



KEHITTYNEET

SALAUSMENETELMÄT

Lasse Rantanen

Opinnäytetyö
Huhtikuu 2013
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan
suuntautuminen
Tampereen ammattikorkeakoulu

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

LASSE RANTANEN: Kehittyneet salausmenetelmät

Opinnäytetyö 70 s., liitteet 40 s.
Huhtikuu 2013

Opinnäytetyöni käsittelee kehittyneitä salausmenetelmiä. Päädyin tähän aiheeseen, koska salausalgoritmien toimintamallit ja matematiikka kiinnostavat minua. Suurin osa työstä käsittelee Advanced Encryption Standardia ja sen toimintaa. Kyseinen salaus valikoitui pääaiheeksi sen maineen ja suuren kannattajakunnan takia. Halusin myös päästä vertailemaan salausten suorituskykyä ja toimintamalleja.

Suorituskykytestit koostuivat 60:sta TrueCrypt Benchmark mittauksesta, joissa mitattiin yhteensä kahdeksan salauksen tai salausten yhdistelmän suorituskykyä eri pakettikoilla. Näistä tuloksista luotiin kuusi kaaviota, joista kaikista näky selvästi, että Advanced Encryption Standard on tämän hetken suorituskykyisin symmetrinen salaus sekä salausten määrä vaikuttaa käänteisesti salausnopeuteen. Teoriaosuudessa saatiin selville, että AES on ainakin teoriassa myös kilpailevia asymmetrisiä salauksia nopeampi, vaikka se ei aivan kaikkiin tehtäviin sovikkaan.

Työn ollessa suorituskykytestejä vaille teoreettinen, ei sen tekemisessä tullut suuria ongelmia ja useiden salausmuotojen toiminta saatiin selitettyä ja suorituskykytestit ajettua. Työn suorituskykytestiin ei ohjelmistorajoituksen vuoksi saatu asymmetrisiä salauksia. Tämä estää AES:än suoran vertailun kyseisiin salauksiin. Työtä voitaisiin helposti syventää kyseisillä mittauksilla. Myös AES:än sovellusalueita voitaisiin tutkia tarkemmin ja samalla selittää yksityiskohtaisemmin kyseistä salausta käyttävien protokollien toimintaa. Algoritmin ollessa julkista tietoa, olisi myös salausmoottorin ohjelmointi työn puitteissa mielenkiintoinen vaihtoehto.

ABSTRACT
Tampere University of Applied Sciences
ICT Engineering
Telecommunications Engineering and Networks

LASSE RANTANEN: Advanced encryption methods

April 2013

I have always been interested on cryptology and mathematics so advanced encryptions were obvious choice when choosing subject of thesis. Most of this thesis is about Advanced Encryption Standard and its competitors and further on composed from theoretical comparing and performance tests.

Performance tests consist of 60 runs with TrueCrypt Benchmark tool. In this test 8 encryptions or there combinations is been tested with different size of packets. From those results were 6 graphs made that tell clearly the lead of Advanced Encryption Standards as industry's number one symmetric encryption. AES was compared to asymmetric encryptions in theoretical part of this thesis with good results.

This thesis being mostly theoretical there were no sign of problems and it accomplishes to explain the operation of most known encryptions and benchmarking the symmetric ones. This thesis could have been improved with asymmetric encryption benchmarks that weren't possible due software limitations. Protocols that use AES could have been explained more thoroughly and working self coded encryption illustration would be nice addition.

Key words: Advanced Encryption Standard, RSA, hash functions, TrueCrypt

SISÄLLYS

1	JOHDANTO.....	7
2	SALAUKSET.....	8
2.1	Symmetriset salausmenetelmät.....	8
2.2	Epäsymmetriset salausmenetelmät	9
2.2.1	RSA-salausmenetelmä	10
2.3	Tiivistefunktio.....	11
3	AES-SALAUUS.....	13
3.1	AES-salauksen synty ja menestys.....	13
3.2	Algoritmi.....	13
3.2.1	Tavujen korvaus	14
3.2.2	Rivin vaihto.....	15
3.2.3	Sarakkeiden yhdistys.....	15
4	AES TURVALLISUUS	16
4.1	AES:n murtoyritykset	16
4.2	Rautatason salaus	16
5	AES IMPLEMENTOINTI	17
5.1	AES käskykanta.....	17
5.2	Ohjelmointikielet	18
6	SOVELLUSALUEET	19
7	SUORITUSKYKY	21
	POHDINTA	28
	LÄHTEET.....	29

LIITTEET	31
Liite 1. Suorituskykymittaus 100 Kt, aes-kiihdytys pois päältä.....	31
Liite 2. Suorituskykymittaus 100 Kt, aes-kiihdytys päällä	33
Liite 3. Suorituskykymittaus 500 Kt, aes-kiihdytys pois päältä.....	35
Liite 4. Suorituskykymittaus 500 Kt, aes-kiihdytys päällä	37
Liite 5. Suorituskykymittaus 1 Mt, aes-kiihdytys pois päältä	39
Liite 6. Suorituskykymittaus 1 Mt, aes-kiihdytys päällä.....	41
Liite 7. Suorituskykymittaus 5 Mt, aes-kiihdytys pois päältä	43
Liite 8. Suorituskykymittaus 5 Mt, aes-kiihdytys päällä.....	45
Liite 9. Suorituskykymittaus 10 Mt, aes-kiihdytys pois päältä	47
Liite 10. Suorituskykymittaus 10 Mt, aes-kiihdytys päällä.....	49
Liite 11. Suorituskykymittaus 50 Mt, aes-kiihdytys pois päältä	51
Liite 12. Suorituskykymittaus 50 Mt, aes-kiihdytys päällä.....	53
Liite 13. Suorituskykymittaus 100 Mt, aes-kiihdytys pois päältä	55
Liite 14. Suorituskykymittaus 100 Mt, aes-kiihdytys päällä.....	57
Liite 15. Suorituskykymittaus 200 Mt, aes-kiihdytys pois päältä	59
Liite 16. Suorituskykymittaus 200 Mt, aes-kiihdytys päällä.....	61
Liite 17. Suorituskykymittaus 500 Mt, aes-kiihdytys pois päältä	63
Liite 18. Suorituskykymittaus 500 Mt, aes-kiihdytys päällä.....	65
Liite 19. Suorituskykymittaus 1 Gt, aes-kiihdytys pois päältä.....	67
Liite 20. Suorituskykymittaus 1 Gt, aes-kiihdytys päällä	69

LYHENTEET JA TERMIT

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
DES	Data Encryption Standard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMAP	Internet Message Access Protocol
IP	Internet Protocol
NIST	National Institute of Standards and Technology
POP	Post Office Protocol
SHA-1	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA-PSK	WPA-Personal
WPA-802.1X	WPA-Enterprise

1 JOHDANTO

Digitaalisen tiedon määrä kasvaa jatkuvasti. Yhä useammat ihmiset ovat siirtäneet ainakin osan sosiaalisesta ja rahallisesta toiminnastaan tietokoneelle ja internettiin. Yritykset ja yksityiset haluavat valvoa tai salata osan tiedoistaan ulkopuolisilta. Tähän on kehitetty useita tapoja, ohjelmistoja ja ohjelmistojen taustalla toimivia salausalgoritmejä, jotka salaavat tietokoneen kiintolevyn, turvaavat yhteyden verkkopankkiin tai mitä ikinä käyttäjä haluaakaan pitää omana tietonaan.

Tämän työn tarkoituksena on tutustuttaa lukija tämän hetken käytetyimpään salaus algoritmiin, Advanced Encryption Standardiin, lyhyemmin sanottuna AES:än. Kyseinen lyhenne esiintyy muunmuassa muistitikuissa, sähköpostiohjelmissa, verkkokaupoissa, verkkopankeissa ja pikaviestin ohjelmissa, vaikka käyttäjä ei sitä välttämättä huomaa tai tunnista.

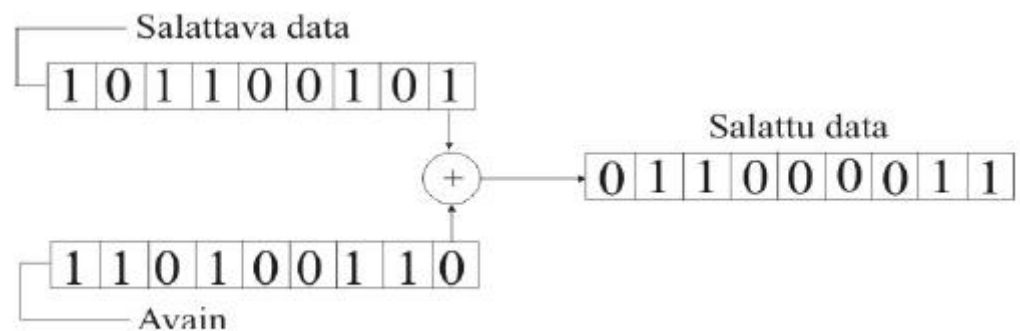
Tässä työssä selvitetään myös suorituskykytestien ja teoriaosuuksien avulla onko pitkään kehitetyllä, monesti validoidulla Yhdysvaltain virastojen ja useiden prosessorivalmistajien tukemalla salausalgoritmi AES:llä jotain mitä muilla ei ole.

2 SALAUKSET

2.1 Symmetriset salausten menetelmät

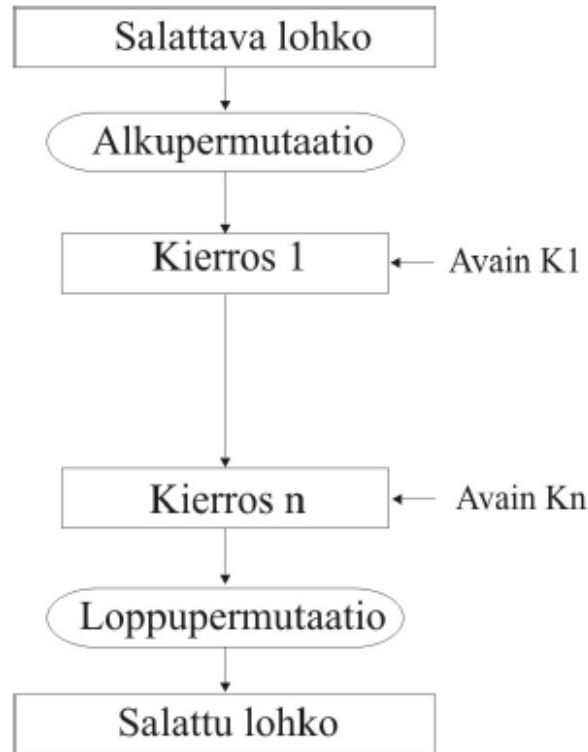
Symmetrisessä salausten menetelmässä lähetys ja vastaanotto tapahtuvat samaa avainta käyttäen. Viestin salauksen purkamiseen tarvittava avain on suoraan johdettavissa salaustavaimesta. Menetelmää käytetään sen nopeuden vuoksi, mutta ongelmana on kuitenkin avainten hallinta, koska purkamiseen vaadittava avain on sama kuin salaamiseen. Avaimen siirtoon, esimerkiksi käyttäjältä toiselle, käytetään usein niin sanottua salaus tokenia tai epäsymmetristä salausta. Symmetriset salausten menetelmät voidaan jakaa kahteen alaluokkaan: jonosalauksella ja lohkosalaus.

Jonosalauksen menetelmässä salattava informaatio salataan bitti bitiltä. Salauksena se onkin nopea, ja sitä käytetään mm. GSM-puheluissa A5-salauksen muodossa, mutta A5-salaus on kuitenkin murrettavissa. Salaus ja purku tapahtuvat samalla operaatiolla, eli avaimen ja selkötökin yhteenlasku XOR-opeaatiolla. Tämä on esitetty kuvassa 1. Yksinkertaista rakennetta ja suurta salausnopeutta haettaessa jonosalauksella on hyvä menetelmä.



KUVA 1. Jonosalauksen periaate (Salo 2005)

Lohkosalauksessa algoritmille annetaan lohko, eli useampi bitti kerrallaan, esimerkiksi 64 tai 128 bittiä. Kryptaaja saa päättää salataanko lohkot samalla salausavaimella, vai käytetäänkö uuden lohkon salaamisen osana aikaisemman lohkon salakirjoitusta. Alussa ja lopussa lohkon bitit permutoidaan, eli niiden järjestystä muutetaan (kuva 2).



KUVA 2. Lohkosalauksen periaate (Salo 2005)

Mikäli salattava tieto on lyhyempi kuin lohko, luodaan sen perään täytebittejä. Nykyisin käytössä olevia symmetrisiä salausalgoritmeja ovat mm. Blowish, AES, CAST ja RC5. (Salo 2005, 20.)

2.2 Epäsymmetriset salausmenetelmät

Epäsymmetriseen salaukseen käytetään avainparia, jonka avaimet eroavat toisistaan. Toinen avaimista on julkinen ja toinen yksityinen. Julkisella avaimella salattu materiaali voidaan avata yksityisellä avaimella ja toisinpäin. Esimerkiksi sähköpostia lähettäessä voidaan teksti salata vastaanottajan julkisella avaimella, jolloin vain hän pystyy avaamaan sen käyttämällä omaa yksityistä avaintaan.

Julkisen avaimen suurin etu, verrattuna symmetrisiin, on sen helppo avainten hallinta, mutta heikkoutena sen raskaus, koska salausavaimet ovat merkittävästi pidempiä kuin symmetrisissä järjestelmissä. Julkisen avaimen heikkoutena on myös sen helpompi purkaminen, koska murrettava salausavain ryhmä voidaan rajata niihin, jotka täyttävät salauksen vaatimat matemaattiset ominaisuudet. Esimerkiksi parillisia lukuja ei tarvitse kokeilla, koska ne eivät kuulu alkulukuihin, joita käytetään salauksen luonnissa. Jos epäsymmetrisellä salauksella tavoitellaan samaa turvatasoa kuin symmetrisellä, pitää avaimen olla pidempi. (Salo 2005, 21, 22.)

2.2.1 RSA-salausmenetelmä

RSA on maailman käytetyin epäsymmetrinen salausalgoritmi. Salaus tapahtuu kahden suuren alkuluvun kertomisella. Systemi perustuu siihen, että on hyvin vaikeaa jakaa tekijöihin kahden suuren alkuluvan tulo, joten sitä voidaan käyttää julkisena avaimena. Alla esitetään RSA-avainparin luomisen vaiheet.

Ensin valitaan kaksi erittäin suurta alkulukua, p ja q . Jonka jälkeen lasketaan luku n kaavalla 1.

$$n = p \cdot q \tag{1}$$

Tämän jälkeen lasketaan phi (Φ) kaavalla 2.

$$\Phi = (p - 1) \cdot (q - 1) \tag{2}$$

Seuraavaksi valitaan pariton luku e , joka on välillä $1 < e < \Phi$. Jonka jälkeen lasketaan luku d kaavalla 3.

$$d = e^{-1} \cdot \text{mod } \Phi \tag{3}$$

Julkinen avain on (n,e) ja salainen avain on d . Salaus on esitetty kaavassa 4 ja sen purku kaavassa 5.

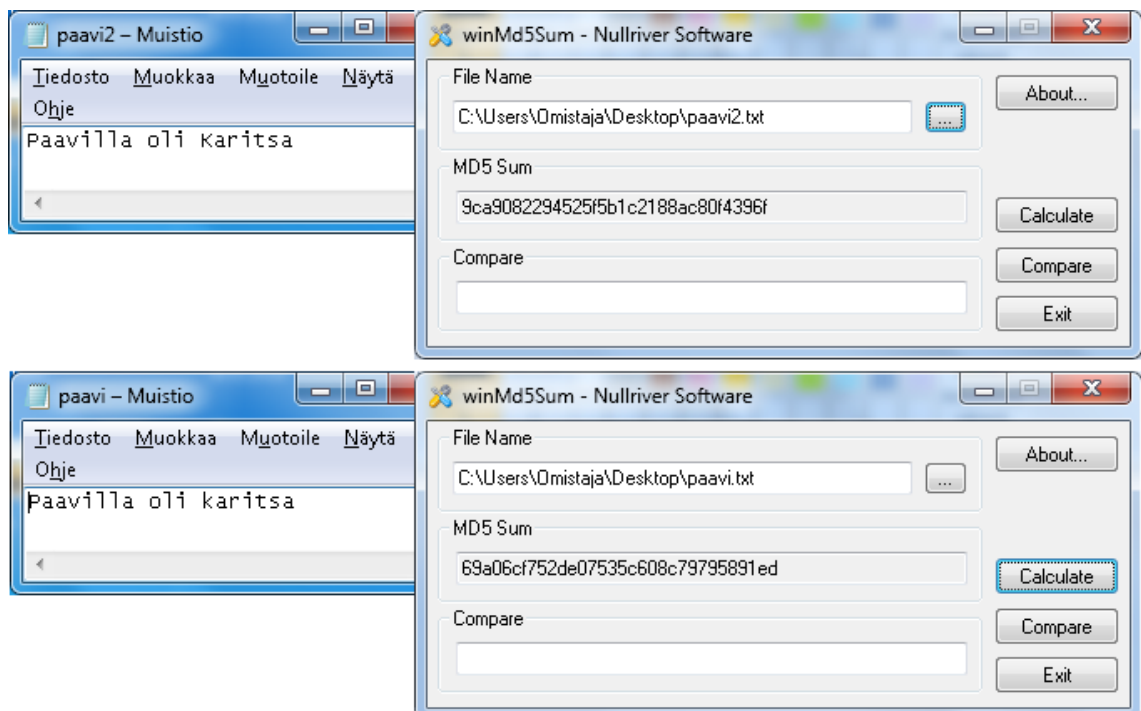
$$c = m^e \cdot \text{mod } n \quad (4)$$

$$m = c^d \cdot \text{mod } n \quad (5)$$

RSA-salauksen turvallisuus johtuu siitä, että modulusta n on hyvin vaikea jakaa alkutekijöihin p ja q . (Salo 2005, 22.)

2.3 Tiivistefunktio

Kolmas yleinen salauksen muoto on tiivistefunktio eli kansankiellä hash. Tiivistefunktion ideana on tuottaa syötetystä datasta ennalta määrätyn mittainen datajono, esimerkiksi 160 bittiä. Tiivistefunktiot ovat yleensä yksisuuntaisia, eli funktion antamaa bittijonoa ei pysty enää muuntamaan alkuperäiseksi syötteenksi. Mitä parempi tiivistefunktio, sitä suurempi on valmiin tiivisteeseen muutos, kun syötettä muutetaan. Tämä näkyy kuvassa 3. (Keränen, Teeriaho 2006, 1,2.)



KUVA 3. Tiivistefunktioiden ero

Kaksi yleisintä tiivistefunktioiden käyttötapaa ovat salasanahallinta ja viestin oikeellisuuden tarkistaminen. Salasanahallinnassa palvelimen tai käyttöjärjestelmän kappale salasanasta hashataan ennen tallennusta, ja sitä verrataan käyttäjän syöttämän salasanan hashiin käyttäjän kirjautuessa. Viestin oikeellisuuden varmistamisessa lähettäjä voi lisätä viestinsä loppuun viestistä lasketun hashin, johon vastaanottaja voi verrata vastaanottamastaan viestistään laskemaan hashiin. Mikäli hashit ovat identtiset, on viesti todennäköisimmin alkuperäinen. (Keränen, Teeriaho 2006, 1,2.)

Tunnettuja tiivistefunktioita ovat muunmuassa Ronald Rivestin kehittämät MD2, MD4 ja MD5, joista jälkimmäisin tuottaa 16 tavuisen tiivisteeseen, sekä NIST:n standardoima SHA-1, joka tuottaa 20 tavuisen tiivisteeseen. MD5-hashia on käytetty muunmuassa edesmenneiden Windows-käyttöjärjestelmien, ja joidenkin Linux-käyttöjärjestelmien salasanahallintaan. (Keränen, Teeriaho 2006, 1, 2.)

3 AES-SALAUUS

3.1 AES-salauksen synty ja menestys

AES-salaus sai alkunsa, kun sen kehittäjät Vincent Rismen ja Joan Daemen osallistuivat ja voittivat kehittämällään salauksella Yhdysvaltain hallituksen järjestämän avoimen kilpailun vuonna 1997. Kilpailun tavoitteena oli löytää seuraaja jo 1976 käyttöön otettuun, ja sittemmin vanhentuneelle Digital Encryption Standard -salaukselle. Salausta kutsuttiin ensin Rijndaeliksi, sen kehittäjien mukaan, mutta Yhdysvaltain National Institute of Standards and Technology julkaisi sen viiden vuoden validointiprosessin jälkeen nimellä Advanced Encryption Standard (AES). Sittemmin se on muun muassa sisällytetty ISO/IEC 18033-3 standardiin. Siitä on tullut ensimmäinen Yhdysvaltain NSA:n hyväksymä avoimen algoritmin salausmenetelmä. Siitä on tullut myös luultavasti suosituin avoin salausmenetelmä kansainvälisesti. (National Institute of Standards and Technology 2001, 1,2.)

3.2 Algoritmi

AES-salauksessa lohkon eli datataulukon koko on 128 bittiä, vaikkakin Rijndael sallisi jopa 256 bitin lohkon ja salausavaimen koko on 128, 192 tai 256 bittiä. Lohkosalaukseen perustuvan algoritmi alkaa tiedon jakamisella neljä kertaa neljän tavun taulukoihin. Loppu koostuu neljästä päätoimituksesta ja neljästä alitoimituksesta, joissa käsitellään taulukoiden dataa, ja joiden toistokerta määräytyy avainkoon perusteella taulukon 1 mukaisesti.

TAULUKKO 1. Avainkoon määräytyminen kierrosten lukumäärän mukaan

kierrosten lukumäärä	avain/bittiä
10	128
12	192
14	256

Seuraavaksi esitetään pää- ja alitoimitukset. Ensimmäinen päätoimitus on avaimen laajennus. Salausavaimesta tehdään uniikit variantit tuleville algoritmin kierroksille. Avainten luontiin käytetään Rijndaelin avaintaulukkoa. Tämän jälkeen seuraava päätoimitus on alustava kierros. Alustavan kierroksen alitoimituksena on avaimen lisäys kierros. Jokainen taulukon tavu yhdistetään xor -toimituksella kyseiselle kierrokselle luotuun avaimeen.

Kolmas päätoimitus on varsinaiset kierrokset. Kierroksien alitoimituksina ovat tavujen korvaus, rivin vaihto, sarakkeiden yhdistys ja avaimen lisäys kierros. Tavujen korvauksessa jokainen taulukon tavu korvataan epälineaaraisesti korvaustaulukkoa hyväksikäyttäen toisella tavulla. Rivin vaihdossa jokainen taulukon rivi siirretään tietyn määrän verran eteenpäin. Sarakkeiden yhdistymisessä taulukossa olevien sarakkeiden tavut yhdistetään. Neljäntenä päätoimituksena on viimeinen kierros. Viimeisen päätoimituksen alitoimituksina ovat tavujen korvaus, rivin vaihto ja avaimen lisäys kierros. (National Institute of Standards and Technology 2001, 14–22.)

3.2.1 Tavujen korvaus

Tavujen korvauksessa jokainen taulukon tavu muutetaan kahdeksi hexamerkiksi. Ensimmäiset neljä bittiä muodostavat ensimmäisen merkin, ja jälkimmäiset neljä muodostavat toisen merkin. Tämän jälkeen hexamerkkejä verrataan tätä varten tehtyyn korvaustaulukkoon, jossa hexamerkit sijoittuvat x- ja y-akselille ja niiden risteyskohdasta tulee taulukon uusi tavu, joka vielä muutetaan takaisin binääriksi. (National Institute of Standards and Technology 2001, 14–22.)

3.2.2 Rivin vaihto

Rivin vaihdossa taulukon neljä riviä kiertävät vasemmalle seuraavasti. Toinen rivi kiertää yhden sarakkeen vasemmalle, kolmas rivi kaksi saraketta ja neljäs rivi kolme saraketta. Tämä on havainnollistettu kuviossa 1.

$$\begin{array}{cccc}
 0.0 & 0.1 & 0.2 & 0.3 \\
 1.0 & 1.1 & 1.2 & 1.3 \\
 2.0 & 2.1 & 2.2 & 2.3 \\
 3.0 & 3.1 & 3.2 & 3.3
 \end{array}
 \quad > \quad
 \begin{array}{cccc}
 0.0 & 0.1 & 0.2 & 0.3 \\
 1.1 & 1.2 & 1.3 & 1.0 \\
 2.2 & 2.3 & 2.0 & 2.1 \\
 3.3 & 3.0 & 3.1 & 3.2
 \end{array}$$

KUVIO 1. Rivinvaihto (National Institute of Standards and Technology 2001, 17, muokattu)

3.2.3 Sarakkeiden yhdistys

Sarakkeiden yhdistys vaiheessa jokaiselle sarakkeen tavulle suoritetaan xor, ennalta määritellyn matriisin kanssa. Esimerkkinä matriisi 128 bittisen avaimelle, kaava 6. (National Institute of Standards and Technology 2001, 14–22.)

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 2311 \\ 1231 \\ 1123 \\ 3112 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \quad (6)$$

4 AES TURVALLISUUS

4.1 AES:n murtoyritykset

AES:n julkaisun jälkeen on dokumentoitu useita hyökkäysyrityksiä salauksen murtamiseksi. Algoritmin toimintaa tutkivaa/hyväksi käyttävää murtoyritystä ei ole toistaiseksi löydetty, vaikkakin sellasien uskottiin onnistuvan AES:n suhteellisen yksinkertaisen algoritmin vuoksi. Kaikki onnistuneet hyökkäykset ovat olleet niin kutsuttuja side channel -hyökkäyksiä, missä ei oteta kantaa itse algoritmiin ollenkaan, vaan tutkitaan salattavaa dataa ja sen salauksen kestoja. Side channel -hyökkäykset vaativat lähes poikkeuksetta ajettavan ohjelman salausta suorittavalla koneella, tai todella suuren tunnetun data määrän toimiakseen. Esimerkkeinä näistä toistaiseksi menestyksekkäin side channel -hyökkäys, vuonna 2010 David Gullasch ja Stephan Krenn julkaisivat dokumentin, jossa kuvailtiin onnistunut hyökkäys 128 bittistä AES-salausta vastaan, ilman, että tiedettiin salausavain taikka salattava data, mutta se vaatii onnistuakseen haittaohjelman ajamisen salausta suorittavassa koneessa. (Krenn, Gullasch, Bangerter, sivunro.)

4.2 Rautatason salaus

AES-salaus voidaan toteuttaa pienellä tarkoitukseen tehdyllä piirillä, joka voidaan liittää emolevyille, USB -tikkuun, puhelimeen tai johonkin muuhun dataa käsittelevään laitteeseen. Vaihdettaessa ohjelmistopohjaisesta rautapohjaiseen salaukseen voidaan välttää osa side channel -hyökkäyksistä, sekä nopeuttaa salausta mikäli isäntäkoneen prosessori ei tue AES – käskykanta.

5 AES IMPLEMENTOINTI

5.1 AES käskykanta

AES-salauksen tullessa yhä suosittumaksi tietotekniikassa, Intelin ehdotuksesta vuonna 2008, Intel ja AMD alkoivat sisällyttää suorittimiinsa erillisen käskykannan AES saluksen eri vaiheiden suorittamiseen. Sittemmin sama käskykanta on levinnyt myös VIA:n x86 pohjaisiin suorittimiin, ja joihinkin ARM-suorittimiin. Vuonna 2010 Intel julkaisi AES-NI käskykannan omille prosessoreilleen, parantaen edelleen suorittimien kykyä AES-salauksen luontiin ja purkamiseen. Alkuperäisessä AES-käskykannassa on erillinen käsky seuraaville suoritteille:

Yksi kierros salatessa

Viimeinen kierros salatessa

Yksi kierrossa purkaessa salausta

Viimeinen kierros purkaessa salausta

Kierros avainten luonti

Sarakkeiden yhdistys

Kahden 64-bittisen luvun kertominen keskenään (Gueron 2009, 15–17.)

AES- ja AES-NI -käskykannallisissa prosessoreissa voidaan suorittaa algoritmin avaimen laajennus osuus itse prosessorissa, eikä erillistä lookup tablea tarvita. Näin estetään avaimiin kohdistuva side channel –hyökkäys, jossa hyökkääjä yrittää päätellä salasanat siitä kuinka kauan prosessorilla menee lukea ulkoista lookup tablea. (Gueron 2009, 23.)

AES-käskykanta on nykyään tuettuna useilla eri alustoilla ja ohjelmilla, esimerkkeinä Solaris Cryptographic Framework, Oracle Database, OpenSSL, FreeBSD:n työkalut, Os X:n FileVault ja Windowsin BitLocker.

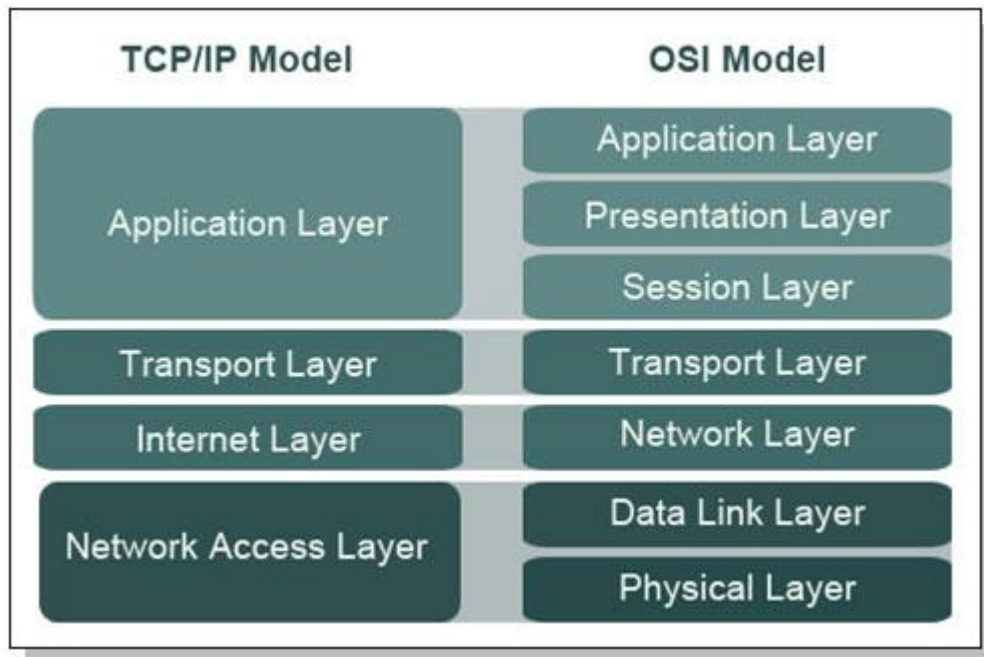
5.2 Ohjelmointikielet

AES-salaus voidaan implementoida tällä hetkellä ainakin c, c++, c#, .NET, Java, Javascript, PHP ja Python ohjelmointikieliin. Viime vuonna (2012) julkaistiin myös ensimmäinen näytönohjainta salaukseen käyttävä ohjelma, jolla pitäisi valmistajan mukaan päästä näytönohjaimesta ja prosessorista riippuen 2-5 kertaisiin nopeuksiin, pelkkään prosessoriin verrattuna. (gKrypt, 2012)

6 SOVELLUSALUEET

AES-salauksella on kaksi pääasiallista sovellusaluetta, datan ja tietoliikenteen salaaminen. Datan salauksessa yksittäisellä tietokoneella tai palvelimella on salaushjelma joka salaa tietoa joko pyydettyä tai juoksevasti normaalin käytön ohella. Pyydettyä tapahtuva salaaminen tarkoittaa yhden tai useamman tiedoston taikka kansion salaamista käyttäjän erikseen pyytämänä. Lähes kaikki jälkikäteen asennettavat salaushjelmat tukevat tätä vaihtoehtoa. Juokseva salaus tarkoittaa sitä, että data salataan tai salaus puretaan automaattisesti, sitä mukaan kun ohjelma tai käyttöjärjestelmä dataa käyttää. Esimerkkinä Windows 7 Ultimate ja Enterprise versioiden mukana tuleva Bitlocker -ohjelmisto, jolla voi salata käyttöjärjestelmän niin halutessaan. (Microsoft 2007.)

Tietoliikenteessä AES-salausta voidaan käyttää kahden tietokoneen tai tietokoneen ja palvelimen välisen tietoliikenteen salaamiseen, näistä esimerkkinä pankkitapahtumat, sähköpostin siirto ja luku sekä Voice over IP puhelut. Suosituin AES-salausta tukeva protokolla on Transport Layer Security eli lyhyemmin TLS. TLS toimii TCP/IP-mallin transport kerroksella ja OSI-mallin session ja presentation kerroksilla (kuva 4). Näillä kerroksilla TLS toimii muiden protokollien kanssa niiden siirtämän datan salaukseen, esimerkkinä HTTP:n suojattu versio HTTPS, joka käyttää TLS:ää siirrettävän datan salaukseen. Muita samalla OSI kerroksella toimivia protokollia jotka osaavat hyödyntää TLS:sää ovat ainakin sähköpostin siirtoon luodut POP, IMAP ja SMTP sekä etäyhteyksiä varten luodut SSH ja VPN. (Gilbert-Knight, Bergfeld, Chapman 2012.)



Kuva 4. TCP/IP- ja OSI-malli. (Learn Networking. 2008)

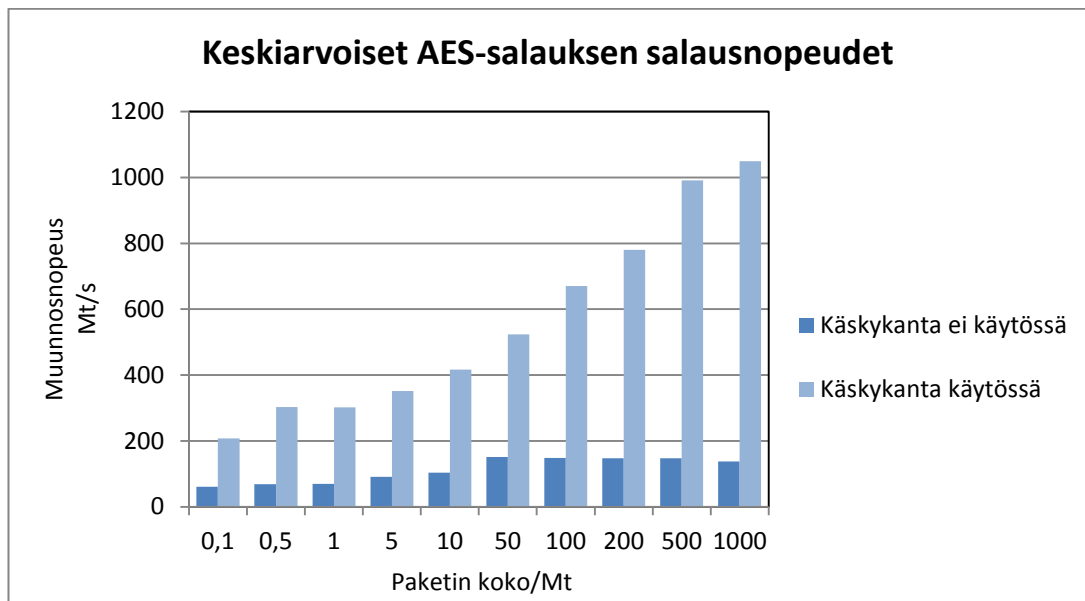
Toinen tietoliikenteessä tunnettu AES-salausta käyttävä protokolla on WPA2, jota käytetään langattomien Wi-Fi verkkojen datan salaukseen. WPA:sta on julkaistu erilliset versiot yksityisten (WPA2-PSK) ja yritysten (WPA-802.1X) käyttöön. WPA2:ssa data salataan 128 bitin lohkoissa ja 128 bitin avaimella. Salaus tapahtuu niin sanotussa CBC moodissa, jossa edeltävän lohkon salaustekstiä käytetään seuraavan lohkon salaukseen eräänlaisella takaisinkytkennällä. (Wi-Fi Alliance 2013.)

7 SUORITUSKYKY

Osana tätä työtä haluttiin mitata symmetristen salausten ja AES-NI-käskykannan suorituskyky (Liitteet 1-20). Mittaukseen käytettiin ilmaisen TrueCrypt -ohjelman benchmark -toimintoa, koska käyttäjän valittavana on käytettävien prosessoriytimien määrä, sekä ohjelma tukee haluttaessa AES-NI-käskykanta. Lisäksi testit ajetaan keskusmuistissa, poistaen näin tallennusmedian suorituskyvyn vaikutukset tuloksiin. Testeihin käytettiin Samsung NP530U3C kannettavaa tietokonetta, jossa on Intel i5-3317U prosessori, neljä gigatavua keskusmuistia ja käyttöjärjestelmänä 64-bittinen Windows 7 Home Premium. Kaikki ylimääräiset ohjelmat ja prosessit lopetettiin testien ajaksi, koska ne saattavat vaikuttaa mittaustuloksiin negatiivisesti, varaamalla kellojaksoja prosessorilta tai viemällä tilaa keskusmuistista.

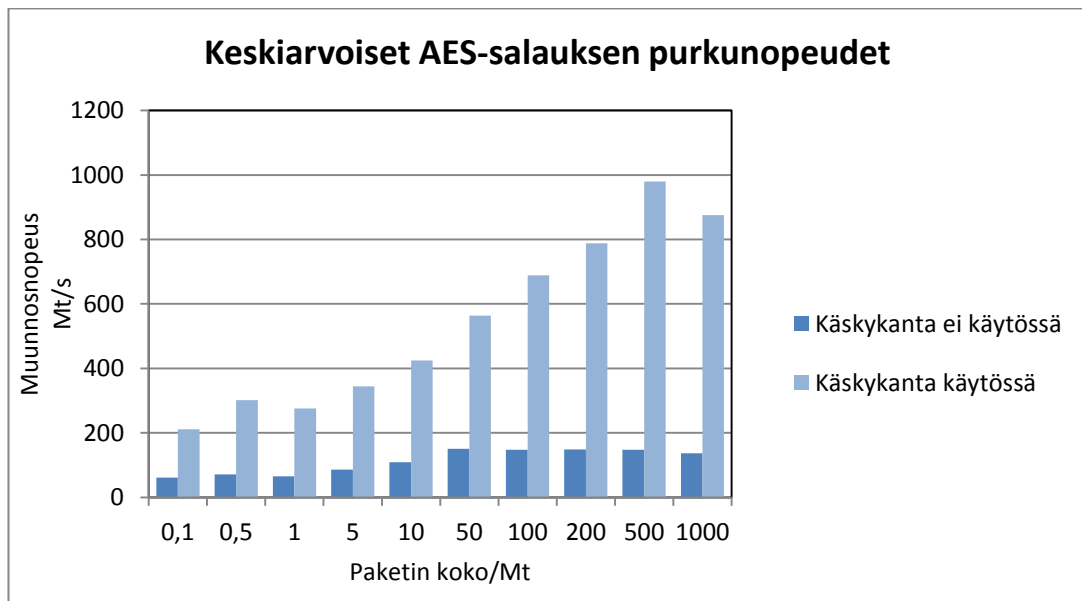
TrueCrypt -ohjelmiston benchmark -toiminnossa on valittavana salattavan paketin koko, jolle on kymmenen arvoa 100 kilotavun ja yhden gigatavun väliltä. Testissä salataan ja puretaan valitun kokoinen testitiedosto, yhteensä kolmella symmetrisellä salauksella tai näiden salauksien yhdistelmällä. Vaihtoehtoina ovat AES, Twofish, Serpent, sekä valittavissa on kahden ja kolmen salauksen yhdistelmiä. Kaikilla pakettikoilla tehtiin kolme testiä AES-NI-käskykanta käytössä ja poissa käytöstä, keskiarvojen saamiseksi. Tulevat kuviot perustuvat näistä mittaustuloksista saatuihin keskiarvoihin.

Kuviossa 2 vertaillaan kaikilla pakettikoilla AES-salauksen salausnopeutta AES-NI-käskykannalla ja ilman. Kuviossa vaaka-akselilla on paketin koko ja pystyakselilla muunnosnopeus. Tuloksista nähdään AES-NI-käskykannan olevan kolmesta kahdeksaan kertaan nopeampi pakettikoosta riippuen, eikä sen nopeuden kehitys pysähdy 50 Megatavun pakettikoon jälkeen toisin kuin ilman käskykanta.



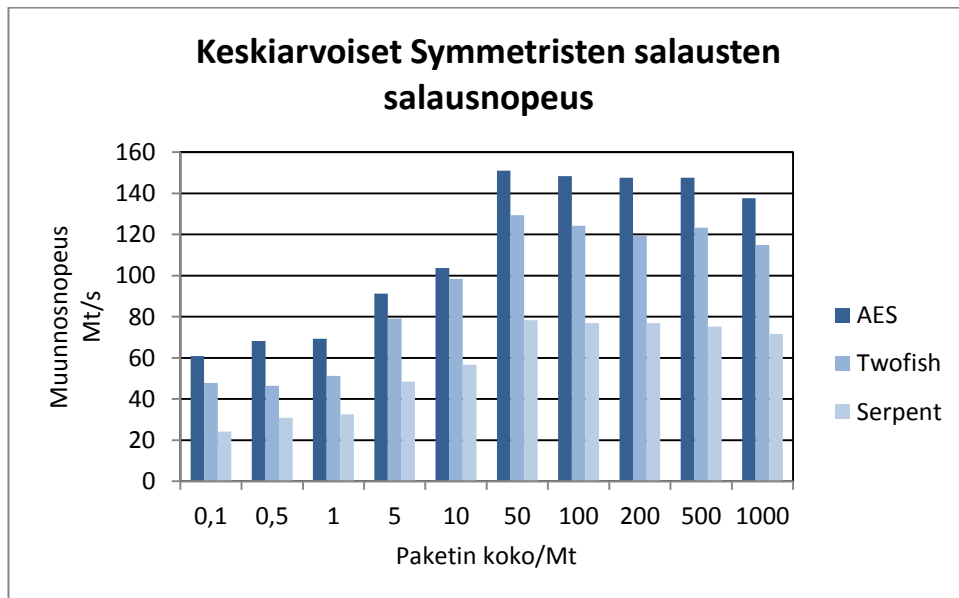
KUVIO 2. AES-salauksen salausnopeus

Kuviossa 3 vertaillaan kuvion 2 mukaisesti salauksen purkunopeutta. Vaaka-akseli kuvaa edelleen paketin kokoa ja pystyakseli muunnosnopeutta. Tulokset ovat hyvin lähellä salausnopeuksia, joka johtuu AES-salauksen symmetrisestä algoritmistä, jossa purkaminen tapahtuu salauksen käänteisversiolla. Kun paketin koko on 1000Mt ja muunnosnopeus n.850Mt/s ja käskykanta on käytössä, havaitaan kuviossa selvä muutos. Pakettikokoon 500Mt asti, kun käskykanta on käytössä, pylväät kasvavat, mutta kun pakettikoko on 1000Mt, muunnosnopeus putoaa n.850Mt/s. Myös pakettikokoa 0,5Mt käytettäessä, kun käskykanta on käytössä, havaitaan selvästi suurempi pylväs kuin pakettikoossa 1Mt, joka poikkeaa selvästi muista saaduista arvoista.



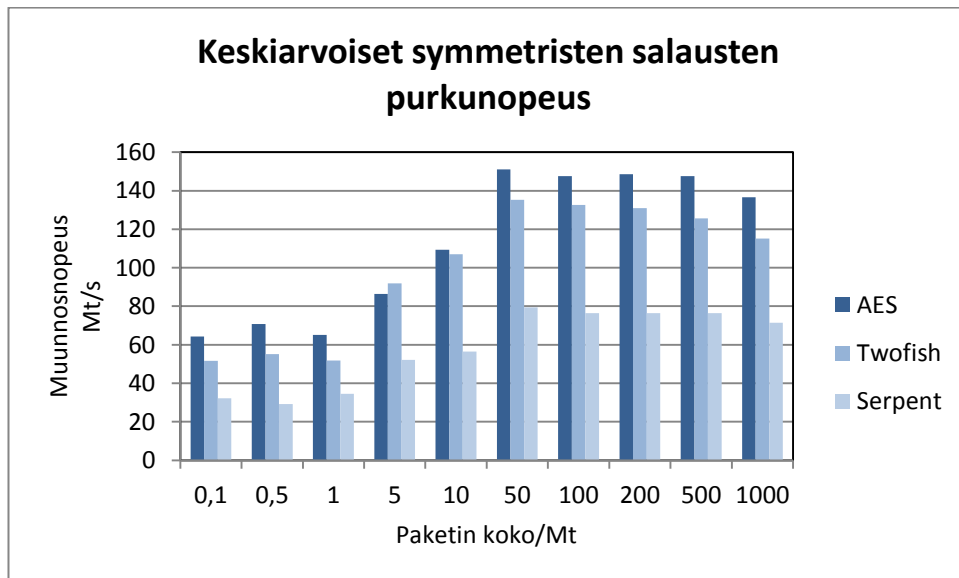
KUVIO 3. AES-salauksen purkunopeus

Kuviossa 4 vertaillaan symmetristen salausalgoritmien salausnopeutta, kun AES-NI käskykanta ei ole käytössä. Kuvaajassa vaaka-akselilla on paketin koko ja pystyakselilla muunnosnopeus. Kuvaajasta nähdään, että AES on nopein ilman käskykantaakin, mutta Twofish jää vain 5-15 prosenttia jälkeen. Kolmanneksi tuli Serpent, joka jää noin puoleen AES-salauksen salausnopeudesta.



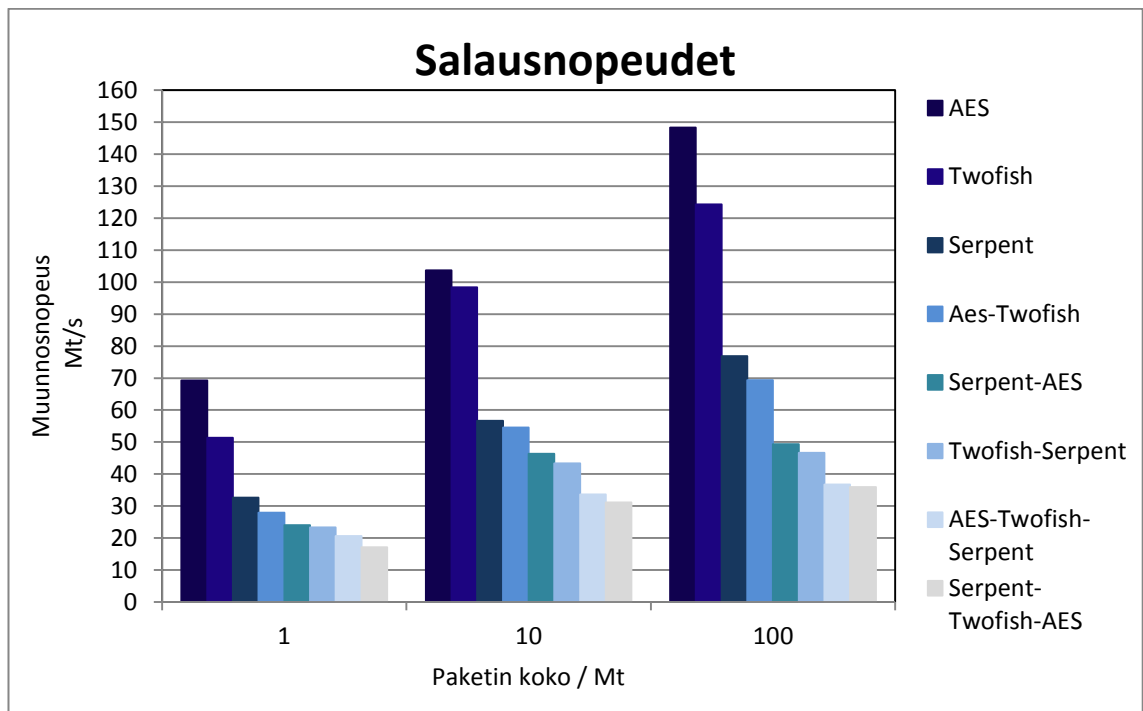
KUVIO 4. Symmetristen salausten salausnopeus

Kuviossa 5 vertaillaan symmetristen salausten purkunopeutta toisiinsa nähden. Tulokset ovat hyvin samankaltaiset kuvion 4 kanssa. Eli kuviosta 5 voidaan päätellä, että AES on nopein purkunopeudessa ja Serpent hitain. Twofishin purkunopeudet ovat näiden kahden välistä. AES-NI käskykanta ei ole käytössä.



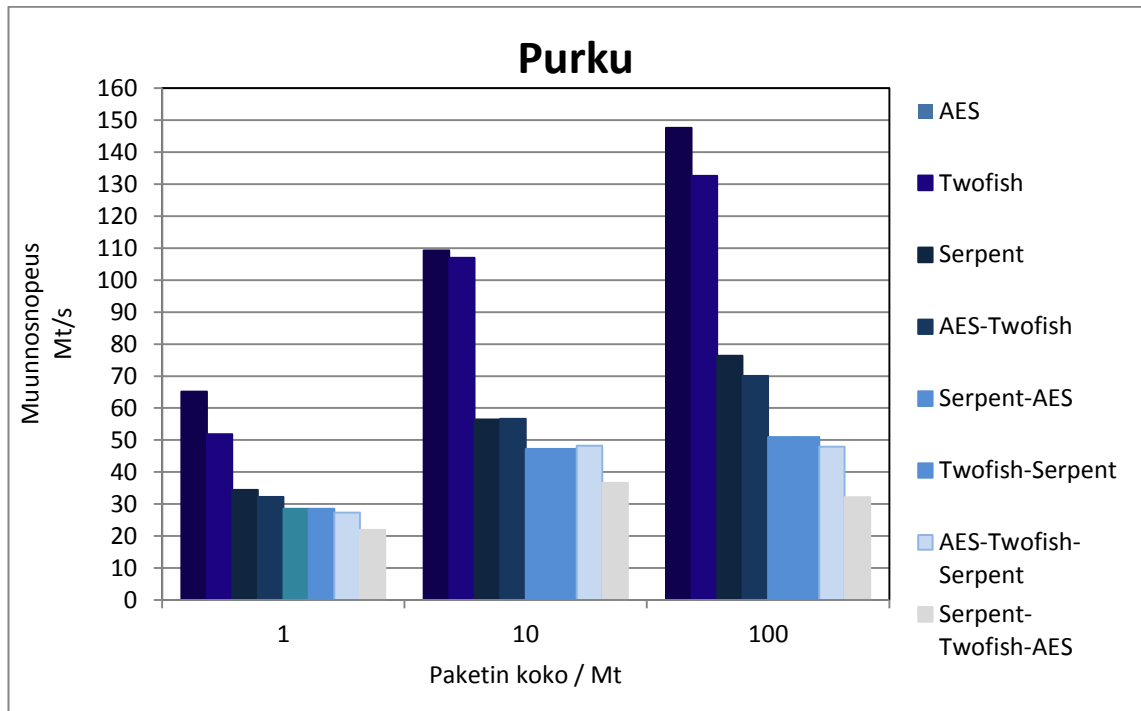
KUVIO 5. Symmetristen salausten purkunopeus

Kuviossa 6 vertaillaan yhdessä ja erikseen ajettujen salausten salaussnopeuksia. Vaaka-akselilla on paketin koko ja pystyakselilla muunnosnopeus. Yhdessä ajettut testit koostuvat joko kahden tai kolmen salauksen jonosta. Kuvioista nähdään, että yksittäiset salaukset ovat huomattavasti nopeampia kuin kahden tai kolmen salauksen jonot, ja, että salausten määrä vaikuttaa käänteisesti salaussnopeuteen. AES-NI käskykanta ei ole käytössä.



KUVIO 6. Salaussnopeudet

Kuviossa 7 vertaillaan yhdessä ja erikseen ajettujen salausten purkunopeuksia. Vaaka-akselilla on paketin koko ja pystyakselilla muunnosnopeus. Yhdessä ajettut testit koostuvat joko kahden tai kolmen salauksen jonosta. Kuvioista nähdään, että yksittäiset salaukset ovat huomattavasti nopeampia kuin kahden tai kolmen salauksen jonot ja, että salausten määrä vaikuttaa käänteisesti purkunopeuteen. AES-NI käskykanta ei ole käytössä.



KUVIO 7. Purku

POHDINTA

Tämän opinnäytetyön tekeminen onnistui suhteellisen tiukasta aikataulusta huolimatta mielestäni hyvin ja sain käsiteltyä kaikki ne asiat jotka halusin. Tietysti joissakin asioissa olisi voinut mennä syvemmälle tekniikkaan, mutta jätin suosiolla kilpailevat tekniikat vähemmälle huomiolle, jotta saisin itse AES:n selostettua riittävän selkeästi. Työssä huomattiin, että AES:lle kehitetystä AES-NI on merkittävä hyöty salaukselle ja sen turvin se onkin markkinoiden nopein.

Lähdeaineiston koostuessa ainoastaan internetsivuista, internettiin ladatuista kirjoista ja oppimisasiaineistosta oli tieto hyvin ja nopeasti saatavilla, sekä käytössä esteittä ympäri vuorokauden, auttaen työn nopeaa valmistumista. Löysin myös muutamia ulkomailla julkaistuja mielenkiintoisia teoksia joihin haluaisin tutustua tämän työn jälkeen. Internet lähdeaineistona oli toisaalta myös hankala, koska piti olla erittäin lähdekriittinen ja tunnettuja julkaisuja aiheesta oli välillä hankala löytää ilman lukumaksuja. Työssäni olisin voinut käyttää monipuolisempia lähteitä esimerkiksi kirjallisuutta, lehtiartikkeleita ja asiantuntijoiden haastatteluja.

Nyt kun työ on tehtynä olen vakuuttunut siitä, että vastaavaa työtä aloittaessa tulevaisuudessa valitsen mieluusti modernimman aiheen. AES-salauksen markkinajohtajuudesta huolimatta se on lähes 15 vuotta vanhaa tekniikkaa, ja siitä johtuen joitain dokumentteja ja julkaisuja ei löydy internetistä, paikallisista kirjastoista tai kaupoista, eikä keskustelu aiheesta ole kovin vilkas.

LÄHTEET

Gueron, S.2009. Intel®'s Advanced Encryption Standard (AES) Instructions Set.

[http://download-software.intel.com/sites/default/files/m/6/5/5/4/7/20457-Advanced Encryption Standard 28AES 29 Instructions Set Rev 2 2801 29.pdf](http://download-software.intel.com/sites/default/files/m/6/5/5/4/7/20457-Advanced%20Encryption%20Standard%2028AES%2029%20Instructions%20Set%20Rev%202%20801%2029.pdf)

Krenn, S., Gullasch, D. & Bangerter, E. Cache Games – Bringing Access-Based Cache Attacks on AES to Practice. Luettu 24.3.2013 <http://eprint.iacr.org/2010/594.pdf>

National Institute of Standards and Technology. 26.10.2001. ADVANCED ENCRYPTION STANDARD (EAS). Luettu 24.3.2013

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Salo T. 2005. Tutkintotyö. Puheensalaus tiedonsiirtoverkossa.

<https://publications.theseus.fi/bitstream/handle/10024/10332/TMP.objres.219.pdf?sequence=2>

Microsoft. 30.4.2007. Windows BitLocker Drive Encryption Step-by-Step Guide.

Luettu 12.4.2013 <http://technet.microsoft.com/en-us/library/c61f2a12-8ae6-4957-b031-97b4d762cf31>

Gilbert-Knight, A., Bergfeld, C., Chapman, A. 12.4.2012. An Introduction to Transport Layer Security. Luettu 12.4.2013 <http://www.techsoup.org/support/articles-and-how-tos/introduction-to-transport-layer-security>

Wi-Fi Alliance 2013 Knowledge Center. Luettu 12.4.2013 <http://www.wi-fi.org/knowledge-center/glossary/w>

Keränen, Teeriaho. 2006. Salausmenetelmät osa 2. Luettu 15.4.2013.

http://ta.ramk.fi/~jouko.teeriaho/krypto2006/salausmenetelmat2_7tiivisteetMACitallekirjoitus.pdf

gKrypt. 2012. Luettu 24.4.2013. <http://www.gkrypt.com/>

Learn Networking. 2008. The TCP/IP Stack and the OSI Model. <http://learn-networking.com/tcp-ip/the-tcpip-stack-and-the-osi-model>

LIITTEET

Liite 1. Suorituskykymittaus 100 Kt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
Twofish	46.4 MB/s	52.0 MB/s	49.2 MB/s
AES	45.5 MB/s	44.5 MB/s	45.0 MB/s
Serpent	20.3 MB/s	31.5 MB/s	25.9 MB/s
Twofish-Serpent	18.9 MB/s	20.6 MB/s	19.8 MB/s
AES-Twofish	18.6 MB/s	19.5 MB/s	19.0 MB/s
Serpent-AES	14.1 MB/s	14.3 MB/s	14.2 MB/s
AES-Twofish-Serpent	10.0 MB/s	13.4 MB/s	11.7 MB/s
Serpent-Twofish-AES	11.7 MB/s	10.7 MB/s	11.2 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	68.3 MB/s	70.3 MB/s	69.3 MB/s
Twofish	48.5 MB/s	47.9 MB/s	48.2 MB/s
AES-Twofish	28.4 MB/s	30.8 MB/s	29.6 MB/s
Serpent	20.7 MB/s	32.0 MB/s	26.4 MB/s
Serpent-AES	20.9 MB/s	22.2 MB/s	21.5 MB/s
Twofish-Serpent	18.7 MB/s	19.9 MB/s	19.3 MB/s
AES-Twofish-Serpent	14.6 MB/s	15.9 MB/s	15.3 MB/s
Serpent-Twofish-AES	14.7 MB/s	15.7 MB/s	15.2 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	68.3 MB/s	70.3 MB/s	69.3 MB/s
Twofish	48.5 MB/s	47.9 MB/s	48.2 MB/s
AES-Twofish	28.4 MB/s	30.8 MB/s	29.6 MB/s
Serpent	20.7 MB/s	32.0 MB/s	26.4 MB/s
Serpent-AES	20.9 MB/s	22.2 MB/s	21.5 MB/s
Twofish-Serpent	18.7 MB/s	19.9 MB/s	19.3 MB/s
AES-Twofish-Serpent	14.6 MB/s	15.9 MB/s	15.3 MB/s
Serpent-Twofish-AES	14.7 MB/s	15.7 MB/s	15.2 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 2. Suorituskykymittaus 100 Kt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	205 MB/s	211 MB/s	208 MB/s
Twofish	34.0 MB/s	51.0 MB/s	42.5 MB/s
AES-Twofish	40.1 MB/s	44.8 MB/s	42.4 MB/s
Serpent-AES	28.0 MB/s	28.7 MB/s	28.4 MB/s
Serpent	29.4 MB/s	21.6 MB/s	25.5 MB/s
Twofish-Serpent	18.6 MB/s	13.7 MB/s	16.2 MB/s
Serpent-Twofish-AES	12.0 MB/s	18.8 MB/s	15.4 MB/s
AES-Twofish-Serpent	16.2 MB/s	12.9 MB/s	14.6 MB/s

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	209 MB/s	206 MB/s	208 MB/s
AES-Twofish	40.0 MB/s	43.7 MB/s	41.8 MB/s
Twofish	25.5 MB/s	36.3 MB/s	30.9 MB/s
Serpent	28.6 MB/s	32.4 MB/s	30.5 MB/s
Serpent-AES	27.3 MB/s	29.1 MB/s	28.2 MB/s
Twofish-Serpent	19.1 MB/s	13.9 MB/s	16.5 MB/s
Serpent-Twofish-AES	10.6 MB/s	18.7 MB/s	14.6 MB/s
AES-Twofish-Serpent	15.0 MB/s	12.8 MB/s	13.9 MB/s

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	209 MB/s	218 MB/s	214 MB/s
Twofish	45.9 MB/s	51.8 MB/s	48.9 MB/s
Serpent	31.4 MB/s	29.6 MB/s	30.5 MB/s
AES-Twofish	21.0 MB/s	35.7 MB/s	28.4 MB/s
Serpent-AES	27.8 MB/s	28.4 MB/s	28.1 MB/s
Twofish-Serpent	18.1 MB/s	13.6 MB/s	15.9 MB/s
Serpent-Twofish-AES	17.5 MB/s	12.7 MB/s	15.1 MB/s
AES-Twofish-Serpent	15.5 MB/s	12.8 MB/s	14.2 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 3. Suorituskykymittaus 500 Kt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	68.7 MB/s	70.2 MB/s	69.5 MB/s
Twofish	49.0 MB/s	54.9 MB/s	51.9 MB/s
Serpent	31.6 MB/s	33.3 MB/s	32.4 MB/s
AES-Twofish	28.8 MB/s	31.2 MB/s	30.0 MB/s
Serpent-AES	24.6 MB/s	22.9 MB/s	23.7 MB/s
Twofish-Serpent	21.8 MB/s	22.6 MB/s	22.2 MB/s
Serpent-Twofish-AES	17.0 MB/s	18.2 MB/s	17.6 MB/s
AES-Twofish-Serpent	16.1 MB/s	15.7 MB/s	15.9 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	69.5 MB/s	70.8 MB/s	70.2 MB/s
Twofish	41.4 MB/s	55.5 MB/s	48.5 MB/s
AES-Twofish	28.8 MB/s	31.1 MB/s	29.9 MB/s
Serpent	29.4 MB/s	21.0 MB/s	25.2 MB/s
Twofish-Serpent	21.8 MB/s	23.5 MB/s	22.6 MB/s
Serpent-AES	24.4 MB/s	19.3 MB/s	21.9 MB/s
Serpent-Twofish-AES	17.1 MB/s	18.1 MB/s	17.6 MB/s
AES-Twofish-Serpent	14.1 MB/s	18.1 MB/s	16.1 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	66.4 MB/s	71.3 MB/s	68.9 MB/s
Twofish	49.1 MB/s	55.1 MB/s	52.1 MB/s
Serpent	31.6 MB/s	33.2 MB/s	32.4 MB/s
AES-Twofish	28.8 MB/s	31.2 MB/s	30.0 MB/s
Twofish-Serpent	19.3 MB/s	20.8 MB/s	20.1 MB/s
Serpent-AES	18.7 MB/s	21.3 MB/s	20.0 MB/s
Serpent-Twofish-AES	15.2 MB/s	14.7 MB/s	14.9 MB/s
AES-Twofish-Serpent	13.7 MB/s	13.7 MB/s	13.7 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 4. Suorituskykymittaus 500 Kt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	310 MB/s	313 MB/s	312 MB/s
Twofish	49.0 MB/s	55.5 MB/s	52.3 MB/s
AES-Twofish	35.9 MB/s	43.5 MB/s	39.7 MB/s
Serpent	31.3 MB/s	33.0 MB/s	32.2 MB/s
Serpent-AES	29.1 MB/s	30.2 MB/s	29.6 MB/s
Serpent-Twofish-AES	18.3 MB/s	19.6 MB/s	18.9 MB/s
AES-Twofish-Serpent	18.1 MB/s	19.4 MB/s	18.8 MB/s
Twofish-Serpent	19.1 MB/s	16.5 MB/s	17.8 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	289 MB/s	290 MB/s	289 MB/s
AES-Twofish	42.4 MB/s	34.6 MB/s	38.5 MB/s
Twofish	35.0 MB/s	39.6 MB/s	37.3 MB/s
Serpent-AES	28.9 MB/s	30.1 MB/s	29.5 MB/s
Serpent	31.0 MB/s	27.2 MB/s	29.1 MB/s
Twofish-Serpent	19.3 MB/s	20.8 MB/s	20.1 MB/s
Serpent-Twofish-AES	18.1 MB/s	19.6 MB/s	18.9 MB/s
AES-Twofish-Serpent	17.6 MB/s	14.8 MB/s	16.2 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 KB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	311 MB/s	303 MB/s	307 MB/s
Twofish	48.7 MB/s	54.3 MB/s	51.5 MB/s
AES-Twofish	30.6 MB/s	46.7 MB/s	38.7 MB/s
Serpent	31.3 MB/s	33.3 MB/s	32.3 MB/s
Serpent-AES	29.1 MB/s	30.0 MB/s	29.6 MB/s
AES-Twofish-Serpent	18.1 MB/s	19.5 MB/s	18.8 MB/s
Twofish-Serpent	18.9 MB/s	15.5 MB/s	17.2 MB/s
Serpent-Twofish-AES	14.9 MB/s	19.5 MB/s	17.2 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 5. Suorituskykymittaus 1 Mt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	77.9 MB/s	65.5 MB/s	71.7 MB/s
Twofish	55.4 MB/s	54.4 MB/s	54.9 MB/s
Serpent	35.4 MB/s	37.5 MB/s	36.5 MB/s
AES-Twofish	26.1 MB/s	41.1 MB/s	33.6 MB/s
Serpent-AES	24.7 MB/s	27.8 MB/s	26.3 MB/s
Twofish-Serpent	23.2 MB/s	29.2 MB/s	26.2 MB/s
AES-Twofish-Serpent	19.9 MB/s	21.3 MB/s	20.6 MB/s
Serpent-Twofish-AES	19.7 MB/s	21.3 MB/s	20.5 MB/s

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	61.3 MB/s	70.8 MB/s	66.1 MB/s
Twofish	49.2 MB/s	45.3 MB/s	47.3 MB/s
Serpent	30.6 MB/s	33.4 MB/s	32.0 MB/s
AES-Twofish	28.8 MB/s	29.6 MB/s	29.2 MB/s
Serpent-AES	24.5 MB/s	28.7 MB/s	26.6 MB/s
Twofish-Serpent	23.7 MB/s	24.0 MB/s	23.8 MB/s
Serpent-Twofish-AES	21.6 MB/s	22.0 MB/s	21.8 MB/s
AES-Twofish-Serpent	15.6 MB/s	19.2 MB/s	17.4 MB/s

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	69.0 MB/s	59.1 MB/s	64.1 MB/s
Twofish	49.3 MB/s	55.7 MB/s	52.5 MB/s
Serpent	31.8 MB/s	32.5 MB/s	32.1 MB/s
AES-Twofish	28.7 MB/s	26.1 MB/s	27.4 MB/s
Twofish-Serpent	22.8 MB/s	29.1 MB/s	26.0 MB/s
Serpent-AES	23.1 MB/s	28.7 MB/s	25.9 MB/s
Serpent-Twofish-AES	20.4 MB/s	22.3 MB/s	21.3 MB/s
AES-Twofish-Serpent	15.9 MB/s	18.6 MB/s	17.3 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 6. Suorituskykymittaus 1 Mt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	303 MB/s	309 MB/s	306 MB/s
Twofish	36.3 MB/s	55.4 MB/s	45.9 MB/s
AES-Twofish	32.7 MB/s	47.3 MB/s	40.0 MB/s
Serpent	25.5 MB/s	33.3 MB/s	29.4 MB/s
Serpent-AES	27.0 MB/s	30.2 MB/s	28.6 MB/s
Twofish-Serpent	25.9 MB/s	21.0 MB/s	23.4 MB/s
Serpent-Twofish-AES	18.3 MB/s	19.2 MB/s	18.8 MB/s
AES-Twofish-Serpent	18.1 MB/s	18.4 MB/s	18.3 MB/s

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	299 MB/s	305 MB/s	302 MB/s
Twofish	41.3 MB/s	54.1 MB/s	47.7 MB/s
AES-Twofish	32.5 MB/s	43.8 MB/s	38.1 MB/s
Serpent-AES	32.8 MB/s	34.1 MB/s	33.5 MB/s
Serpent	25.7 MB/s	33.1 MB/s	29.4 MB/s
Twofish-Serpent	26.1 MB/s	27.4 MB/s	26.8 MB/s
Serpent-Twofish-AES	20.6 MB/s	25.7 MB/s	23.2 MB/s
AES-Twofish-Serpent	21.4 MB/s	22.0 MB/s	21.7 MB/s

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	305 MB/s	213 MB/s	259 MB/s
Twofish	48.4 MB/s	55.4 MB/s	51.9 MB/s
AES-Twofish	40.6 MB/s	51.2 MB/s	45.9 MB/s
Serpent-AES	32.7 MB/s	34.1 MB/s	33.4 MB/s
Serpent	31.2 MB/s	29.4 MB/s	30.3 MB/s
Twofish-Serpent	22.9 MB/s	29.8 MB/s	26.3 MB/s
Serpent-Twofish-AES	20.7 MB/s	26.8 MB/s	23.8 MB/s
AES-Twofish-Serpent	22.1 MB/s	19.0 MB/s	20.5 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 7. Suorituskykymittaus 5 Mt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 5 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	91.4 MB/s	81.9 MB/s	86.7 MB/s
Twofish	79.2 MB/s	86.4 MB/s	82.8 MB/s
Serpent	46.0 MB/s	54.6 MB/s	50.3 MB/s
AES-Twofish	46.6 MB/s	46.3 MB/s	46.4 MB/s
Twofish-Serpent	39.4 MB/s	38.4 MB/s	38.9 MB/s
Serpent-AES	35.6 MB/s	38.4 MB/s	37.0 MB/s
Serpent-Twofish-AES	28.5 MB/s	28.2 MB/s	28.4 MB/s
AES-Twofish-Serpent	24.5 MB/s	26.9 MB/s	25.7 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 5 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	91.9 MB/s	87.0 MB/s	89.4 MB/s
Twofish	72.0 MB/s	98.5 MB/s	85.3 MB/s
AES-Twofish	47.5 MB/s	47.3 MB/s	47.4 MB/s
Serpent	36.5 MB/s	51.9 MB/s	44.2 MB/s
Serpent-AES	36.2 MB/s	37.8 MB/s	37.0 MB/s
Twofish-Serpent	36.6 MB/s	37.0 MB/s	36.8 MB/s
Serpent-Twofish-AES	26.1 MB/s	29.8 MB/s	27.9 MB/s
AES-Twofish-Serpent	23.6 MB/s	25.3 MB/s	24.4 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 5 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	90.3 MB/s	90.4 MB/s	90.4 MB/s
Twofish	86.3 MB/s	90.6 MB/s	88.4 MB/s
Serpent	51.9 MB/s	54.7 MB/s	53.3 MB/s
AES-Twofish	48.8 MB/s	49.5 MB/s	49.2 MB/s
Twofish-Serpent	39.1 MB/s	38.7 MB/s	38.9 MB/s
Serpent-AES	37.9 MB/s	38.5 MB/s	38.2 MB/s
Serpent-Twofish-AES	27.2 MB/s	30.1 MB/s	28.6 MB/s
AES-Twofish-Serpent	24.8 MB/s	27.1 MB/s	25.9 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 8. Suorituskykymittaus 5 Mt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 5 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	352 MB/s	315 MB/s	334 MB/s
AES-Twofish	66.7 MB/s	70.9 MB/s	68.8 MB/s
Twofish	73.2 MB/s	63.5 MB/s	68.3 MB/s
Serpent-AES	41.4 MB/s	47.6 MB/s	44.5 MB/s
Serpent	34.5 MB/s	44.4 MB/s	39.4 MB/s
Twofish-Serpent	32.0 MB/s	34.4 MB/s	33.2 MB/s
Serpent-Twofish-AES	29.5 MB/s	31.4 MB/s	30.5 MB/s
AES-Twofish-Serpent	27.2 MB/s	27.5 MB/s	27.3 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 5 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	346 MB/s	357 MB/s	352 MB/s
Twofish	75.8 MB/s	78.0 MB/s	76.9 MB/s
AES-Twofish	63.3 MB/s	69.1 MB/s	66.2 MB/s
Serpent-AES	43.4 MB/s	42.4 MB/s	42.9 MB/s
Serpent	41.3 MB/s	40.0 MB/s	40.6 MB/s
Twofish-Serpent	32.5 MB/s	35.6 MB/s	34.0 MB/s
Serpent-Twofish-AES	29.9 MB/s	31.4 MB/s	30.7 MB/s
AES-Twofish-Serpent	27.0 MB/s	30.2 MB/s	28.6 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 5 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	358 MB/s	360 MB/s	359 MB/s
Twofish	70.2 MB/s	81.6 MB/s	75.9 MB/s
AES-Twofish	58.2 MB/s	76.9 MB/s	67.6 MB/s
Serpent-AES	41.0 MB/s	43.0 MB/s	42.0 MB/s
Serpent	35.3 MB/s	44.4 MB/s	39.9 MB/s
Twofish-Serpent	32.0 MB/s	35.0 MB/s	33.5 MB/s
Serpent-Twofish-AES	31.5 MB/s	31.4 MB/s	31.5 MB/s
AES-Twofish-Serpent	25.9 MB/s	28.5 MB/s	27.2 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 9. Suorituskykymittaus 10 Mt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 10 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	108 MB/s	106 MB/s	107 MB/s
Twofish	99 MB/s	110 MB/s	104 MB/s
Serpent	55.8 MB/s	62.6 MB/s	59.2 MB/s
AES-Twofish	54.7 MB/s	60.1 MB/s	57.4 MB/s
Serpent-AES	46.9 MB/s	46.3 MB/s	46.6 MB/s
Twofish-Serpent	43.0 MB/s	49.6 MB/s	46.3 MB/s
Serpent-Twofish-AES	34.6 MB/s	36.4 MB/s	35.5 MB/s
AES-Twofish-Serpent	31.1 MB/s	32.9 MB/s	32.0 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 10 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	104 MB/s	114 MB/s	109 MB/s
Twofish	97.7 MB/s	115 MB/s	106 MB/s
Serpent	57.7 MB/s	55.5 MB/s	56.6 MB/s
AES-Twofish	53.0 MB/s	55.7 MB/s	54.3 MB/s
Serpent-AES	45.6 MB/s	47.2 MB/s	46.4 MB/s
Twofish-Serpent	42.7 MB/s	49.0 MB/s	45.9 MB/s
Serpent-Twofish-AES	32.8 MB/s	37.0 MB/s	34.9 MB/s
AES-Twofish-Serpent	31.1 MB/s	30.4 MB/s	30.7 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 10 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	99 MB/s	108 MB/s	104 MB/s
Twofish	98.6 MB/s	96.0 MB/s	97.3 MB/s
AES-Twofish	56.0 MB/s	54.1 MB/s	55.1 MB/s
Serpent	56.4 MB/s	51.2 MB/s	53.8 MB/s
Twofish-Serpent	46.5 MB/s	48.1 MB/s	47.3 MB/s
Serpent-AES	44.2 MB/s	46.2 MB/s	45.2 MB/s
Serpent-Twofish-AES	33.5 MB/s	36.5 MB/s	35.0 MB/s
AES-Twofish-Serpent	31.1 MB/s	30.5 MB/s	30.8 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 10. Suorituskykymittaus 10 Mt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 10 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	455 MB/s	366 MB/s	410 MB/s
Twofish	82.3 MB/s	82.1 MB/s	82.2 MB/s
AES-Twofish	72.2 MB/s	75.1 MB/s	73.6 MB/s
Serpent-AES	50.4 MB/s	54.9 MB/s	52.7 MB/s
Twofish-Serpent	41.2 MB/s	42.0 MB/s	41.6 MB/s
Serpent	38.3 MB/s	41.3 MB/s	39.8 MB/s
Serpent-Twofish-AES	35.6 MB/s	37.5 MB/s	36.5 MB/s
AES-Twofish-Serpent	29.3 MB/s	34.0 MB/s	31.6 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 10 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	379 MB/s	455 MB/s	417 MB/s
Twofish	79.7 MB/s	78.3 MB/s	79.0 MB/s
AES-Twofish	69.7 MB/s	76.4 MB/s	73.1 MB/s
Serpent-AES	50.0 MB/s	53.7 MB/s	51.9 MB/s
Serpent	42.4 MB/s	47.4 MB/s	44.9 MB/s
Twofish-Serpent	40.4 MB/s	43.3 MB/s	41.8 MB/s
Serpent-Twofish-AES	35.7 MB/s	37.1 MB/s	36.4 MB/s
AES-Twofish-Serpent	30.9 MB/s	33.0 MB/s	31.9 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 10 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	416 MB/s	454 MB/s	435 MB/s
Twofish	84.4 MB/s	81.5 MB/s	83.0 MB/s
AES-Twofish	70.6 MB/s	77.2 MB/s	73.9 MB/s
Serpent-AES	52.6 MB/s	52.7 MB/s	52.6 MB/s
Serpent	42.3 MB/s	47.8 MB/s	45.0 MB/s
Twofish-Serpent	41.3 MB/s	41.5 MB/s	41.4 MB/s
Serpent-Twofish-AES	35.5 MB/s	36.6 MB/s	36.1 MB/s
AES-Twofish-Serpent	30.2 MB/s	32.9 MB/s	31.5 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 11. Suorituskykymittaus 50 Mt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 50 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	150 MB/s	151 MB/s	151 MB/s
Twofish	130 MB/s	135 MB/s	133 MB/s
Serpent	78.2 MB/s	79.8 MB/s	79.0 MB/s
AES-Twofish	68.7 MB/s	69.0 MB/s	68.9 MB/s
Serpent-AES	50.0 MB/s	52.6 MB/s	51.3 MB/s
Twofish-Serpent	49.1 MB/s	50.0 MB/s	49.6 MB/s
AES-Twofish-Serpent	38.0 MB/s	37.5 MB/s	37.8 MB/s
Serpent-Twofish-AES	37.0 MB/s	38.2 MB/s	37.6 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 50 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	151 MB/s	151 MB/s	151 MB/s
Twofish	129 MB/s	135 MB/s	132 MB/s
Serpent	77.7 MB/s	78.8 MB/s	78.2 MB/s
AES-Twofish	70.9 MB/s	70.7 MB/s	70.8 MB/s
Serpent-AES	50.0 MB/s	52.4 MB/s	51.2 MB/s
Twofish-Serpent	49.1 MB/s	50.5 MB/s	49.8 MB/s
Serpent-Twofish-AES	36.9 MB/s	38.4 MB/s	37.7 MB/s
AES-Twofish-Serpent	37.7 MB/s	35.5 MB/s	36.6 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 50 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	152 MB/s	151 MB/s	152 MB/s
Twofish	129 MB/s	136 MB/s	132 MB/s
Serpent	79.2 MB/s	79.5 MB/s	79.3 MB/s
AES-Twofish	70.8 MB/s	70.7 MB/s	70.7 MB/s
Serpent-AES	51.8 MB/s	51.9 MB/s	51.8 MB/s
Twofish-Serpent	49.4 MB/s	50.1 MB/s	49.8 MB/s
AES-Twofish-Serpent	37.9 MB/s	37.9 MB/s	37.9 MB/s
Serpent-Twofish-AES	36.5 MB/s	38.1 MB/s	37.3 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 12. Suorituskykymittaus 50 Mt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 50 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	549 MB/s	583 MB/s	566 MB/s
Twofish	119 MB/s	132 MB/s	126 MB/s
AES-Twofish	113 MB/s	114 MB/s	114 MB/s
Serpent-AES	67.3 MB/s	74.2 MB/s	70.8 MB/s
Serpent	60.0 MB/s	67.8 MB/s	63.9 MB/s
Twofish-Serpent	50.5 MB/s	51.2 MB/s	50.8 MB/s
Serpent-Twofish-AES	47.5 MB/s	48.3 MB/s	47.9 MB/s
AES-Twofish-Serpent	48.0 MB/s	42.0 MB/s	45.0 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 50 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	549 MB/s	583 MB/s	566 MB/s
Twofish	119 MB/s	132 MB/s	126 MB/s
AES-Twofish	113 MB/s	114 MB/s	114 MB/s
Serpent-AES	67.3 MB/s	74.2 MB/s	70.8 MB/s
Serpent	60.0 MB/s	67.8 MB/s	63.9 MB/s
Twofish-Serpent	50.5 MB/s	51.2 MB/s	50.8 MB/s
Serpent-Twofish-AES	47.5 MB/s	48.3 MB/s	47.9 MB/s
AES-Twofish-Serpent	48.0 MB/s	42.0 MB/s	45.0 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 50 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	474 MB/s	526 MB/s	500 MB/s
Twofish	117 MB/s	128 MB/s	122 MB/s
AES-Twofish	101 MB/s	99 MB/s	100 MB/s
Serpent-AES	73.8 MB/s	74.0 MB/s	73.9 MB/s
Serpent	57.1 MB/s	64.4 MB/s	60.7 MB/s
Twofish-Serpent	50.7 MB/s	51.6 MB/s	51.1 MB/s
Serpent-Twofish-AES	47.8 MB/s	48.3 MB/s	48.1 MB/s
AES-Twofish-Serpent	47.2 MB/s	48.4 MB/s	47.8 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 13. Suorituskykymittaus 100 Mt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	148 MB/s	147 MB/s	148 MB/s
Twofish	126 MB/s	132 MB/s	129 MB/s
Serpent	77.4 MB/s	77.9 MB/s	77.6 MB/s
AES-Twofish	68.4 MB/s	68.7 MB/s	68.5 MB/s
Serpent-AES	50.6 MB/s	51.9 MB/s	51.2 MB/s
Twofish-Serpent	47.0 MB/s	46.9 MB/s	46.9 MB/s
AES-Twofish-Serpent	36.4 MB/s	36.9 MB/s	36.7 MB/s
Serpent-Twofish-AES	36.1 MB/s	36.6 MB/s	36.4 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics. These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	149 MB/s	148 MB/s	149 MB/s
Twofish	126 MB/s	133 MB/s	130 MB/s
Serpent	76.9 MB/s	77.3 MB/s	77.1 MB/s
AES-Twofish	69.7 MB/s	70.8 MB/s	70.2 MB/s
Serpent-AES	47.4 MB/s	50.2 MB/s	48.8 MB/s
Twofish-Serpent	47.0 MB/s	48.4 MB/s	47.7 MB/s
Serpent-Twofish-AES	35.8 MB/s	37.0 MB/s	36.4 MB/s
AES-Twofish-Serpent	36.3 MB/s	22.8 MB/s	29.5 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics. These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	148 MB/s	148 MB/s	148 MB/s
Twofish	121 MB/s	133 MB/s	127 MB/s
Serpent	76.4 MB/s	73.8 MB/s	75.1 MB/s
AES-Twofish	70.0 MB/s	70.8 MB/s	70.4 MB/s
Serpent-AES	49.9 MB/s	50.7 MB/s	50.3 MB/s
Twofish-Serpent	46.0 MB/s	48.4 MB/s	47.2 MB/s
AES-Twofish-Serpent	37.4 MB/s	36.7 MB/s	37.0 MB/s
Serpent-Twofish-AES	35.9 MB/s	36.8 MB/s	36.4 MB/s

Benchmark

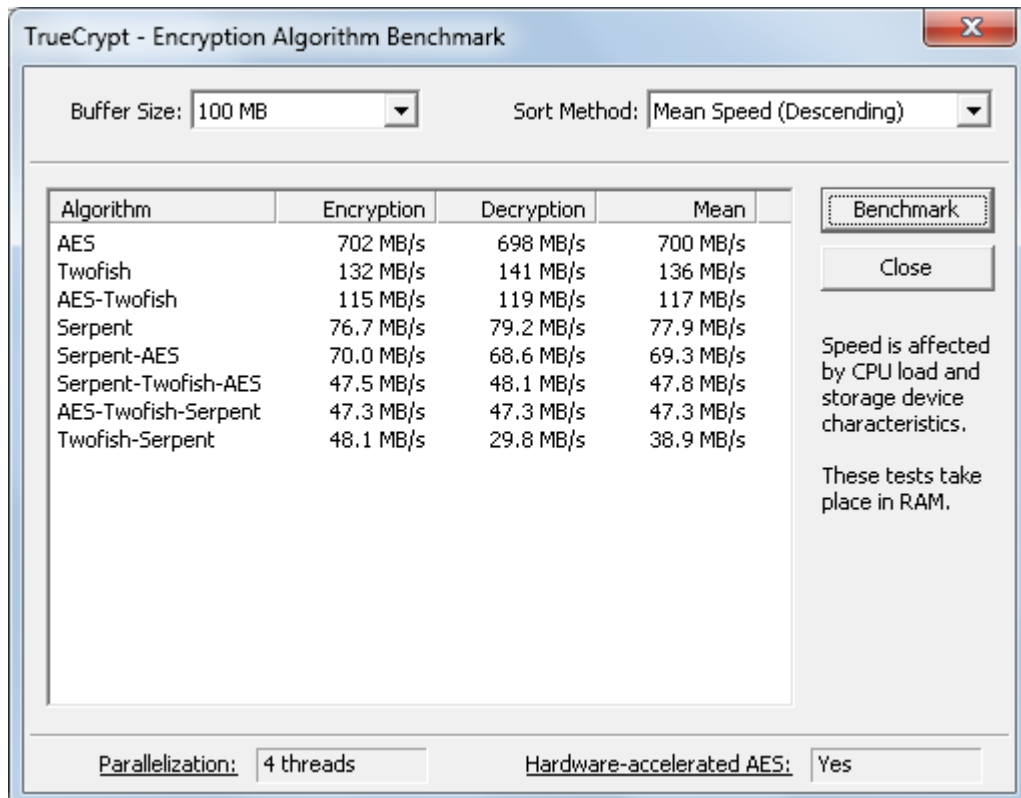
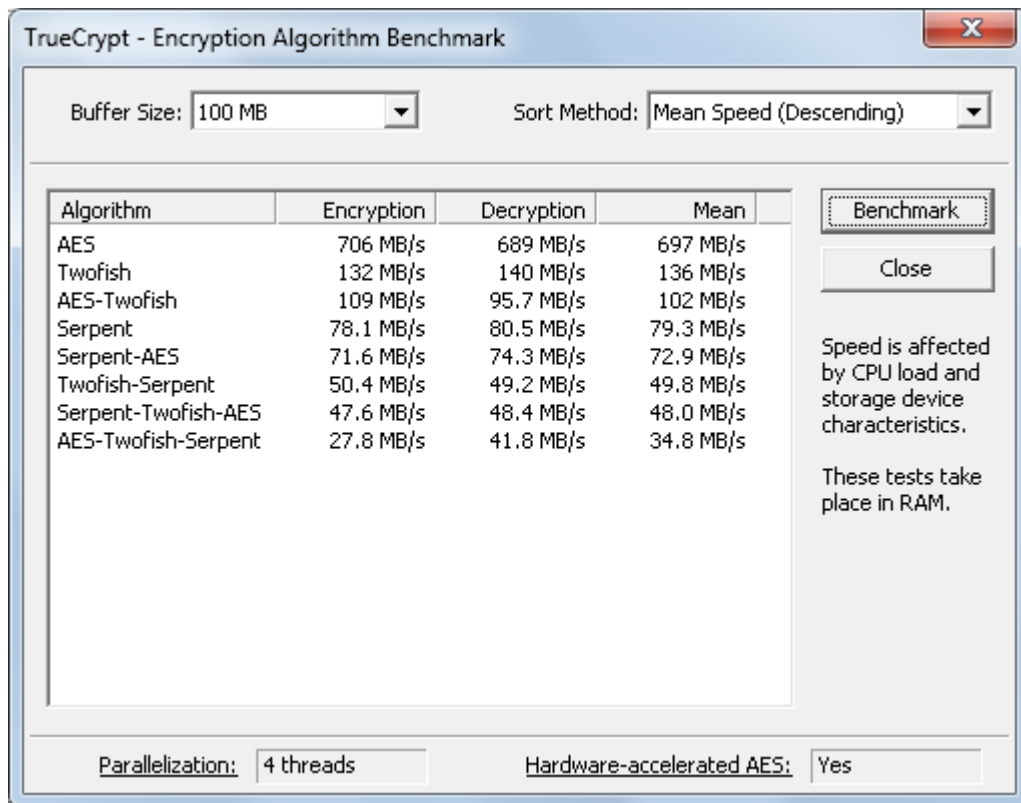
Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 14. Suorituskykymittaus 100 Mt, aes-kiihdytys päällä



TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 100 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	602 MB/s	679 MB/s	640 MB/s
Twofish	133 MB/s	141 MB/s	137 MB/s
AES-Twofish	116 MB/s	119 MB/s	117 MB/s
Serpent	75.5 MB/s	80.1 MB/s	77.8 MB/s
Serpent-AES	75.3 MB/s	73.7 MB/s	74.5 MB/s
Twofish-Serpent	49.2 MB/s	51.2 MB/s	50.2 MB/s
AES-Twofish-Serpent	47.0 MB/s	48.6 MB/s	47.8 MB/s
Serpent-Twofish-AES	47.3 MB/s	48.3 MB/s	47.8 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 15. Suorituskykymittaus 200 Mt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 200 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	145 MB/s	150 MB/s	148 MB/s
Twofish	116 MB/s	132 MB/s	124 MB/s
Serpent	77.1 MB/s	76.1 MB/s	76.6 MB/s
AES-Twofish	69.7 MB/s	69.0 MB/s	69.3 MB/s
Serpent-AES	51.5 MB/s	51.9 MB/s	51.7 MB/s
Twofish-Serpent	47.2 MB/s	48.4 MB/s	47.8 MB/s
Serpent-Twofish-AES	35.8 MB/s	37.4 MB/s	36.6 MB/s
AES-Twofish-Serpent	36.2 MB/s	36.5 MB/s	36.4 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 200 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	150 MB/s	147 MB/s	149 MB/s
Twofish	120 MB/s	134 MB/s	127 MB/s
Serpent	77.2 MB/s	76.8 MB/s	77.0 MB/s
AES-Twofish	68.6 MB/s	69.9 MB/s	69.2 MB/s
Serpent-AES	49.8 MB/s	52.0 MB/s	50.9 MB/s
Twofish-Serpent	46.2 MB/s	44.8 MB/s	45.5 MB/s
AES-Twofish-Serpent	36.4 MB/s	36.7 MB/s	36.6 MB/s
Serpent-Twofish-AES	35.1 MB/s	36.7 MB/s	35.9 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 200 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	148 MB/s	149 MB/s	148 MB/s
Twofish	122 MB/s	127 MB/s	124 MB/s
Serpent	76.7 MB/s	76.1 MB/s	76.4 MB/s
AES-Twofish	65.9 MB/s	69.0 MB/s	67.5 MB/s
Serpent-AES	49.4 MB/s	51.5 MB/s	50.4 MB/s
Twofish-Serpent	46.9 MB/s	48.1 MB/s	47.5 MB/s
Serpent-Twofish-AES	36.3 MB/s	37.3 MB/s	36.8 MB/s
AES-Twofish-Serpent	36.5 MB/s	36.6 MB/s	36.5 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 16. Suorituskykymittaus 200 Mt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 200 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	773 MB/s	798 MB/s	785 MB/s
Twofish	134 MB/s	140 MB/s	137 MB/s
AES-Twofish	116 MB/s	115 MB/s	115 MB/s
Serpent	81.1 MB/s	81.5 MB/s	81.3 MB/s
Serpent-AES	71.2 MB/s	74.2 MB/s	72.7 MB/s
Twofish-Serpent	49.6 MB/s	50.6 MB/s	50.1 MB/s
AES-Twofish-Serpent	47.8 MB/s	46.6 MB/s	47.2 MB/s
Serpent-Twofish-AES	47.0 MB/s	34.5 MB/s	40.7 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 200 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	785 MB/s	783 MB/s	784 MB/s
Twofish	129 MB/s	139 MB/s	134 MB/s
AES-Twofish	114 MB/s	119 MB/s	117 MB/s
Serpent	80.1 MB/s	74.6 MB/s	77.3 MB/s
Serpent-AES	73.6 MB/s	72.5 MB/s	73.0 MB/s
AES-Twofish-Serpent	44.9 MB/s	47.6 MB/s	46.3 MB/s
Twofish-Serpent	35.7 MB/s	49.3 MB/s	42.5 MB/s
Serpent-Twofish-AES	44.5 MB/s	33.6 MB/s	39.1 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 200 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	782 MB/s	782 MB/s	782 MB/s
Twofish	132 MB/s	141 MB/s	136 MB/s
AES-Twofish	114 MB/s	120 MB/s	117 MB/s
Serpent	80.8 MB/s	78.4 MB/s	79.6 MB/s
Serpent-AES	71.1 MB/s	73.6 MB/s	72.4 MB/s
Twofish-Serpent	49.3 MB/s	50.6 MB/s	49.9 MB/s
Serpent-Twofish-AES	47.9 MB/s	47.3 MB/s	47.6 MB/s
AES-Twofish-Serpent	47.5 MB/s	44.8 MB/s	46.2 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 17. Suorituskykymittaus 500 Mt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	148 MB/s	147 MB/s	147 MB/s
Twofish	124 MB/s	130 MB/s	127 MB/s
Serpent	75.7 MB/s	76.3 MB/s	76.0 MB/s
AES-Twofish	68.9 MB/s	69.2 MB/s	69.1 MB/s
Serpent-AES	49.4 MB/s	51.4 MB/s	50.4 MB/s
Twofish-Serpent	48.1 MB/s	49.0 MB/s	48.5 MB/s
AES-Twofish-Serpent	37.1 MB/s	36.9 MB/s	37.0 MB/s
Serpent-Twofish-AES	36.0 MB/s	37.3 MB/s	36.6 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics. These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	147 MB/s	148 MB/s	147 MB/s
Twofish	124 MB/s	129 MB/s	126 MB/s
Serpent	72.6 MB/s	75.3 MB/s	73.9 MB/s
AES-Twofish	64.3 MB/s	59.4 MB/s	61.8 MB/s
Serpent-AES	49.8 MB/s	51.9 MB/s	50.9 MB/s
Twofish-Serpent	47.6 MB/s	49.1 MB/s	48.3 MB/s
AES-Twofish-Serpent	37.0 MB/s	37.1 MB/s	37.0 MB/s
Serpent-Twofish-AES	36.6 MB/s	37.4 MB/s	37.0 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Speed is affected by CPU load and storage device characteristics. These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	148 MB/s	148 MB/s	148 MB/s
Twofish	122 MB/s	118 MB/s	120 MB/s
Serpent	77.2 MB/s	77.5 MB/s	77.4 MB/s
AES-Twofish	69.5 MB/s	69.5 MB/s	69.5 MB/s
Serpent-AES	50.4 MB/s	51.5 MB/s	51.0 MB/s
Twofish-Serpent	47.7 MB/s	49.1 MB/s	48.4 MB/s
Serpent-Twofish-AES	36.3 MB/s	37.5 MB/s	36.9 MB/s
AES-Twofish-Serpent	36.8 MB/s	36.9 MB/s	36.9 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 18. Suorituskykymittaus 500 Mt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	774 MB/s	739 MB/s	756 MB/s
Twofish	189 MB/s	192 MB/s	191 MB/s
AES-Twofish	166 MB/s	172 MB/s	169 MB/s
Serpent	113 MB/s	115 MB/s	114 MB/s
Serpent-AES	72.9 MB/s	73.3 MB/s	73.1 MB/s
AES-Twofish-Serpent	64.9 MB/s	47.8 MB/s	56.3 MB/s
Twofish-Serpent	50.2 MB/s	51.1 MB/s	50.7 MB/s
Serpent-Twofish-AES	46.9 MB/s	47.9 MB/s	47.4 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	1.1 GB/s	1.1 GB/s	1.1 GB/s
Twofish	192 MB/s	204 MB/s	198 MB/s
AES-Twofish	158 MB/s	116 MB/s	137 MB/s
Serpent	117 MB/s	117 MB/s	117 MB/s
Serpent-AES	70.8 MB/s	73.3 MB/s	72.0 MB/s
Twofish-Serpent	49.9 MB/s	51.0 MB/s	50.5 MB/s
AES-Twofish-Serpent	47.3 MB/s	48.0 MB/s	47.7 MB/s
Serpent-Twofish-AES	46.9 MB/s	48.1 MB/s	47.5 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 500 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	1.1 GB/s	1.1 GB/s	1.1 GB/s
Twofish	194 MB/s	154 MB/s	174 MB/s
Serpent	116 MB/s	115 MB/s	115 MB/s
AES-Twofish	111 MB/s	116 MB/s	114 MB/s
Serpent-AES	71.7 MB/s	73.5 MB/s	72.6 MB/s
Twofish-Serpent	45.1 MB/s	51.2 MB/s	48.2 MB/s
Serpent-Twofish-AES	47.3 MB/s	45.7 MB/s	46.5 MB/s
AES-Twofish-Serpent	43.5 MB/s	43.4 MB/s	43.4 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes

Liite 19. Suorituskykymittaus 1 Gt, aes-kiihdytys pois päältä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 GB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	147 MB/s	147 MB/s	147 MB/s
Twofish	126 MB/s	98.7 MB/s	112 MB/s
Serpent	76.2 MB/s	76.6 MB/s	76.4 MB/s
AES-Twofish	66.5 MB/s	69.6 MB/s	68.0 MB/s
Serpent-AES	50.5 MB/s	51.6 MB/s	51.0 MB/s
Twofish-Serpent	50.8 MB/s	46.2 MB/s	48.5 MB/s
Serpent-Twofish-AES	36.8 MB/s	37.5 MB/s	37.1 MB/s
AES-Twofish-Serpent	37.1 MB/s	36.8 MB/s	36.9 MB/s

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 GB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	142 MB/s	146 MB/s	144 MB/s
Twofish	124 MB/s	131 MB/s	128 MB/s
Serpent	74.9 MB/s	76.2 MB/s	75.5 MB/s
AES-Twofish	69.0 MB/s	63.0 MB/s	66.0 MB/s
Serpent-AES	50.1 MB/s	50.8 MB/s	50.5 MB/s
Twofish-Serpent	47.3 MB/s	49.0 MB/s	48.1 MB/s
AES-Twofish-Serpent	37.8 MB/s	36.5 MB/s	37.1 MB/s
Serpent-Twofish-AES	36.0 MB/s	37.5 MB/s	36.7 MB/s

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 GB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	124 MB/s	117 MB/s	121 MB/s
Twofish	94.9 MB/s	116 MB/s	105 MB/s
Serpent	63.9 MB/s	61.5 MB/s	62.7 MB/s
AES-Twofish	49.5 MB/s	49.0 MB/s	49.2 MB/s
Serpent-AES	45.9 MB/s	44.7 MB/s	45.3 MB/s
Twofish-Serpent	34.5 MB/s	50.1 MB/s	42.3 MB/s
AES-Twofish-Serpent	34.4 MB/s	31.0 MB/s	32.7 MB/s
Serpent-Twofish-AES	30.9 MB/s	31.5 MB/s	31.2 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Disabled

Liite 20. Suorituskykymittaus 1 Gt, aes-kiihdytys päällä

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 GB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	1.1 GB/s	1.1 GB/s	1.1 GB/s
Twofish	112 MB/s	138 MB/s	125 MB/s
AES-Twofish	114 MB/s	117 MB/s	116 MB/s
Serpent	116 MB/s	88.4 MB/s	102 MB/s
Serpent-AES	73.1 MB/s	73.8 MB/s	73.5 MB/s
Twofish-Serpent	50.1 MB/s	51.4 MB/s	50.8 MB/s
AES-Twofish-Serpent	47.4 MB/s	48.1 MB/s	47.8 MB/s
Serpent-Twofish-AES	47.3 MB/s	48.0 MB/s	47.7 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 GB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	1.1 GB/s	772 MB/s	926 MB/s
Twofish	128 MB/s	138 MB/s	133 MB/s
AES-Twofish	112 MB/s	116 MB/s	114 MB/s
Serpent	79.5 MB/s	79.2 MB/s	79.4 MB/s
Serpent-AES	71.3 MB/s	72.5 MB/s	71.9 MB/s
Twofish-Serpent	46.5 MB/s	50.1 MB/s	48.3 MB/s
Serpent-Twofish-AES	46.8 MB/s	47.6 MB/s	47.2 MB/s
AES-Twofish-Serpent	46.8 MB/s	47.4 MB/s	47.1 MB/s

Parallelization: 4 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

TrueCrypt - Encryption Algorithm Benchmark

Buffer Size: 1 GB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	949 MB/s	755 MB/s	852 MB/s
Twofish	125 MB/s	132 MB/s	129 MB/s
AES-Twofish	108 MB/s	114 MB/s	111 MB/s
Serpent	78.2 MB/s	78.0 MB/s	78.1 MB/s
Serpent-AES	71.0 MB/s	71.4 MB/s	71.2 MB/s
Twofish-Serpent	51.1 MB/s	49.9 MB/s	50.5 MB/s
AES-Twofish-Serpent	46.0 MB/s	47.0 MB/s	46.5 MB/s
Serpent-Twofish-AES	43.2 MB/s	46.5 MB/s	44.9 MB/s

Benchmark

Close

Speed is affected by CPU load and storage device characteristics.

These tests take place in RAM.

Parallelization: 4 threads Hardware-accelerated AES: Yes