PERANCANGAN APLIKASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD BERBASIS ANDROID

SKRIPSI

disusun oleh

Soraya Kusumawati

09.11.3502

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013

PERANCANGAN APLIKASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD BERBASIS ANDROID

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Soraya Kusumawati

09.11.3502

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2013

PERSETUJUAN

SKRIPSI

PERANCANGAN APLIKASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD BERBASIS ANDROID

yang dipersiapkan dan disusun oleh

Soraya Kusumawati

09.11.3502

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 19 Maret 2012

Dosen Pembimbing,

Ema Utami, Dr., S.Si, M.Kom
NIK : 190302037

PENGESAHAN

SKRIPSI

PERANCANGAN APLIKASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD BERBASIS ANDROID

yang dipersiapkan dan disusun oleh

Soraya Kusumawati

09.11.3502

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Juli 2013

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Armadyah Amborowati, S.Kom, M.Eng **NIK : 190302063**	
Ema Utami, Dr., S.Si, M.Kom **NIK : 190302037**	
Dony Ariyus, S.S, M.Kom **NIK : 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 29 Juli 2013

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN KEASLIAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI) , dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan / atau diterbitkan orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 25 Juli 2013

Soraya Kusumawati
09.11.3502

MOTTO

"Hai orang-orang yang beriman, Jadikanlah sabar dan shalatmu sebagai penolongmu, sesungguhnya Allah beserta orang-orang yang sabar"

(Al-Baqarah: 153)

"Setiap cobaan akan terasa ringan, bila disertai kesabaran penuh doa"

"Sesungguhnya sesudah kesulitan itu ada kemudahan"

"Jangan merasa tidak memiliki siapa-siapa karena jika kita memiliki iman, maka kita memiliki Tuhan"

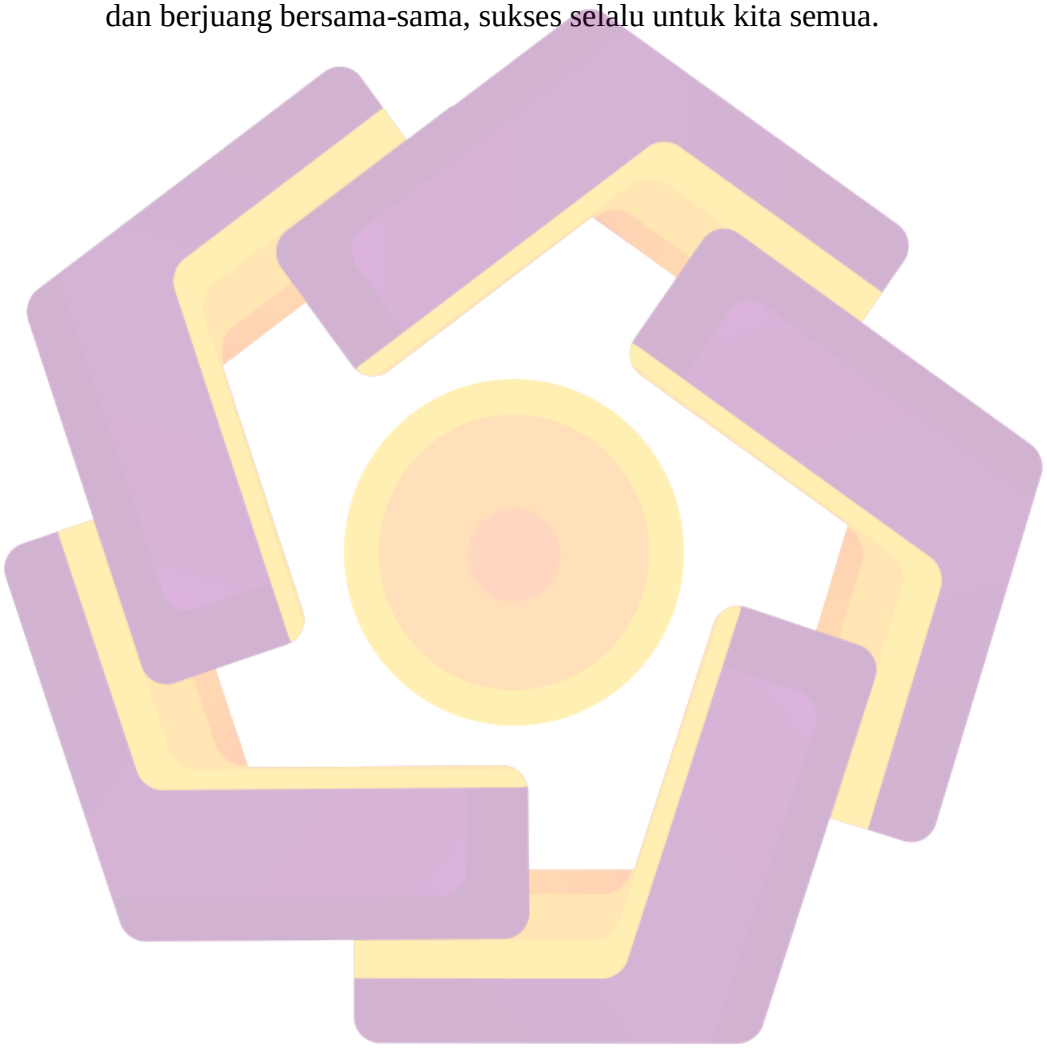
"Jadilah seperti karang di lautan yang kuat dihantam ombak dan kerjakanlah hal yang bermanfaat untuk diri sendiri dan orang lain, karena hidup hanyalah sekali. Ingat hanya pada Allah apapun dan di manapun kita berada kepada Dia-lah tempat meminta dan memohon"

PERSEMBAHAN

Alhamdulillahirrobil'alamin Segala Puji bagi-Mu Ya allah Yang telah melimpahkan segala rezeki, kekuatan, nikmat iman dan islam, sehingga hamba-Mu ini telah menyelesaikan Skripsi dengan diiringi barokah-Mu Ya Allah meskipun kesempurnaan hanyalah milik-Mu. Sholawat serta salam bagi nabi Muhammad SAW, beserta keluarga dan para sahabatnya. Laporan skripsi ini penulis persembahkan untuk :

- Kedua orangtua, kak Sinta yang tak henti-hentinya mendoakan, memberikan dukungan dan memberikan semangat demi terselesaikannya skripsi ini.
- Ibu Ema Utami, Dr., S.Si, M.Kom yang telah membantu dan mendampingi sampai pendadaran, saran, masukan dan revisi serta supportnya yang selalu mengiringi.
- Keluarga besar kelas 09 S1 TI M teman seperjuangan dalam menuntut ilmu, kalian luar biasaa, aku tak merasa seberuntung ini tanpa kalian, dan membuat semua kegiatan di kampus Amikom ini menjadi menyenangkan.
- Andhika Bayu Dewantara, terimakasih untuk dukungannya selama ini dan selalu mengingatkan untuk segera lulus.
- Sahabat-sahabatku penghuni kost Astria Silver House (Cindy Violita Sari, Sany Yulistia Pusparaga, Dhaniar Mustika Sari, Ester Normalita, dan adekku Veti Jayanti) terimakasih atas semangat, doa dan dukungannya.

- Sahabatku tercinta Dhaniar, Niken, Rini yang selalu memotivasi dan memberi semangat untuk menyelesaikan skripsi ini.
- Teman-teman seperjuangan yang tak pernah lelah untuk selalu memotivasi dan berjuang bersama-sama, sukses selalu untuk kita semua.



KATA PENGANTAR

Assalamualaikum Wr.Wb.

Segala puji bagi Allah Tuhan Seluruh Alam yang telah memberikan rahmat, hidayah, rezeki dan segala kesempatan, sehingga penulis dapat menyelesaikan skripsi ini yang berjudul "Perancangan Aplikasi Kriptografi Advanced Encryption Standard Berbasis Android", yang merupakan salah satu persyaratan akademik untuk menyelesaikan pendidikan Strata Satu (S1) Teknik Informatika pada STMIK AMIKOM Yogyakarta.

Dalam penyusunan ini banyak pihak yang membantu secara moril dan materi, yang memberikan penulis kekuatan dan kesabaran dalam menyelesaikan skripsi ini. Oleh karena itu pada kesempatan ini penulis menyampaikan terimakasih kepada :

1. Bapak Prof. Dr. M.Suyanto, M.M selaku ketua Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta
2. Bapak Sudarmawan, M.T selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, Dr., S.Si, M.Kom selaku dosen pembimbing yang telah membimbing, memberikan banyak arahan dan masukan dengan penuh kesabaran sehingga skripsi ini selesai dengan baik.
4. Ibu Armadyah Amborowati, S.Kom, M.Eng dan Bapak Dony Ariyus, S.S, M.Kom selaku dosen penguji yang telah memberikan kritik dan saran.

5. Kedua orang tua dan saudara-saudaraku yang telah memberikan dorongan moral dan materi.
6. Seluruh teman dan sahabatku kelas 09 S1 TI M
7. Semua pihak yang telah membantu dalam penyelesaian Skripsi ini.

Penulis menyadari dengan segala keterbatasan pengetahuan bahwa skripsi ini tentu masih banyak kekurangan dan kesalahan serta jauh dari kata sempurna, maka dari itu penulis mengharapkan masukan, kritik dan saran dari pihak manapun demi penyempurnaan dan perbaikan di masa yang akan datang.

Akhir kata penulis mengharapkan semoga skripsi ini dapat bermanfaat dan dapat digunakan sebagaimana mestinya oleh para pembaca dan sebagai kajian mahasiswa dalam menyusun skripsi.

Yogyakarta, 25 Juli 2013

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Di era informasi global saat ini, kriptografi merupakan suatu bagian yang tidak dapat dipisahkan dari sistem keamanan data karena hal ini berhubungan dengan aspek keamanan dari sebuah data seperti : kerahasiaan data, integritas data dan autentikasi data. Salah satu cara untuk menjaga kerahasiaan data, dibutuhkan proses penyandian data yaitu dengan menggunakan aplikasi yang mampu mengamankan dan menjaga kerahasiaan data tersebut.

Dalam keamanan data terdapat dua aspek utama yaitu proses enkripsi dan dekripsi. Enkripsi dilakukan saat data akan dikirim. Proses ini akan mengubah sebuah data awal menjadi data rahasia atau penyandian data yang tidak dapat dibaca dan diketahui oleh pihak lain. Sementara itu proses dekripsi dilakukan oleh penerima data, dimana data rahasia yang diterima akan diubah kembali menjadi data awal. Sehingga bisa dimengerti oleh penerima data, dimana penerima data harus memiliki kunci dekripsi dari data tersebut. Sehingga perlu diciptakan sebuah aplikasi kriptografi AES sebagai media untuk mengamankan data, agar data tersebut tidak dengan mudah diakses oleh pihak lain.

Perancangan algoritma AES untuk pengiriman pesan di Android bisa menjadi salah satu solusi untuk masalah diatas, aplikasi ini memiliki tampilan yang simpel sehingga aplikasi ini mudah digunakan dan bisa menjadi solusi keamanan dalam bertukar informasi.

Kata kunci :AES, Keamanan Data, Enkripsi, Dekripsi, Android

ABSTRACT

In the current era of global information, cryptography is an inseparable part of the system data security as it relates to the security aspects of the data such as data confidentiality, data integrity and authentication of data. One way to maintain the confidentiality of data, data encryption process that is required to use an application that is able to secure and maintain the confidentiality of such data.

In data security, there are two main aspects: the encryption and decryption process. Encryption is done when the data is sent. This process will transform an initial data into confidential data or data encryption that can not be read and known by others. While the decryption process is done by the data receiver, wherein the received confidential data will be converted back to the initial data.So that it can be understood by the recipient of the data, where the data recipient must have the decryption key from the data. So it is necessary to create an AES cryptographic applications as a medium for securing the data, so that data is not easily accessible to others.

AES algorithm design for sending messages on the Android could be one solution to the problem above, this application has a simple view that this application is easy to use and can be a security solution in exchanging information.

***Keywords**: AES, Data Security, Encryption, Decryption, Android*