

TESIS

**ANALISIS PERBANDINGAN ALGORITMA
KRIPTOGRAFI AES, DES DAN IDEA YANG TEPAT
UNTUK PERANGKAT MOBILE**



BUDY

No. Mhs : 115301627/PS/MTF

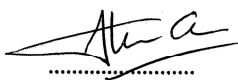
PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA
PROGRAM PASCASARJANA
UNIVERSITAS ATMA JAYA YOGYAKARTA
2013



UNIVERSITAS ATMA JAYA YOGYAKARTA
PROGRAM PASCASARJANA
PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PENGESAHAN TESIS

Nama : BUDY
Nomor Mahasiswa : 115301627/PS/MTF
Konsentrasi : *Mobile Computing*
Judul Tesis : Analisis Perbandingan Algoritma Kriptografi *AES*,
DES dan *IDEA* yang tepat untuk perangkat *mobile*.

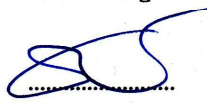
Nama Pembimbing	Tanggal	Tanda Tangan
Prof. Ir. Suyoto, M.Sc., Ph.D	26-03-2013	
Kusworo Anindito, S.T., M.T	26-03-2013	



UNIVERSITAS ATMA JAYA YOGYAKARTA
PROGRAM PASCASARJANA
PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PENGESAHAN TESIS

Nama : BUDY
Nomor Mahasiswa : 115301627/PS/MTF
Konsentrasi : *Mobile Computing*
Judul Tesis : Analisis Perbandingan Algoritma Kriptografi *AES*,
DES dan *IDEA* yang tepat untuk perangkat *mobile*.

Nama Pembimbing	Tanggal	Tanda Tangan
Prof. Ir. Suyoto, M.Sc., Ph.D	19-04-2013	
Kusworo Anindito.,ST., MT	19-04-2013	
Dr. Pranowo, ST, MT	19/04/13	

Ketua Program Studi
Magister Teknik Informatika



Dra. Ernawati, MT.

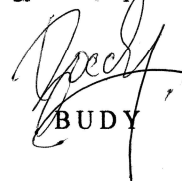
PERNYATAAN

Nama : B U D Y
Nomor Mahasiswa : 115301627 / PS / MTF
Program Studi : Magister Teknik Informatika.
Konsentrasi : *Mobile Computing*
Judul Tesis : Analisis Perbandingan Algoritma Kriptografi
AES, DES dan IDEA yang Tepat Untuk Perangkat
Mobile.

Menyatakan bahwa penelitian ini adalah hasil karya pribadi dan bukan duplikasi dari karya tulis yang telah ada sebelumnya. Karya tulis yang telah ada sebelumnya dijadikan penulis sebagai acuan dan referensi untuk melengkapi penelitian dan dinyatakan secara tertulis dalam penulisan acuan dan daftar pustaka.

Demikian pernyataan ini dibuat untuk digunakan sebagaimana mestinya.

Yogyakarta, April 2013



BUDY

INTISARI

Sistem operasi untuk perangkat mobile semakin berkembang. Android merupakan salah satu sistem operasi mobile yang kian kini sangat populer dan banyak digunakan orang-orang. Android juga merupakan sistem operasi yang berbasis perangkat lunak yang dapat dikembangkan secara terbuka (open source) sehingga banyak pengembang yang kini turut serta ikut mengembangkan aplikasi untuk Android. Keamanan data untuk melakukan proses komunikasi perlu ditingkatkan. Proses teknik mengamankan data yaitu dengan memanfaatkan beberapa jenis algoritma simetri. Dengan adanya banyak algoritma kriptografi yang ditawarkan sampai saat ini, mungkin menjadi salah satu masalah yang menarik untuk diteliti. Untuk itu penulis mencoba menganalisis beberapa algoritma yaitu Data Encryption Standart (DES), Anvanced Encryption Standart (AES) dan Internasional Data Encryption Algorithm (IDEA) yang tepat digunakan untuk aplikasi proses enkripsi dan dekripsi data teks pada perangkat *mobile* sesuai dengan kapasitas spesifikasi perangkat *mobile* tersebut yang tentunya kinerja optimal yang diharapkan yaitu penggunaan resources setiap algoritma tidak terlalu banyak. Penggunaan resources dalam hal ini yaitu CPU, Memory dan Waktu. Algoritma DES lebih diunggulkan dalam kegiatan kriptografi dibandingkan algoritma AES dan IDEA.

Kata kunci : Kriptografi, enkripsi, algoritma simetri, DES, AES, IDEA, mobile.

ABSTRACT

Operating system for mobile devices is growing. Android is a mobile operating system that is now becoming very popular and widely used ones. Android is also the operating system-based software that can be developed openly (open source) so that many developers are now taking part come to develop applications for Android. Data security to make the process of communication needs to be improved. Secure data processing technique is by using some kind of symmetry algorithm. With the existence of many cryptographic algorithms offered so far, may be one of the interesting problems to be studied. To the authors attempted to analyze the algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA) is appropriately used for application data encryption and decryption process text on the mobile device according to the capacity of the mobile device specifications optimal performance is certainly expected that the algorithm does not use any resources too much. The use of resources in this case the CPU, Memory and Time. DES algorithm is more favored in comparison algorithm AES cryptographic activities and IDEA.

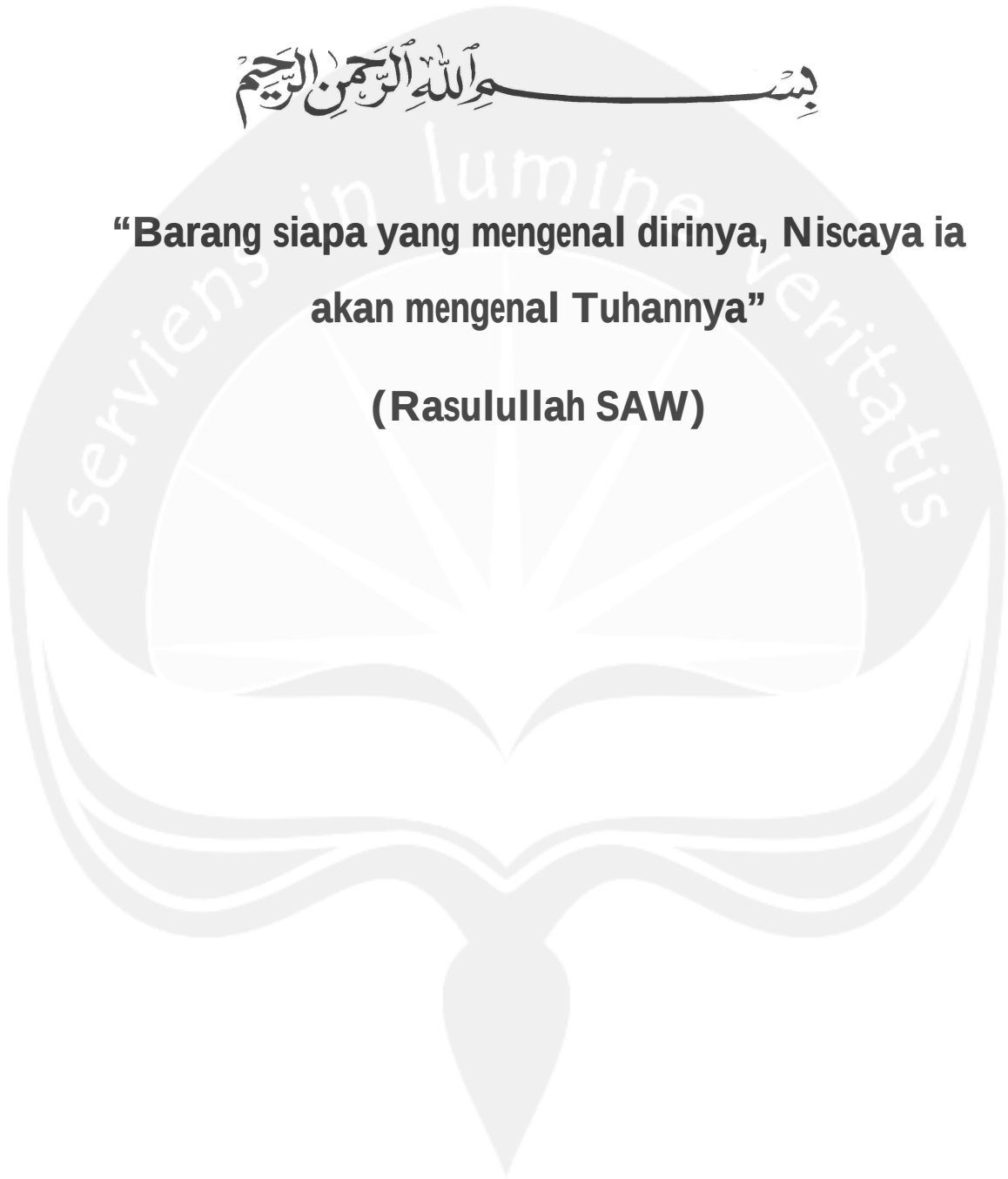
Keywords : cryptography, encryption, symmetric algorithm, DES, AES, IDEA, mobile

MOTTO

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

**“Barang siapa yang mengenal dirinya, Niscaya ia
akan mengenal Tuhannya”**

(Rasulullah SAW)



HALAMAN PERSEMBAHAN

Kupersembahkan penelitian ini untuk semua Manusia yang ada di bumi ini



KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamu'alaikum Wr. Wb

Puji syukur, penulis panjatkan kehadiran Allah SWT, atas rahmat serta hidayah-Nya, sehingga Tesis dengan judul Analisis Perbandingan Algoritma Kriptografi AES, DES dan IDEA yang Tepat Untuk Perangkat Mobile ini dapat terselesaikan.

Tesis ini merupakan salah satu syarat untuk menyelesaikan program studi strata dua (S-2) Jurusan Teknik Informatika pada Program Studi Magister Teknik Informatika Program Pasca Sarjana Universitas Atma Jaya Yogyakarta.

Dalam mengerjakan Tesis ini penulis banyak mendapatkan dukungan dan semangat dari berbagai pihak baik secara langsung maupun tidak. Untuk itu penulis ingin mengucapkan terima kasih yang setulusnya kepada :

1. Sang Pencipta Alam Semesta.
2. Keluarga tercinta papa dan mama (Bpk. Thamrin M. Nur dan Ibu Mardia Marsaoly), Rindy, Ady dan Akbar atas do'a dan kasih sayang yang tulus selama ini semoga selalu diberika nikmat kesehatan dan keselamatan oleh Allah SWT
3. Dra. Ernawati, MT., selaku ketua Program Studi Magister Teknik Informatika Universitas Atma Jaya Yogyakarta.
4. Prof. Ir. Suyoto, M.Sc., Ph.D., selaku dosen pembimbing I yang telah memberikan bimbingan kepada penulis.
5. Kusworo Anindito, ST., MT., selaku dosen pembimbing II yang telah memberikan bimbingan kepada penulis.
6. Dr. Pranowo, ST, MT. Selaku Dosen Penguji. Makasih masukannya pak.

7. Yang Terkasih Melda Gienardy, Makasih atas doa, dukungan, pengertian dan kesabarannya...
8. Teman” kelas MTF September 2011 Pak Patris, Noel, Bayu, Ryan Joko, Mario mimi, Riko Nusa dan Bangsa, Kak Engki, Mas Ardi Leo, Mas Rasyid, Pak Oscar, Bimo, Martinus, Mas Galih, Pak Nazar, Nona Kariting, Mbak Esti, Kak Indry, Kak Melda, Christa Poni, Ibu Suci. Teman-teman MM.. Fandi, ci manti, ria upil, aron, putu, ryan, mario yang selalu kompak dalam segala hal..
9. Keluarga besar penulis di jogja Mama ade sekeluarga..
10. Keluarga besar “PKPM NUKU” asrama : abang anas, iki ogan , alces, jainudin, ilon, laketo, amar, ka ono, amat, ko dul, ansar, ul, taher, noel, faldo, irsanudin, yaser, ardiman, monex, diman paniki, yudi, dex. Gamping : ono, ina, azhul zynga, becardi, ayank, ayy (enam bulan), ade bebe, ami, arif suryo, Zulkarnaeen Zakiya (ZUZA), Haekal Anisa, Reza real madrid club robot, Ean Lolita, leo, isto, mido, reza bule, jessen, ucyt, udu, oji, pangeo, ay dia laju, baladi, upy, bams, opik, ikbal, enda, as, uny, buang. Srikaloka : ais, andika, anto, imin (jang talu add lagi). Andy, itin, rio. Seturan : chimed, pipo, rodik & onco, anto & nita, chibo & dewi. Janti : Abang Helmi & chan, nidus, alex, ul pangeo dan semua teman” yang tak dapat penulis sebutkan satu-persatu. Makasih ee...
11. Keluarga besar di tidore, tete zen & almarhuma nene ajha, nene em, almarhum tete aba, & almarhumah nene cindra, almarhum Papa ade & mama wia, ci linda & ko muis, ko fuad & mba tessa (makasih atas didikannya selama ini ko), aba am & mama tenga, ko tua, kaka itha & mas, mama eba, ino, ano, ata, bibi nona, om nas, onco & ko mi, chicken & kk rini, papa ko, papa ko & mama ade, abang pei, ibu ama & papa akon, kk en & ci bonda, kaiz & ci ma, thunder & ci ica, putet, kekes, latak. Dan semua keluarga yang tak bisa penulis sebutkan satu-persatu, terima kasih yang tak terhingga atas dukungan yang telah diberikan kepada penulis selama ini.

12. NUKU Fc, yang sudah punya banyak piala delapan besar....
13. Ustad A.M Safwan & Semua Teman” Di Rausyan Fikr, makasih...
14. **Teman-teman paaaaaaaalingggggg TERCINTA Jaringan Aktivis Islam Disposesi (JAID)..**

Penulis menyadari bahwa karya ini jauh dari sempurna. Hal ini karena keterbatasan penulis dalam hal wawasan, pengalaman dan penguasaan ilmu yang penulis miliki, oleh karena itu kritik dan saran yang bersifat membangun sangat penulis harapkan.

Akhir kata, dengan segala kerendahan hati penulis mengharapkan semoga karya yang sederhana ini bisa bermanfaat bagi pembaca sekalian. Amin..
Wassalamu’alaikum Wr.Wb.

Yogyakarta, april 2013

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN DOSEN PEMBIMBING.....	ii
HALAMAN PENGESAHAN TIM PENGUJI	iii
HALAMAN PERNYATAAN.....	iv
INTISARI.	v
ABSTRACT	vi
MOTTO.....	vii
HALAMAN PERSEMBAHAN	viii
KATA PENGANTAR	ix
DAFTAR ISI	xii
DAFTAR TABEL	xvii
DAFTAR GAMBAR	xviii
DAFTAR LAMPIRAN.....	xx
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	4
1.3. Batasan Masalah	4
1.4. Keaslian Penelitian.....	4
1.5. Tujuan dan Manfaat Penelitian.....	5

BAB II TINJAUAN PUSTAKA	6
2.1. Tinjauan Pustaka.....	6
2.2. Landasan Teori	8
2.2.1. Kriptografi Secara Umum.....	13
2.2.2. Algoritma Secara Umum.....	13
2.2.3. Algoritma Kriptografi.....	14
2.2.4. <i>Data Encryption Standart (DES)</i>	17
2.2.5. <i>Advanced Encryption Standart (AES)</i>	23
2.2.6. <i>International Data Encryption Standart</i>	26
2.2.7. <i>Android</i>	28
BAB III METODOLOGI PENELITIAN.....	38
3.1. Studi Kepustakaan	38
3.2. Metode Pengembangan Perangkat Lunak	38
3.2.1. Analisis Kebutuhan Perangkat Lunak	38
3.2.2. Perancangan Perangkat Lunak	38
3.2.3. Implementasi Perangkat Lunak (<i>coding</i>)	39
3.2.4. Pengujian Perangkat Lunak	39
BAB IV ANALISIS DAN PERANCANGAN SISTEM.....	40
4.1. Analisis Sistem	40
4.2. Deskripsi Produk	43
4.2.1. Perspektif Produk	43

4.3. Kebutuhan Khusus	44
4.3.1. Kebutuhan Antarmuka Eksternal	44
4.3.1.1. Antarmuka Pemakai	44
4.3.1.2. Antarmuka Perangkat Keras	44
4.3.1.3. Antarmuka Perangkat Lunak	45
4.3.2. Kebutuhan Fungsionalitas Perangkat Lunak	46
4.3.2.1 <i>Use Case Diagram</i>	46
4.4. Perancangan Perangkat Lunak	47
4.4.1. Perancangan Arsitektur Sistem	47
4.4.2. <i>Class Diagram</i>	47
4.4.3. Deskripsi Perancangan Antarmuka	48
4.4.3.1. <i>Splash Screen</i>	48
4.4.3.2. Halaman Utama	49
4.4.3.3. Halaman <i>Comparing Algorithm</i>	50
4.4.3.4. Halaman <i>Encryption</i>	51
4.4.3.5. Halaman <i>Decryption</i>	52
4.4.3.6. Halaman <i>Result</i>	53
BAB V IMPLEMENTASI DAN PENGUJIAN SISTEM	54
5.1. Implementasi Sistem Perangkat Lunak	54
5.2. Pengujian Antarmuka Perangkat Lunak	56
5.2.1. Halaman Menu Utama	56

5.2.2. Halaman <i>Comparing Algorithm</i>	57
5.2.3. Halaman <i>Choose File</i>	58
5.2.4. Halaman <i>Encryption</i>	60
5.2.5. Halaman <i>Decryption</i>	63
5.2.6. Halaman <i>Result</i>	66
5.3. Pengujian Sistem	68
5.3.1. Pengujian Fungsionalitas	68
5.3.2. Pengujian Pengguna	69
5.4. Hasil Pengujian Fungsionalitas	70
5.4.1. Hasil Pengujian <i>use case</i> membandingkan	70
5.4.2. Hasil Pengujian <i>use case</i> mengenkripsi	71
5.4.3. Hasil Pengujian <i>use case</i> mendekripsi	73
5.5. Hasil Pengujian Kinerja Algoritma Pada Perangkat <i>Mobile</i>	75
5.5.1. Pegujian Menggunakan <i>Smartphone</i> Lenovo S560	75
5.6. Analisa Hasil	77
5.7. Kelebihan dan Kekurangan Aplikasi JAID	79
5.7.1. Kelebihan	79
5.7.2. Kekurangan	80
BAB V KESIMPULAN DAN SARAN	81
6.1. Kesimpulan	81
6.2. Saran	82

DAFTAR PUSTAKA	83
----------------------	----

DAFTAR LAMPIRAN	85
-----------------------	----



DAFTAR TABEL

Tabel 2.1 Perbandingan Penelitian	11
Tabel 2.2 Jenis-jenis Algoritma AES	24
Tabel 5.1 Hasil Pengujian menggunakan <i>smartphone</i> Lenovo S560 dengan ukuran <i>file</i> teks (.txt) sebesar 100-500 KB untuk kegiatan Enkripsi.....	76
Tabel 5.2 Hasil Pengujian menggunakan <i>smartphone</i> Lenovo S560 dengan ukuran <i>file</i> teks (.txt) sebesar 435-2.188 KB untuk kegiatan Dekripsi.....	76

DAFTAR GAMBAR

Gambar 2.1 Putaran pertama enkripsi DES (Dony Ariyus, 2008)	19
Gambar 2.2 Rincian DES Fungsi f (Dony Ariyus, 2008)	20
Gambar 2.3 Pemakaian Kunci pada DES.....	21
Gambar 2.4 Gambaran Umum Algoritma DES.....	22
Gambar 2.5 Proses Enkripsi Algoritma AES.....	25
Gambar 2.6 Proses Enkripsi Algoritma IDEA.....	27
Gambar 2.7 Logo Android	28
Gambar 2.8 Arsitektur Android.....	30
Gambar 3.1 Flowchart metodologi penelitian	39
Gambar 4.1 Use Case Diagram.....	46
Gambar 4.2 layer architecture sistem	47
Gambar 4.3 Class Diagram.....	48
Gambar 4.4. Splash Screen JAID	48
Gambar 4.5 Halaman Utama JAID	49
Gambar 4.6. Halaman <i>comparing algorithm</i>	50
Gambar 4.7. Halaman <i>encryption</i> JAID	51
Gambar 4.8 Halaman <i>decryption</i> JAID.....	52
Gambar 4.9 Halaman <i>Result</i> JAID	53
Gambar 5.1 Halaman Menu Utama	56

Gambar 5.2 Halaman <i>Comparing Algorithm</i>	57
Gambar 5.3 Halaman <i>Choose File</i>	58
Gambar 5.4 <i>source code</i> fungsi halaman <i>choose file</i>	59
Gambar 5.5 Halaman <i>Encryption</i>	60
Gambar 5.6 <i>source code</i> menu <i>encryption</i>	61
Gambar 5.6 <i>source code</i> menu <i>encryption</i> (lanjutan).....	62
Gambar 5.7 Halaman <i>Decryption</i>	63
Gambar 5.8 <i>source code</i> menu <i>decryption</i>	64
Gambar 5.8 <i>source code</i> menu <i>decryption</i> (lanjutan).....	65
Gambar 5.9 Halaman <i>Result</i>	66
Gambar 5.10 <i>source code</i> fungsi <i>result</i>	67

DAFTAR LAMPIRAN

Lampiran 1. Spesifikasi Kebutuhan Perangkat Lunak (SKPL).....	86
Lampiran 2. Deskripsi Perancangan Perangkat Lunak (DPPL).....	104

