseen muotoon ja tarvittiin keinoja, joilla rahasiirrot voitiin tehdä turvallisesti pitkienkin välimatkojen päähän. IBM:n ratkaisu pankkien tiedonsalausongelmiin oli DES- salausmenetelmä. DES levisi nopeasti ympäri maailmaa ja lopulta myös pankkimaailman ulkopuolelle. Erikoisinta DES:issä oli, että sen toimintaperiaate julkistettiin armeijan kovasta vastustuksesta huolimatta. Armeijan kannalta oli eduksi, ettei ulkopuolinen tiennyt salausmenetelmän toimintaa, mutta tietoliikenteen yhteensopivuus edellytti standardeja. Tietotekniikka alkoi liittyä yhä kiinteämmin salaukseen ja niille olikin kova kaupallinen kysyntä erilaisissa palveluissa. Internet ja langaton matkaviestintä räjäyttivät pankin lopullisesti 1990-luvun puolivälissä. (Järvinen 2003, 24-25.)

4.2 Salausmenetelmät

Salausmenetelmillä pyritään varmistamaan tietojen luottamuksellisuus, eheys ja kiistämättömyys. Riippumatta siitä, mihin salausta käytetään, tavoitteena tulisi olla salaus, jonka murtaminen kohtuullisessa ajassa ja kohtuullisin resurssein ei ole mahdollista. Kaikki salaukset

ovat murrettavissa. On kyse vain siitä, paljonko aikaa ja tietokonetehoa tarvitaan. (Salausmenetelmät 2009; Järvinen 2003, 79.)

Salaustekniikat pohjautuvat joko tietokoneella tapahtuvaan bittien sekoittamiseen (symmetriset salaukset) tai matemaattiseen laskentaan (epäsymmetriset salaukset). Symmetrisessä tekniikassa käytetään samaa avainta sekä viestin salaukseen että salauksen purkuun, kun taas epäsymmetrisessä käytetään eri avaimia: yhtä avainta (public key) viestin salaukseen ja toista (private key) viestin purkamiseen. (Järvinen 2003, 78.; Salausmenetelmät 2009.)

Salausmenetelmät jakaantuvat kahteen pääluokkaan: jonosalaukseen (stream cipher) ja lohkosalaukseen (block cipher). Jonosalauksessa salataan yleensä merkki kerrallaan, kun taas lohkosalauksessa teksti salataan lohkoina (block). Lohkosalausta käytetään yleisimmissä symmetrisissä ja epäsymmetrisissä salausalgoritmeissa. (Salausmenetelmät 2009.)

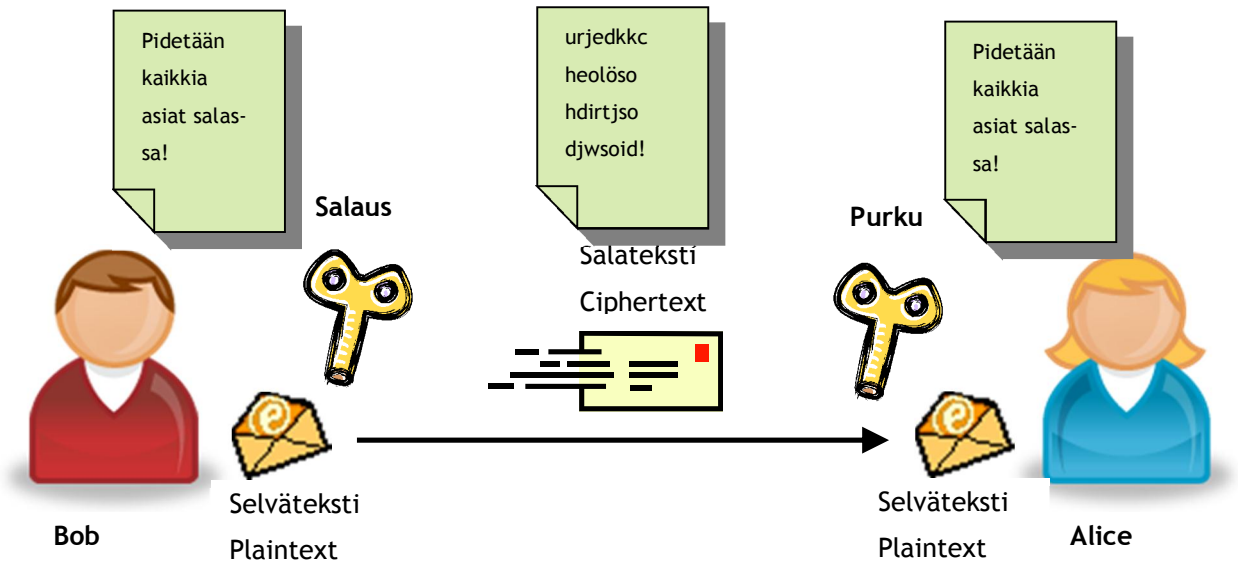
4.2.1 Vahva salaus

1980-luvulla pidettiin yli 40 bitin salausta vahvana, koska salauksen purkamiseen olisi tarvittu supertietokoneita, joiden käyttö ei ollut mahdollista. Tietokoneiden kehittyessä ja 1990-luvulle tultaessa supertietokoneen laskentateho oli kenen tahansa ulottuvilla, ja niin jouduttiin vahvan salauksen rajaa nostamaan 56 bittiin ja myöhemmin 64 bittiin asti. Koska jokainen uusi bitti avaimeen kaksinkertaistaa vaihtoehtojen määrän, 64-bittisen salauksen murtaminen kestää 2^{24} eli 16 777 216 kertaa kauemmin kuin 40-bittisen salauksen murtaminen. (Järvinen 2003, 83–84.)

Verrataan vielä 40- ja 128-bittisen salauksen murtamista käytännössä. Jos käytössä on miljoona avainta sekunnissa kokeileva tietokone, 40 bitin avainmahdollisuudet on käyty läpi vajaassa kahdessa viikossa. Kun käytetään 128-bittistä salausta ja käytössä on miljardi tietokonetta, joista jokainen kokeilee miljardi avainta sekunnissa, avainmahdollisuuksien läpikäynti kestää enemmän kuin maailmakaikkeudella on ikää. Jos 40-bittisen salauksen murtamiseen tarvittavaa laskentatehoa kuvataan yhdellä lusikallisella hiekkaa, 128-bittisen salauksen murtamiseen tarvitaan kolme kokonaista maapalloa. (Järvinen 2003, 84–85.)

4.3 Symmetrinen salaus

Symmetrisessä salauksessa lähettäjällä ja viestin vastaanottajalla on käytössä sama salausavain, jonka he ovat etukäteen sopineet. Ongelmaksi tulee salausavaimen sopiminen niin, ettei kukaan ulkopuolinen saa tietoonsa käytettävää avainta, joka mahdollistaisi viestien salauksen purkamisen. Alapuolella olevassa kuvassa on selitetty symmetrisen salauksen periaate.



Kuva 4: Symmetrinen salaus

Symmetrisellä salauksella tarkoitetaan tietokoneella tapahtuvaa bittien sekoittamista. Claude Shannon esitti 1940-luvulla ajatuksen siitä, miten hyvän salaimen tulisi toimia. Hyvän salaimen tulee sotkea selväkielisen ja salakirjoituksen välinen yhteys niin, ettei niiden välistä yhteyttä voi päätellä. Lisäksi salaimen pitää hajottaa selvätekstin vaikutus mahdollisimman laajalle salatekstiin niin, että pienikin muutos selvätekstiin tekee suuren muutoksen salatekstiin. Hajautus peittää toistot ja säännönmukaisuudet, jolloin salatekstin analyysi ei auta murtajaa. Symmetriset salaimet voidaan jakaa edelleen kahteen ryhmään: lohko- ja jonosalaimiin. (Järvinen 2003, 77–78.)

Lohkosalain käsittelee tekstiä nimensä mukaisesti lohkoina, jotka salataan aina samalla avaimella. Tyypillisiä lohkon kokoja ovat 64 ja 128 bittiä. Jonosalain käsittelee tekstiä pienissä yksiköissä, bitti tai merkki kerrallaan, mutta avain vaihtuu jokaisen yksittäisen salausoperaation jälkeen. Varsinainen salaus tapahtuu yhdistämällä sen hetkinen avain ja selväteksti yksinkertaisella XOR-operaatiolla salatekstiksi. Operaatio tuottaa avainjonon, johon tarvitaan algoritmi, joka alustetaan osapuolten valitsemalla salausavaimella. Sen jälkeen algoritmi tuottaa jatkuvasti uusia avaimia, joita salaus käyttää.

4.3.1 Käytetyimmät symmetriset salausjärjestelmät

DES (Data Encryption Standard) syntyi, kun IBM:n tutkijat alkoivat 1970-luvulla kehittää kaupallista salausohjelmaa pankeille. Pohjaksi otettiin tutkija Horst Feistelin kehittämä 128-bittinen Lucifer-algoritmi. DES:n avaimen pituus lyhennettiin 64 bittiin, jotta salaustekniikka saatiin mahtumaan yhdelle piirille ja toimimaan nopeammin. IBM halusi olla varma salausohjelman turvallisuudesta, joten sitä kehitettiin yhteistyössä NSA:n (National Security Agency) kanssa. DES valmistui lopullisesti vuonna 1975, jolloin myös sen määritys julkistettiin. DES:n avainpituudeksi tuli 56 bittiä NSA:n aloitteesta. NSA pidätti itsellään mahdollisuuden salauksen murtamiseen, koska ilmeisesti 64-bittistä avainta ei ollut vielä mahdollista heidänkään murtaa. Pari vuotta myöhemmin DES - järjestelmästä tuli Yhdysvaltojen virallinen salausstandardi. (Järvinen 2003, 87–88.)

Itse DES-algoritmista ei ole lukuisista yrityksistä huolimatta löytynyt vakavia puutteita, jotka heikentäisivät sen luotettavuutta. Sen sijaan ongelmana on DES:n käyttämä 56-bittinen avain, joka on niin lyhyt, että se on mahdollista murtaa nykyisin käytössä olevilla laitteilla varsin nopeasti käyttäen brute force menetelmää, eli kaikkien mahdollisten avainten kokeilua yksi kerrallaan. Nykyisillä tietokoneilla murtaminen on varsin nopeaa. DES:n turva riittää kotikäyttöön, mutta ei mihinkään tärkeämpään. 3DES menetelmässä käytetään kolmea DES:iä peräkkäin, jolloin avaimen pituutta saadaan kasvatettua (3 x 56) 168 bittiin. Haittapuolena on, että 3DES on lähes kolme kertaa hitaampi kuin DES. (Järvinen 2003, 93–95.)

AES (Advanced encryption standard) on vuonna 2001 avoimen kansainvälisen kilpailun voittanut Rijndael-salausmenetelmä. Avaimen pituus voi olla mikä tahansa 32:n monikerta ja lohkon koko on 128 bittiä. AES:ssa on käytössä vain yksi 256 alkion S-laatikko, mikä tekee siitä elegantin ja nopean. Menetelmä on kuitenkin niin uusi, ettei sen kaikkia heikkouksia vielä tunneta. AES hyväksyttiin myös Yhdysvaltojen viralliseksi salausstandardiksi vuonna 2001. (Järvinen 2003, 96.)

IDEA (International Data Encryption algorithm) on Xuejia Lain ja James Masseyn Sveitsissä kehittämä salausmenetelmä, joka käyttää 128- bittistä avainta. Salainta pidetään erittäin turvallisena, mutta hitaana. Menetelmän patentin omistaa sveitsiläinen Ascom, mikä rajoittaa sen käyttöä. Ascom on kuitenkin antanut joustavasti lupia menetelmän käyttöön ei-kaupallisissa ohjelmissa. IDEA on PGP- ohjelman oletussalain. (Järvinen 2003, 97–98.)

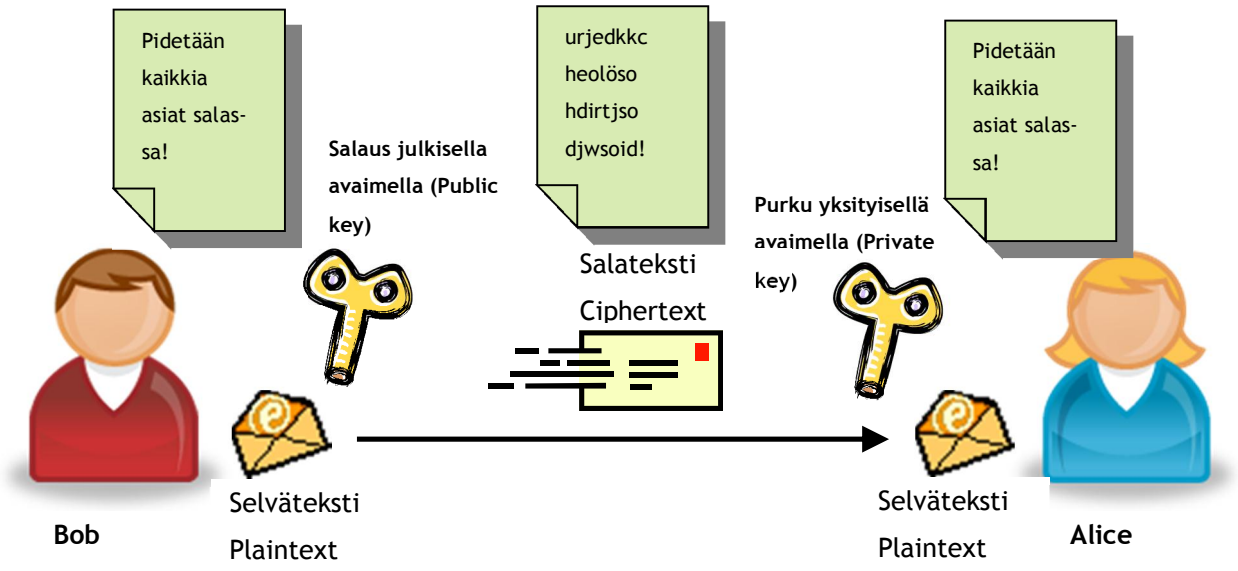
Muita käytettyjä symmetrisiä salaimia ovat: Serpent, Twofish, RC6, MARS, Blowfish, CAST, FEAL, GOST, LOKI, RC2, RC4, RC5, Safer, SEAL, Skipjack ja SOBER.

4.4 Epäsymmetrinen (asymmetrinen) salaus

Tuhansien vuosien ajan salaustekniikat perustuivat lähettäjän ja vastaanottajan yhteiseen salaisuuteen (symmetrinen salaus). Tietokoneiden yleistyminen mahdollisti uudentyyppisen tekniikan, jossa salaukseen ja purkamiseen käytetään eri avaimia. Epäsymmetrisessä salauksessa on siis kaksi eri avainta, julkinen (public key) ja yksityinen (private key) avain. Salausavaimet ovat erilaisia, mutta silti yhteydessä toisiinsa matemaattisella tavalla, jota ulkopuolisen on käytännössä mahdotonta keksiä. (Järvinen 2003, 131–132.)

Julkista avainta voi levittää vapaasti, yleensä se laitetaankin henkilökohtaiselle www-sivustolle tai yleiseen hakemistoon. Koska sitä käytetään vain salaukseen, sen paljastamista ei tarvitse pelätä. Yksityistä avainta pitää sen sijaan varjella kuten mitä tahansa salaisuutta. Jos yksityinen avain paljastuu, on julkisen avaimen järjestelmä yhtä haavoittuva kuin perinteinenkin salaus. (Järvinen 2003, 132.)

Se, mitä julkisella avaimella on salattu, voidaan purkaa vain vastaavalla yksityisellä avaimella. Edes lähettäjä ei pysty purkamaan koodattua viestiä. Tästä syystä, jos lähettäjä haluaa säilyttää alkuperäisen viestin, täytyy siitä tehdä kopio ennen salausta. Julkisen avaimen järjestelmä poistaa ongelman, joka perinteisissä salauksissa on. Koska yhteistä salaisuutta ei vaadita, avaimesta sopiminen on pelkkä ilmoitusasia. (Järvinen 2003,132–133.)



Kuva 5: Epäsymmetrinen salaus

Bob lähettää sähköpostin Alicelle, jonka hän salaa käyttäen Alicen julkista avainta. Avaimen hän on saanut Alicen kotisivulta. Alice vastaanottaa viestin ja purkaa salauksen käyttäen omaa yksityistä avainta.

4.4.1 Epäsymmetrisen salauksen rajoitukset

Epäsymmetrisen avaimen tekniikka ei kuitenkaan ole täydellinen, vaikka järjestelmä on toimiva ja monipuolinen. Seuraavassa käydään läpi muutamia sen rajoituksia. (Järvinen 2003, 134.)

Epäsymmetrinen salaus tarvitsee huomattavasti pidemmät avaimet kuin symmetrisen avaimen tekniikka. Pidempi avain vie enemmän tilaa ja on hankalampi käsitellä. Jopa useisiin tuhansiin bitteihin venyvän avaimen muistaminen on hankalaa, joten käyttöön tarvitaan fyysinen laite tai tiedosto, joka sitten suojataan symmetrisellä salauksella. (Järvinen 2003, 134.)

Epäsymmetriset menetelmät pohjautuvat matematiikkaan, RSA - lukujen jakamiseen tekijöihin. Riittävän nopeaa tekijöihin jakoa ei tällä hetkellä tunneta, mutta ei voida myöskään todistaa, ettei sellaista olisi. Pahimmassa tapauksessa löydetään nopea ja toimiva menetelmä, ja silloin RSA:ta käyttävät ohjelmat, laitteet ja palvelut joudutaan korvaamaan toisella tekniikalla. (Järvinen 2003, 135.)

Epäsymmetrisissä salauksissa lasketaan suurilla luvuilla, mikä tekee siitä erittäin hitaan menetelmän. Jos verrataan symmetrisen menetelmän DES- salausta epäsymmetrisen RSA- salausalgoritmiin, niin RSA- menetelmä on noin sata kertaa hitaampi. Aineisto, jonka salaaminen DES:llä kestää 10 sekuntia, kestäisi RSA:lla salattuna vajaat 17 minuuttia. (Järvinen 2003, 135.)

Forward search-hyökkäys on mahdollinen, koska salaviesti ja käytetty julkinen avain tiedetään. Esimerkki kyseisestä hyökkäyksestä: Alice lähettää Bobille lyhyen viestin, jonka hän salaa käyttäen Bobin julkista avainta. Eve kaappaa salatun viestin ja alkaa testailla erilaisilla selväteksteillä, mikä niistä Bobin julkisella avaimella salattuna tuottaisi saman salatekstin. Jos tulos täsmää, Eve tietää vastaavan selvä tekstin. Viestin on kuitenkin oltava lyhyt tai siitä tulee tietää suurin osa. Silloinkin kokeiltavien vaihtoehtojen määrä kasvaa epäkäytännöllisen suureksi ja vie paljon aikaa, koska Eve joutuu testimielessä salaamaan jokaisen kokeilemansa vaihtoehdon. (Järvinen 2003, 135–136.)

Julkisen avaimen järjestelmä ei kuitenkaan takaa että lähettäjä on oikeasti Alice. Bobin on esimerkiksi tavattava Alice henkilökohtaisesti ja vaihdettava julkisia avaimia ensimmäisellä

kerralla. Näin toimiessa luottamusta voidaan siirtää tulevaisuudessa eteenpäin, kun Bob lähettää uuden julkisen avaimen Alicelle koodattuna yksityisellä avaimella allekirjoitettuna. (Järvinen 2003, 136.)

4.4.2 Käytetyimmät epäsymmetriset salausjärjestelmät

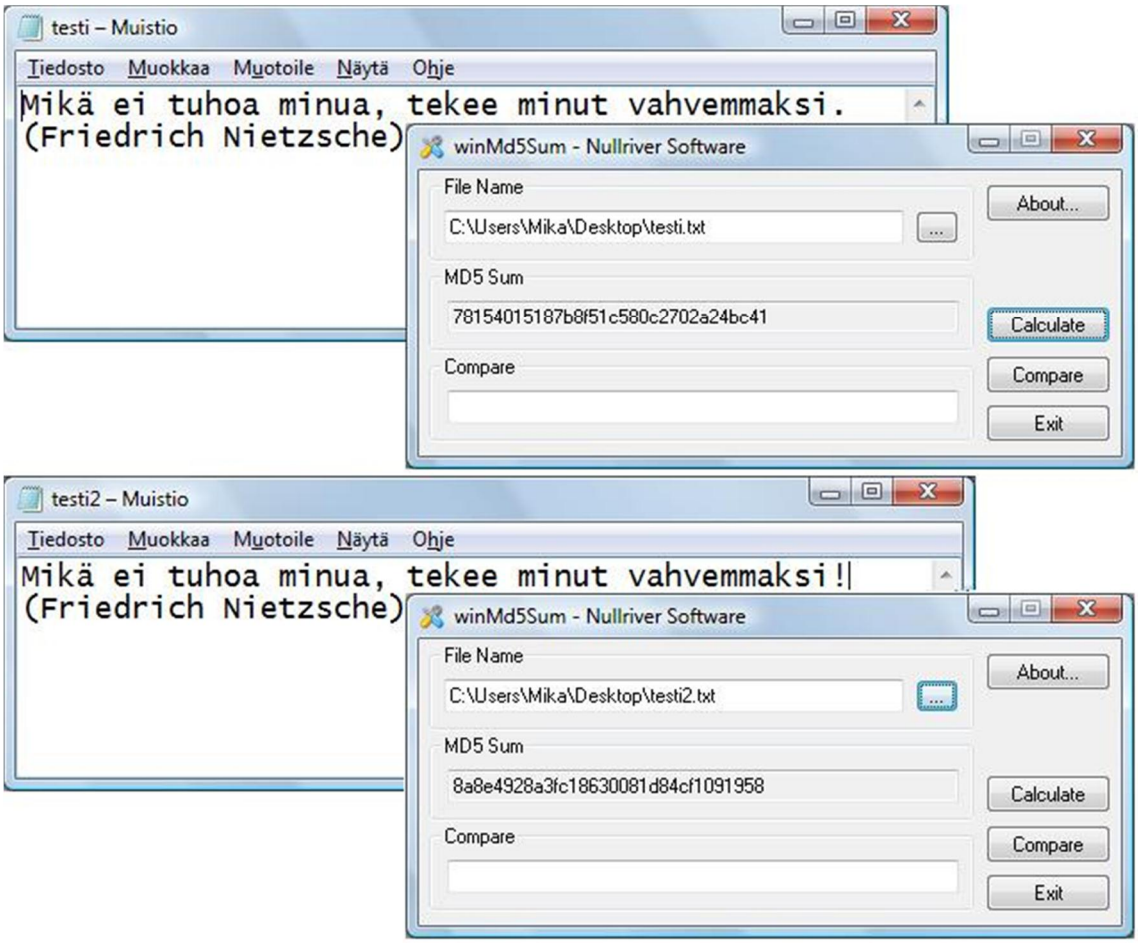
RSA (Rivest, Shamir, Adleman) on vuonna 1977 kolmen nuoren matemaatikon kehittämä salausalgoritmi, mikä perustuu suuriin alkulukuihin, eli lukuihin jotka ovat jaollisia ykkösellä ja itsellään. Nimi on johdettu heidän sukunimiensä alkukirjaimista (Rivest, Sharmir, Adleman) ja on suosituin epäsymmetristä salausta käyttävä menetelmä. RSA- menetelmässä julkinen ja yksityinen avain ovat symmetrisiä eli ne toimivat molempiin suuntiin, joten menetelmä mahdollistaa epäsymmetrisen salauksen ja digitaalisen allekirjoituksen. (Järvinen 2003, 131–140.)

Digitaalisessa allekirjoituksessa lähettäjä koodaa viestinsä omalla yksityisellä avaimellaan ja vastaanottaja (tai kuka tahansa, joka on saanut tietoonsa lähettäjän julkisen avaimen) purkaa jälleen viestin käyttäen lähettäjän julkista avainta. Jos viesti purkautuu selkeään muotoon, voidaan olla vakuuttuneita viestin lähettäjästä. (Järvinen 2003, 154–155.)

Elliptiset käyrät (ECC, Elliptic curve cryptography) kehitettiin 1980-luvun puolivälissä. Mikäli nopea tekijöihin jako keksitään ja RSA:sta joudutaan luopumaan, ECC on sen todennäköinen seuraaja. (Järvinen 2003, 153.)

4.5 Tiivistealgoritmit

Tiivistefunktion (hash) avulla lasketaan mielivaltaisen pitkästä ryhmästä bittejä (esim. tiedosta ja sähköpostiviesti) lyhyt vakiopituinen tiivistearvo (hash value). Tiiviste on yksisuuntainen funktio, ja sitä ei voi ajaa takaperin. Jos ulostullut arvo tiedetään, ei voida mitenkään päätellä, minkälainen syöte ne on tuottanut. Hyvä tiivistefunktio ei tuota samanlaista tiivistettä eri syötteillä; yhdenkin bitin muuttuminen syötteessä aiheuttaa myös suuren muutoksen saadussa tiivistearvossa. (Järvinen 2003, 122–124.)



Kuva 6: Hash value esimerkki.

Koska tiiviste yksilöi sille syötetyn bittijonon, tiivistettä kutsutaan myös bittijoukon sormenjäljeksi (fingerprint). Vaikka bittijoukkoa ei nähtäisi, sormenjäljen perusteella tiedetään, mikä joukko on ollut asialla. Tiivistefunktioita käytetään apuna viestien digitaalisessa allekirjoittamisessa sekä käyttöjärjestelmien salasanojen tallentamisessa. Tiivistefunktioista käytetään myös nimitystä yksisuuntaiset funktiot tai hajautusfunktiot. (Järvinen 2003, 122; Salausmenetelmät 2009.)

4.5.1 Tiivisteiden käyttömuotoja

Digitaalisessa allekirjoituksessa lähettäjä laskee lähetettävästä viestistä tiivisteen, jonka hän salaa yksityisellä avaimellaan. Vastaanottaja avaa salatun tiivisteen lähettäjän julkisella avaimella, laskee itse viestistä tiivisteen ja vertaa sitä lähettäjän julkisella avaimella avaamaansa tiivisteeseen. Jos tiivisteet ovat samat, on viesti todistettavasti allekirjoitettu lähettäjän yksityisellä avaimella eikä kukaan ole muuttanut viestiä matkalla. Eheyden lisäksi varmistuu lähettäjän henkilöllisyys. (Salausmenetelmät 2009.)

Tiivisteillä voidaan varmistua tietokoneella olevien ohjelmien ja www-sivuilta ladattavien ohjelmien muuttumattomuudesta. Kiintolevyn ohjelmatiedostoista voidaan laskea heti asennuksen jälkeen tiivisteet, jotka tallennetaan suojattuun tietokantaan. Tiivisteet lasketaan uudelleen myöhemmin ja niitä verrataan tietokannassa oleviin arvoihin, ja näin nähdään heti, mikäli jokin tiedosto on muuttunut. Mahdolliset muutokset saattavat johtua ohjelmaan tarttuneesta viruksesta. Ladatessa www-sivuilta ohjelmia, varsinkin avoimen lähdekoodin ohjelmia, käyttäjä voi varmistaa ohjelmien kehittäjien kotisivulta tiivistearvon varmistuakseen ohjelman olevan aito ja varmasti uusin versio. (Järvinen 2003, 125–127.)

Salasanoja voidaan ajaa tiivistefunktion läpi, jolloin salasana muuttuu kiinteämittaiseksi arvoksi, jota voidaan käyttää avaimena. Käyttäjien salasanojen pituudet vaihtelevat, mutta avaimeksi tarvitaan tasan 64, 128 tai 256 bittiä. Jos saadussa tiivistearvossa on liikaa bittejä, niistä käytetään esimerkiksi 64 ensimmäistä. Tiivistearvosta ei voi enää päätellä, mikä oli alkuperäinen salasana. (Järvinen 2003, 125–127.)

4.5.2 Yleisesti käytettyjä tiivistefunktioita

SHA-1 (Secure Hash Algorithm 1) on NSA:n kehittämä ja NIST:in (National Institute of Standards and Technology) standardoima tiivistefunktio, joka tuottaa 160-bittisen tiivisteen. Käytetään muun muassa PGP:ssä (Pretty Good Privacy, sähköpostin salaus) ja SSH:ssa (Secure Shell, pääteyhteyksien salaus). (Järvinen 2003, 123–124.)

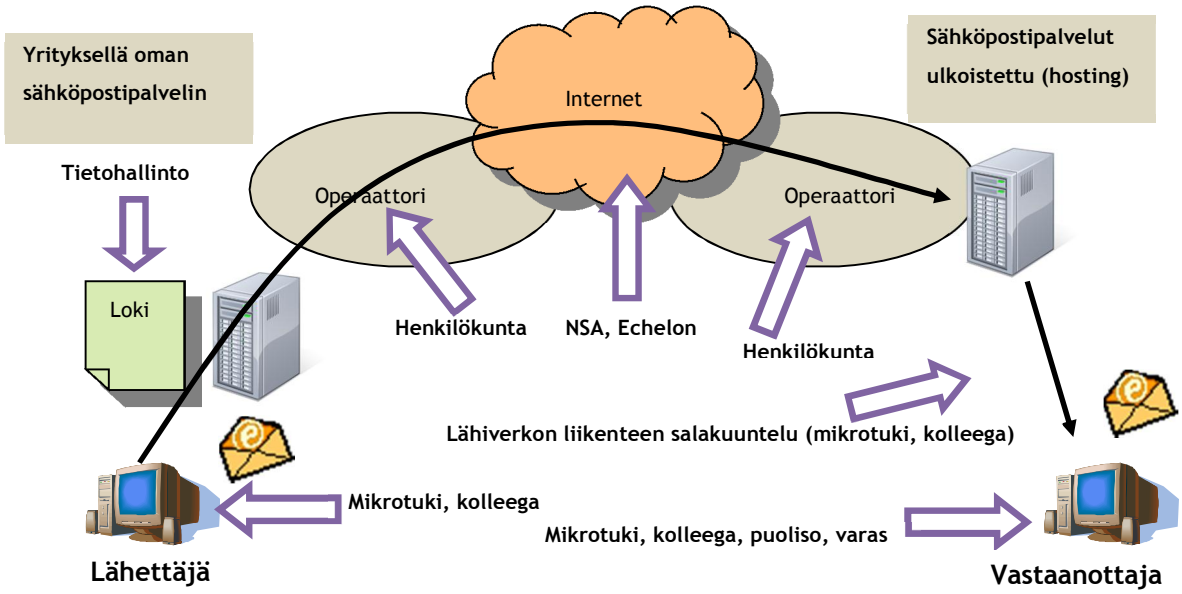
MD5 (Message-Digest algorithm 5) on Ron Rivestin vuonna 1991 kehittämä tiivistefunktio, joka tuottaa 128- bittisen (16 tavua) tiivisteen. (Järvinen 2003, 123.)

SHA-256 ja SHA-512:sta käytettään useimmiten yhteisnimitystä SHA-2 ja on SHA-1 paranneltuja versioita. SHA-256 tuottaa 256 bittisen (32 tavua) tiivistearvon ja SHA-512 tuottaa 512 bittisen (64 tavua) tiivistearvon. Pidemmät tiivistearvot ovat tarpeen AES:ää ja muita vähintään 256-bittistä avainta käyttäviä salaimia varten. (Järvinen 2003, 124.)

4.6 Sähköpostin salaaminen

Perinteisessä sähköpostiliikenteessä ei käytetä minkäänlaista salausta. Viestit ovat siis periaatteessa kenen tahansa luettavissa verkossa. Salaamatonta sähköpostiviestiä voidaan verrata postikorttiin ilman kirjekuorta. Postikortissa olevan viestin voi lukea kuka tahansa korttia käsittelevä henkilö: postinkantaja, postin lajittelija tai kuka tahansa ohikulkija. Samoin salaamaton sähköpostiviesti on kaikkien niiden luettavissa, jotka pystyvät kuuntelemaan viestin välitykseen käytettävän verkon liikennettä. Jos sähköposti salakirjoitetaan, viestin turvallisuus voidaan rinnastaa postikorttiin, joka on kirjekuoressa. (Järvinen 2003, 249–250.)

Sähköpostiviestinnän luottamuksellisuus voidaan varmistaa salaamalla viesti ennen sen lähettämistä. Lisäksi sähköpostiviesti voidaan allekirjoittaa digitaalisesti, jolloin voidaan varmistua viestin lähettäjän henkilöllisyydestä sekä viestin välittymisestä lähettäjältä vastaanottajalle muuttumattomana (viestin eheys). Jotta henkilöllisyys voidaan varmistaa luotettavasti, tulee käyttää varmenteisiin perustuvia allekirjoitusmenetelmiä. (Sähköpostin tietoturva 2007.)



Kuva 7: Sähköpostin kulku, jossa viestintäsalaisuus voi vaarantua

4.6.1 Kriittisiä kohtia sähköpostin liikkumisessa

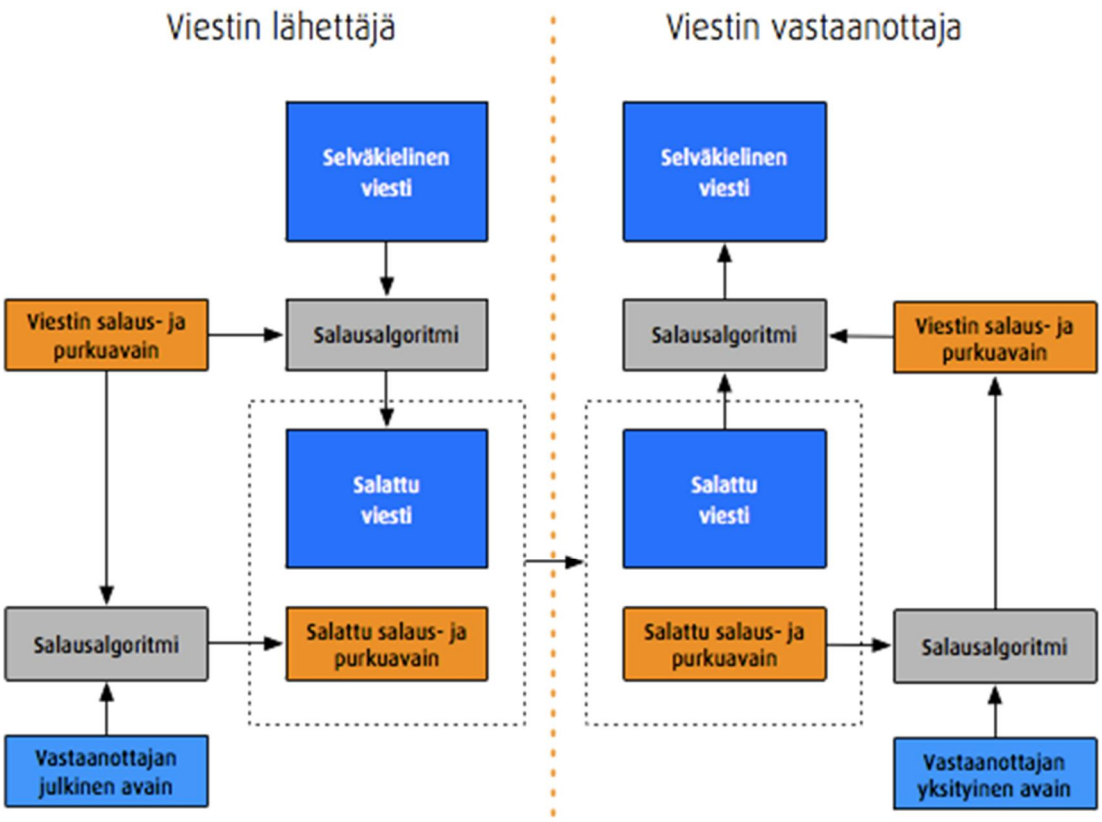
Jos lähettäjän/vastaanottajan tietokone ja sähköpostiohjelma jää auki, kuka tahansa koneelle tuleva henkilö voi katsoa lähetetyt ja vastaanotetut viestit. Kone saatetaan varastaa tai tunkeutua verkon läpi, jolloin salaamattomat viestit ovat helposti luettavissa. Lähettäjän ja vastaanottajan kone on yleensä organisaation lähiverkossa, jolloin verkon liikenne on kaikkien muiden työasemien nähtävissä. Sopivalla analysaattoriohjelmalla liikenteestä on helppo poimia sähköpostiviesteiltä näyttävät tekstit lukemista varten. Posti lähtee ja saapuu yhden koneen kautta. Toisen kriittisen pisteen muodostaa organisaation palomuuri, joka asennuksesta riippuen saattaa kirjata ylös myös sähköpostiliikenteen tiedot. Sähköpostipalvelimen tai palomuurin ylläpitohenkilöt voivat nähdä tiedot kaikista viesteistä jopa sisältöineen, jos lokiasetukset on tehty sopivasti. (Järvinen 2003, 253–254.)

Sekä lähettäjän että vastaanottajan oma operaattori näkee kaiken asiakkaalle menevän ja sieltä tulevan liikenteen. On teknisesti mahdollista, että joku seuraa viestejä. Viesti on parhaimmassa turvassa liikkuessaan miljoonien muiden viestien seassa kansainvälisten operaatto-

reiden runkoverkossa. Sieltä yksittäisen viestin nappaamiseen pystyy korkeintaan NSA tai vastaava valtiollinen tiedustelupalvelu. (Järvinen 2003, 253–254.)

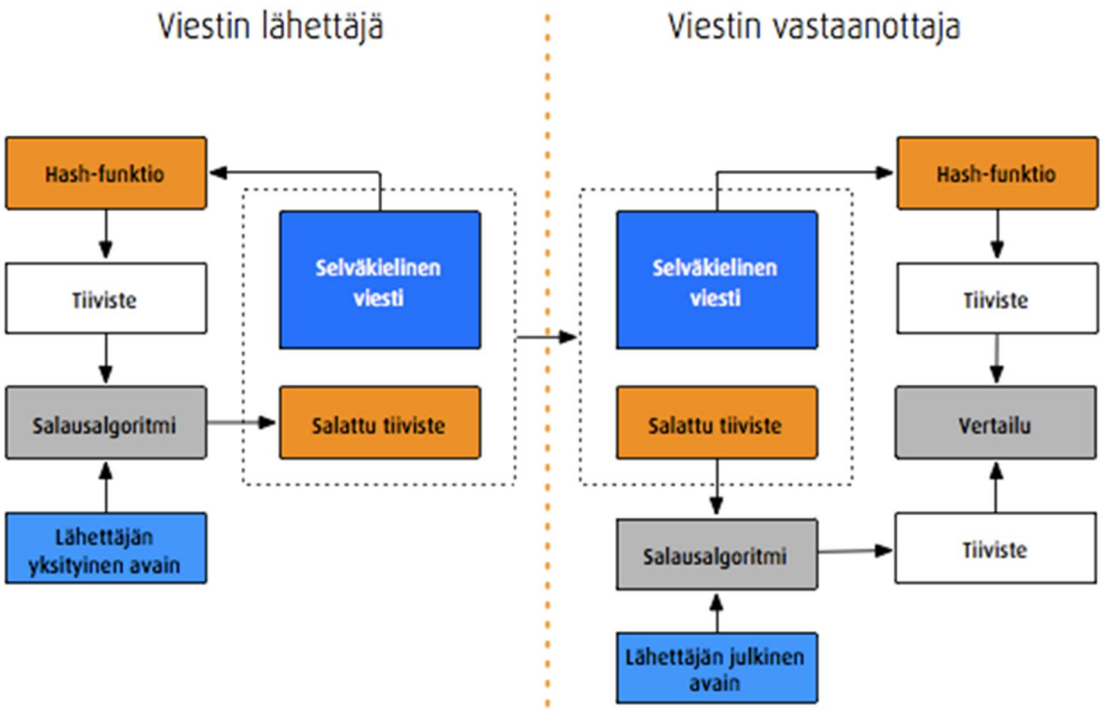
4.6.2 PGP (Pretty Good Privacy)

PGP (Pretty Good Privacy) on Phil Zimmermanin vuonna 1991 ohjelmoima julkisen avaimen salaukseen perustuva salakirjoitusohjelma, joka toi vahvan salauksen kaikkien käyttäjien ulottuville ilmaiseksi. PGP:llä voidaan salata sekä symmetrisillä että epäsymmetrisillä tekniikoilla. Ohjelman käyttöliittymä on graafinen ja suhteellisen helppokäyttöinen. (Järvinen 2003, 287–289.)



Kuva 8: Salaus (Viestintävirasto)

PGP on yleisin sähköpostin salaamiseen käytetty menetelmä ja monet sähköpostiohjelmat tukevat sen käyttöä. Sillä käyttäjä voi suojata tiedostojaan sekä lähettää ja vastaanottaa luottamuksellisia sähköpostiviestejä ja niiden liitteitä. Tiedostot ja sähköpostit voidaan halutessa varmentaa sähköisellä allekirjoituksella. (Singh 1999, 399–402.)



Kuva 9: Sähköinen allekirjoitus (Viestintävirasto)

5 Internetpohjainen koulutuspaketti

Valmis tuotos on internetsivusto, joka toimitetaan ammattikorkeakoululle cd-levyllä. Näin tuotos on helppo sijoittaa haluamaansa verkkoon ja mahdollistaa tulevaisuuden kehittämisen. Sivusto pitää sisällään teorian salausmenetelmistä ja niihin liittyviä harjoitustehtäviä, jotka opiskelija palauttaa opettajalle salatussa sähköpostissa.

Tehtävät ovat erilaisiin salausmenetelmiin liittyviä pähkinöitä, joilla voi testata salausmenetelmiä menneiden aikojen menetelmistä nykyaikaisiin. Tarkoitus on muuttaa työssä läpi käyty teoria käytännöksi erityyppisillä tehtävillä. Olen päätynyt käytettäviin tehtäviin, koska tutustuessani itse aiheeseen koin hyödylliseksi testata lukemaani ja sitä miten voisin hyödyntää tietoa omassa elämässäni. Tehtävät eivät ole hankalia, mutta pystyäkseen tekemään ne pitää ymmärtää ja sisäistää niissä käytettävien menetelmien toiminta. Opiskelijan täytyy osata hakea tietoa myös muista lähteistä suoriutuakseen tehtävistä ja syventääkseen osaamistaan. Tehtävät antavat mahdollisuuden soveltaa opittua tietoa salausmenetelmistä käytäntöön, sekä haastavat opiskelijan hakemaan lisätietoa ja oppimaan aiheesta uutta.

6 Johtopäätökset ja oman työn arviointi

Mielestäni onnistuin työssäni ratkaisemaan ongelman, eli tuottamaan tiivistetyn itseopiskelunpaketin harjoitustehtävineen, mistä pystyy oppimaan perusteet salausmenetelmistä pintaa

syvemmältä. Aloittaessa työtäni en tiennyt mitään salausmenetelmistä, joten tekeminen on ollut uuden oppimista myös itselleni. Täytyy myöntää kiinnostukseni heränneen kyseistä tieteenalaa kohtaan, ja mielenkiintoista on seurata, miten salausmenetelmät tulevat kehittymään tulevaisuudessa teknologian kehittyessä. Salaukset ja niiden purkaminen tulevat aina olemaan kissa ja hiiri- leikkiä hyvän ja pahan välillä.

Kun keräsin tietoa ja lähdemateriaalia salausmenetelmistä, niin englanninkielisissä lähteissä käytettiin lähteenä tai viitattiin aina Simon Singhin vuonna 1999 julkaistuun ” The Code Book” - kirjaan ja suomenkielisessä materiaalissa vastaavasti viitattiin useasti Petteri Järvisen vuonna 2003 julkaistuun ”Salausmenetelmät” – kirjaan. Työssäni oli luontaisinta käyttää kahden tunnetun kirjoittajan materiaalina lähteenä. Kirjat toimivat pääasiallisina lähteinä työssäni. Muuta tukevaa materiaalia löytyi sähköisistä lähteistä.

Työn arviointi on hankalaa, koska käytännön testaaminen, joka olisi paras mittari, suoritetaan vasta myöhemmin syksyllä. Opiskelijoiden tulevasta palautteesta työtä pystyy kehittämään tulevaisuudessa paremmaksi kokonaisuudeksi, koska on mahdollista, etten ole osannut painottaa tarpeeksi olennaisia ja tärkeitä asioita. Yritin selittää teorian mahdollisimman yksinkertaisesti, jotta asiat olisivat helposti ymmärrettävissä. Toivon kuitenkin herättäväni työlläni opiskelijoiden mielenkiinnon salausmenetelmiin, niin että he mahdollisesti haluavat etsiä vielä lisää tietoa pintaa syvemmältä.

Lähteet

Kirjallisuuslähteet:

Järvinen, P. 2003. Salaus-menetelmät. Porvoo: Docendo Finland Oy.

Kajanto, A. (toim.) 1993. Aikuisten oppimisen uudet muodot. Helsinki: Kirjastopalvelu Oy Helsinki.

Keränen, V. & Penttinen, J. 2007. Verkko-oppimateriaalin tuottajan opas. Porvoo: Docendo Finland.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro.

Otala, L. 2001. Osaajana Opintiellä. Porvoo: WS Bookwell.

Singh, S. 1999. Koodikirja. Suomentaja Karjalainen, H.Jyväskylä: Gummerus kirjapaino.

Internetlähteet

Sähköpostin tietoturva. Viestintävirasto 2007. Viitattu 10.11.2010.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/sahkoposti.html

Salausmenetelmät. Viestintävirasto 2009. Viitattu 15.11.2010.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat.html

Salausalgoritmit. Viestintävirasto 2007. Viitattu 03.12.2010.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/salausalgoritmit.html

Symmetrinen salaus. Viestintävirasto 2007. Viitattu 09.01.2011.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/symmetrinensalaus.html

Epäsymmetrinen salaus. Viestintävirasto 2007. Viitattu 24.01.2011.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/epasymmetrinensalaus.html

Tiivistefunktiot. Viestintävirasto 2007. Viitattu 27.02.2011.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/tiivistefunktiot.html

Sähköpostin tietoturva. Viestintävirasto 2010. Viitattu 27.02.2010.
http://www.viestintavirasto.fi/index/tietoturva/sahkoposti.html

Oracle ThinkQuest. Skytale. Viitattu 05.05.2011.
http://library.thinkquest.org/07aug/01676/downtheages_hazybeginning_toolsanddevices_skytale.html

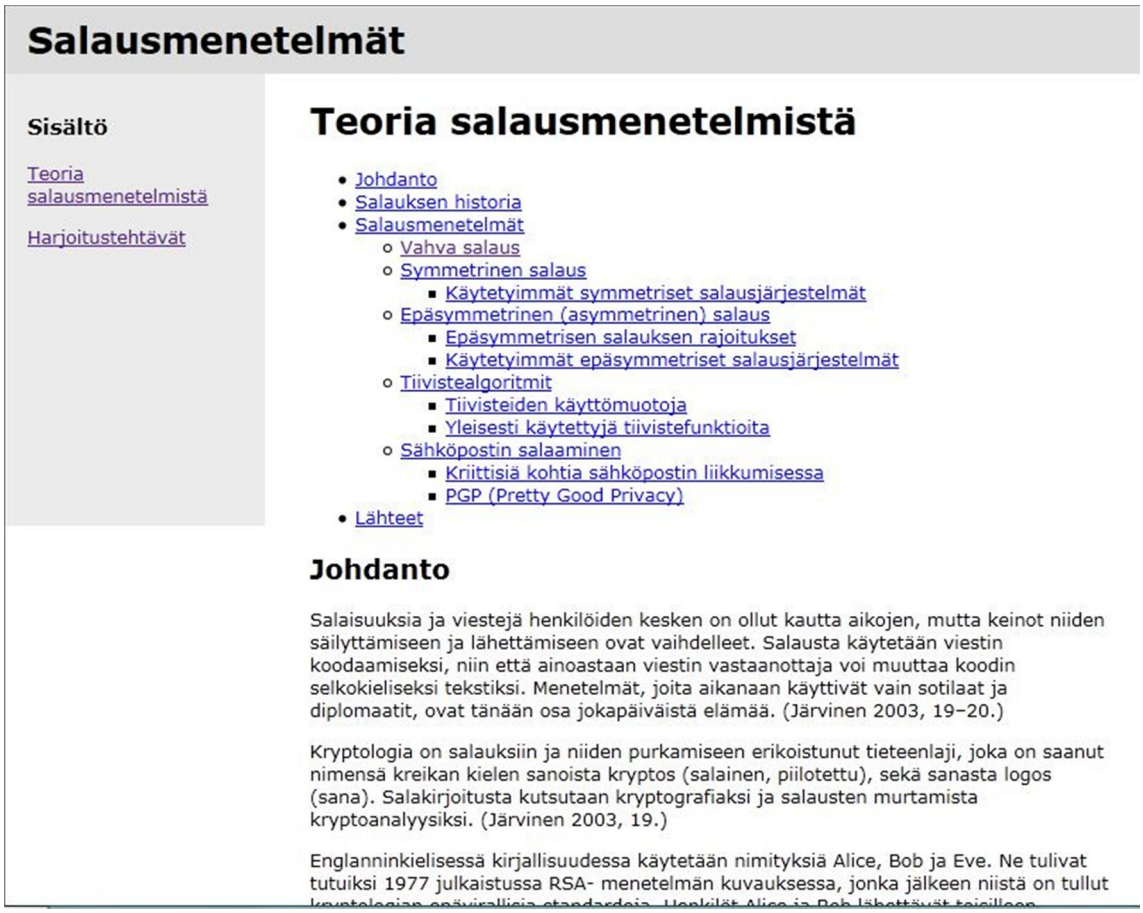
MBnet. Enigma - kaaoksen sinetöimä salaisuus. Viitattu 05.05.2011.
http://www.mbnet.fi/nettijatkot/2002/01/enigma/Enigma.jpg

Kuvat

Taulukot

Liitteet

Liite 1: Kuvat Internetpohjaisesta koulutuspaketista



Salausmenetelmät

Sisältö

Teoria salausmenetelmistä

Harjoitustehtävät

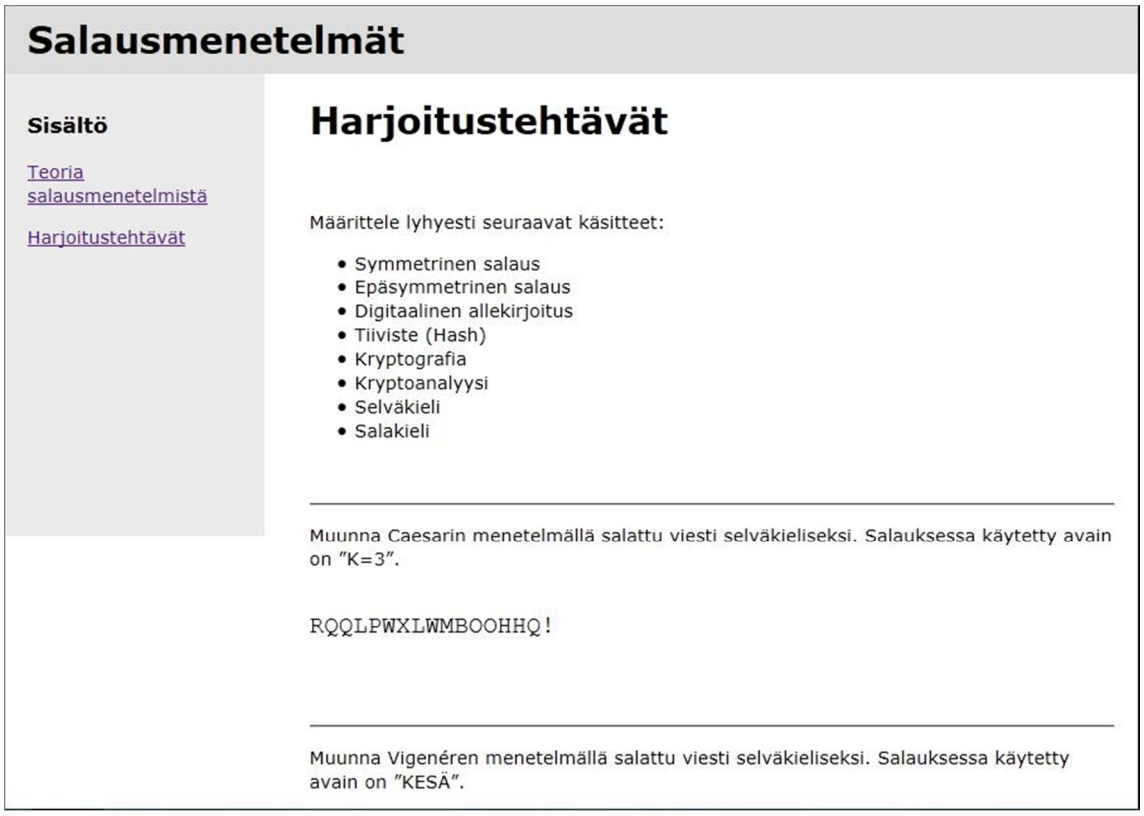
Teoria salausmenetelmistä

Johdanto

Salaisuuksia ja viestejä henkilöiden kesken on ollut kautta aikojen, mutta keinot niiden säilyttämiseen ja lähettämiseen ovat vaihdelleet. Salausta käytetään viestin koodaamiseksi, niin että ainoastaan viestin vastaanottaja voi muuttaa koodin selkokieliseksi tekstiksi. Menetelmät, joita aikanaan käyttivät vain sotilaat ja diplomaatit, ovat tänään osa jokapäiväistä elämää. (Järvinen 2003, 19–20.)

Kryptologia on salauksiin ja niiden purkamiseen erikoistunut tieteenlaji, joka on saanut nimensä kreikan kielen sanoista kryptos (salainen, piilotettu), sekä sanasta logos (sana). Salakirjoitusta kutsutaan kryptografiaksi ja salausten murtamista kryptoanalyysiksi. (Järvinen 2003, 19.)

Englanninkielisessä kirjallisuudessa käytetään nimityksiä Alice, Bob ja Eve. Ne tulivat tutuiksi 1977 julkaistussa RSA- menetelmän kuvauksessa, jonka jälkeen niistä on tullut



Salausmenetelmät

Sisältö

Teoria salausmenetelmistä

Harjoitustehtävät

Harjoitustehtävät

Määrittele lyhyesti seuraavat käsitteet:

- Symmetrinen salaus
- Epäsymmetrinen salaus
- Digitaalinen allekirjoitus
- Tiiviste (Hash)
- Kryptografia
- Kryptoanalyysi
- Selväkieli
- Salakieli

Muunna Caesarin menetelmällä salattu viesti selväkieliseksi. Salauksessa käytetty avain on ”K=3”.

RQQLPWXLWMBOOHHQ!

Muunna Vigenéren menetelmällä salattu viesti selväkieliseksi. Salauksessa käytetty avain on ”KESÄ”.

Liite 2: Harjoitustehtävät

Harjoitustehtävät

Määrittele lyhyesti seuraavat käsitteet:

- Symmetrinen salaus
- Epäsymmetrinen salaus
- Digitaalinen allekirjoitus
- Tiiviste (Hash)
- Kryptografia
- Kryptoanalyysi
- Selväkieli
- Salakieli

Muunna Caesarin menetelmällä salattu viesti selväkieliseksi. Salauksessa käytetty avain on ”K=3”.

RQQLPWXLWMBOOHHQ!

Muunna Vigenéren menetelmällä salattu viesti selväkieliseksi. Salauksessa käytetty avain on ”KESÄ”.

Y	R	C	G	Ö		X	J	G	A	T		J	P	U	E	B		Ä	K	R	K	G
O	W	Å	G	X		W	W	J	U	S		Ö	G	O	P	Å		Q	O	O	H	G

Mikä keskeinen ongelma symmetrisessä salauksessa on?

Etsi kolme eri julkista avainta internetsivustoilta ja kopioi osoitteet vastaukseksi.

Sait ystävältäsi tiedoston ”OOo_3.3.0_Win_x86_install_fi.exe”, jonka hän sanoi ladanneensa download.openoffice.org sivustolta. Miten voit varmistua tiedoston olevan alkuperäinen openoffice.org sivustolta ladattu tiedosto?

Toimi seuraavasti:

1. Tallenna tehtävien vastaukset tiedostoon <opiskelijanro>_vastaukset.txt
2. Luo itsellesi PGP-avainpari
3. Tuo (import) opettajan julkinen avain käyttöösi
4. Allekirjoita vastaukset omalla avaimellasi ja salaa ne opettajan julkisella avaimella
5. Lähetä oma julkinen avaimesi ja salattu vastaustiedosto sähköpostin liitteinä osoitteeseen xxxxxx@xxxxxxx.fi

Opettajan julkinen avain:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.17 (MingW32)

mQENBE3lK4gBCADFWgPivLMM+WPqAG0zEktdKcvhdWD1x69v7HCWsHCw7GfVBI26
Z1WJu6xhvRC/XWdcwP4OBqGfQu0OmayXtbSVtrVJ9V+sH2HKJaGcle76p5EKWTuv
JK5emIiCw2ZPQPVCx/2l5HZnmZ1g+ZDiuHrj9CTi3nb3+JzXtIIGYz14YOV268zE
2U6ikX1CNtHeZ69FWg4zj3Qo2A3ej5tZDRLyoH/8j22SIFsZDyv8CMzFle34c8Ug
KTHgKbo3qQxgwGT6yEawUCPjZgdGqcK5mO4EXnmbaDY40FrYekoVSIDwMVYLoEyC
n0W2k/7PLiPeI0NzjFS2rC59oy17T55Ce4v1ABEBAAG0ME9sbGkgT3BldHRhamEg
KE1hbGxpb3BldHRhamEpIDxvbGxpQG9wZXR0YWphLmZpPokBOAQTAQIAIgUCTeUr
iAIbDwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQ9PRTyMOSKB3WUAf/XEdl
RLiQZSROnbDYzMNXMRMn+R+vWvM40qQpxvm646xeSee1ev6dh3DhWqN6ex5r4/O0
nPldJKOOeOUKLCSPr8/e7KJWnZGa2pQcK3h34++wkY6B7itrIBRuWZlzUkBZrnG8
acr/IIkyMXz7Lju6BM83p3uRpf+vGgog8rqJx8ZitZLby8GTAfVtHYo29V0/h4NM
UQzPWOFZ0p+E2NARnwdubuzZikQ1XIuijiggcqkqHET6l+AZv6EHSOsA4Iy0LzyB
qynlt78Djxn/0b0522iJqflmlzLM+h6zWq+HdTVJsJujfjVnwrvuFsMilreRrzd4
xSLHFYC0x84jz3bJqw==
=ea5q
-----END PGP PUBLIC KEY BLOCK-----