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
Kosentrasi	:	*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
Kosentrasi	:	*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.

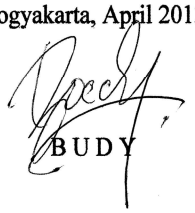
PERNYATAAN

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), Anvanced 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 dibumi ini .....

KATA PENGANTAR

Assalamu'alaikum Wr. Wb

Puji syukur, penulis panjatkan kehadirat 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 Punguji. 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. Keluaga 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, beckardi, 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, chiken & 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 paaaaaaaalinggggggg 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN