IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128 BIT SEBAGAI PENGAMAN SMS PADA SMARTPHONE BERBASIS ANDROID

SKRIPSI

disusun oleh

Joko Tri Susilo Widodo

10.11.3599

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128 BIT SEBAGAI PENGAMAN SMS PADA SMARTPHONE BERBASIS ANDROID

SKRIPSI

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

disusun oleh

Joko Tri Susilo Widodo

10.11.3599

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014

PERSETUJUAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128 BIT SEBAGAI PENGAMAN SMS PADA SMARTPHONE BERBASIS ANDROID

Yang dipersiapkan dan disusun oleh

Joko Tri Susilo Widodo

10.11.3599

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Pebruari 2013

Dosen Pembimbing,

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

PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128 BIT SEBAGAI PENGAMAN SMS PADA SMARTPHONE BERBASIS ANDROID

yang dipersiapkan dan disusun oleh

Joko Tri Susilo Widodo

10.11.3599

telah dipertahankan di depan Dewan Penguji
pada tanggal 27 Januari 2014

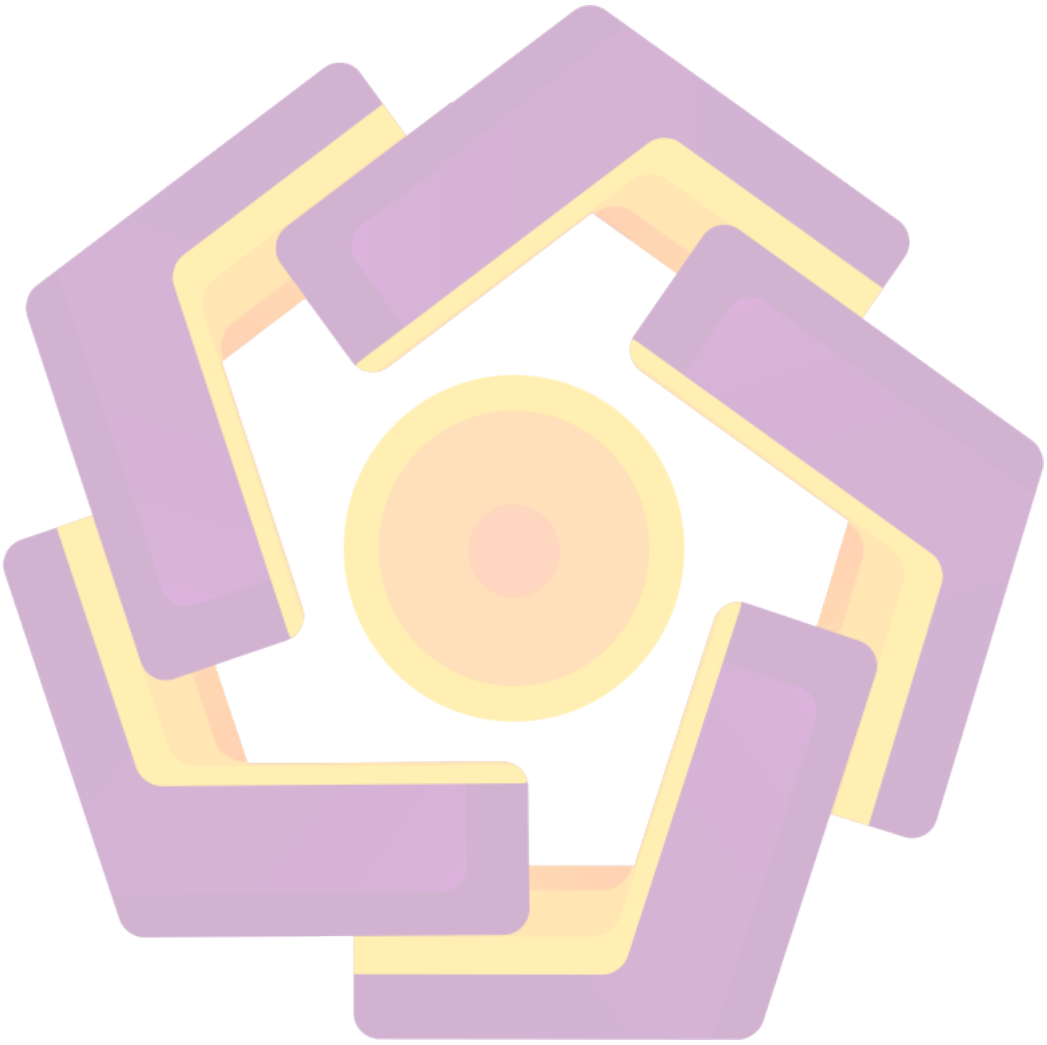
Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ema Utami, Dr., S.Si, M.Kom **NIK. 190302037**	
Barka Satya, M.Kom **NIK. 190302126**	
Ferry Wahyu Wibowo, S.Si., M.Cs **NIK. 190302207**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 7 Pebruari 2014

KETUA STMIK AMIKOM YOGYAKARTA

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



PERNYATAAN

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

Yogyakarta, 7 Februari 2014

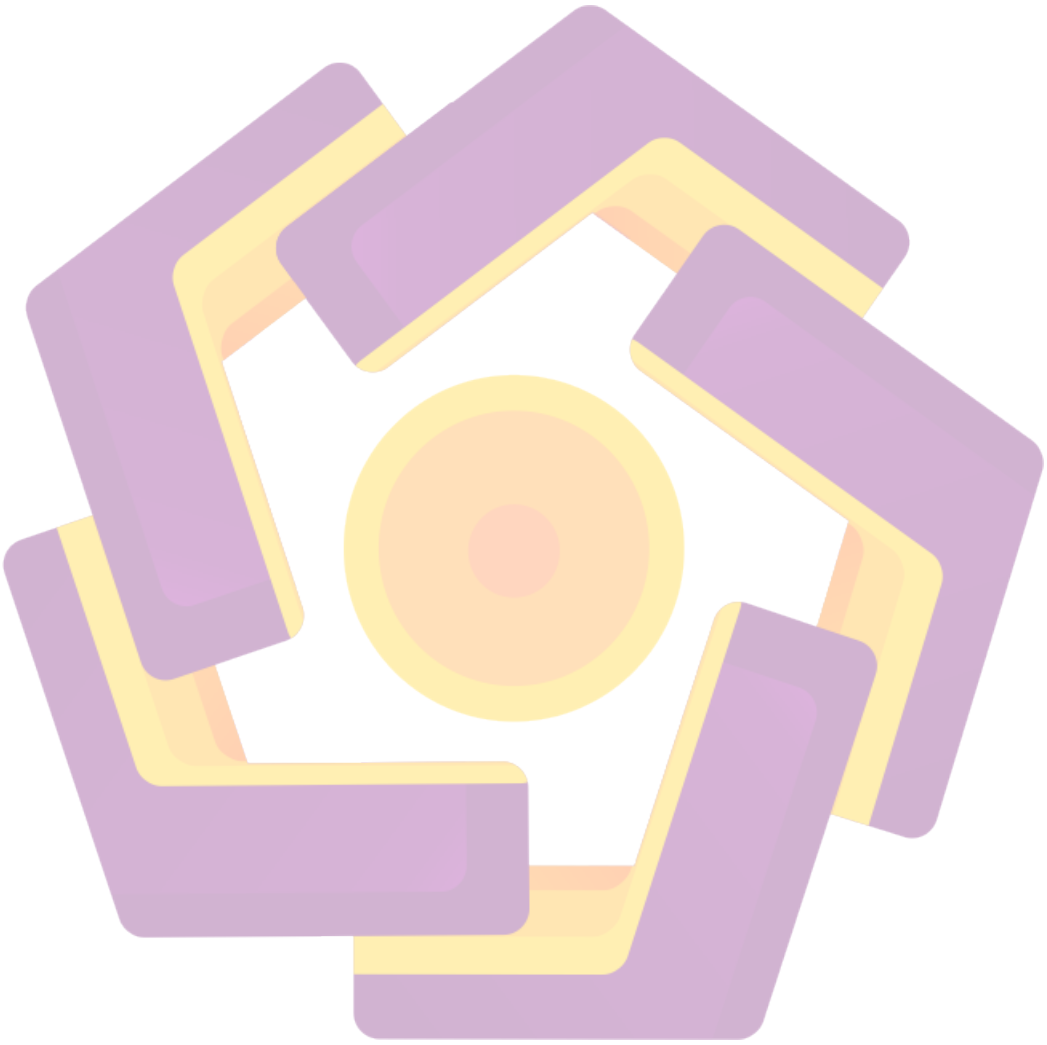
Joko Tri Susilo Widodo

10.11.3599

MOTTO

"Tidak ada cita-cita yang terlalu tinggi, namun yang ada adalah kaesungguhan seseorang yang tidak terlalu tinggi untuk menggapainya"

(Joko Tri Susilo Widodo)



PERSEMBAHAN

Dengan mengucap syukur Alhamdulillah, kupersembahkan karya kecilku ini untuk orang-orang yang kusayangi :

- *Alm. Ayah, yang telah memberikan nama yang hebat kepada anakmu ini.*
- *Bunda dan kedua kakakku tercinta, kalian adalah motivator terbesar dalam hidupku yang tak pernah lelah mendo'akan dan menyayangiku, atas semua pengorbanan dan kesabaran mengantarku sampai kini.*
- *Ibu Ema Utami, terima kasih atas semua bimbingan dan masukan anda yang telah menuntun saya sampai akhir dan mendapatkan hasil yang terbaik.*
- *Keluarga besar 10S1TI-01 angkatan 2010, special thanks to Wahyu Nur Wibowo., Ardian Nur Romadhan., Agustinus Dwi Mawardi., yang selalu memberikan semangat hingga penyusunan skripsi sampai tuntas.*
- *M.Adam Yusup yang telah membantu percetakan Skripsi, M. Alamsyah dan Ardian Nur Romadhan yang telah memberikan pinjaman smartphonenya untuk keperluan ujian.*
- *Keluarga besar Kos Krisna yang telah memberikan hiburan selama ini, sebagai penghilang kepenatan di sela-sela pengerjaan skripsi.*

KATA PENGANTAR

Puji syukur kepada Allah SWT, atas segala nikmat yang telah dicurahkan-nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul ”Implementasi Algoritma Kriptografi Aes 128 Bit Sebagai Pengaman Sms Pada Smartphone Berbasis Android”. Skripsi ini disusun sebagai salah satu persyaratan untuk mencapai derajat Sarjana Komputer di STMIK Amikom Yogyakarta.

Dalam penelitian dan penyusunan skripsi ini, penulis banyak dibantu, dibimbing, dan didukung oleh berbagai pihak. Oleh karena itu, pada kesempatan ini dengan penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada.

1. M. Suyanto, Prof. Dr, M.M. selaku ketua STMIK 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 atas bimbingan, petunjuk dan masukan yang diberikan selama pengerjaan Skripsi ini sejak awal hingga akhir.
4. Bapak Barka Satya, M.Kom dan Bapak Ferry Wahyu Wibowo, S.Si., M.Cs selaku dosen penguji, terima kasih atas saran dan kritiknya yang merupakan langkah awal penyempurnaan skripsi ini.
5. Segenap Dosen dan Karyawan STMIK AMIKOM Yogyakarta yang telah memberikan ilmu pengetahuan dan pengalamannya kepada penulis.

6. Alm. Ayah, ibu dan kakak penulis yang selalu memberikan semangat, dukungan dan doa untuk kelancaran penyelesaian Skripsi ini.
7. Semua pihak yang yang telah membantu dan mendoakan penulis menyelesaikan skripsi ini.

Semoga Allah SWT membalas kebaikan dan ketulusan semua pihak yang telah membantu menyelesaikan skripsi ini dengan melimpahkan rahmat dan karunia-Nya.

Dengan segala kerendahan hati penulis menyadari masih jauh dari kesempurnaan, sehingga penulis mengharapkan adanya saran dan kritik yang bersifat membangun demi kesempurnaan skripsi ini.

Semoga karya penelitian skripsi ini dapat memberikan manfaat dan kebaikan bagi banyak pihak demi kemaslahatan bersama serta bernilai ibadah di hadapan Allah SWT.

Yogyakarta, 21 Februari 2014

Penulis,

Joko Tri Susilo Widodo

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Dewasa ini kasus penyadapan sms semakin meningkat di Indonesia. Pada pembahasan penelitian ini, penulis membangun rancangan aplikasi pengamanan SMS menggunakan algoritma kriptografi AES 128 bit yang diterapkan pada Smart Phone berbasis Android. Penulis memilih Algoritma AES 128 bit karena Algoritma AES menggunakan substitusi, permutasi, dan sejumlah putaran yang dikenakan pada setiap blok yang akan dienkripsi atau didekripsi kemudian untuk setiap putarannya, AES menggunakan kunci yang berbeda, sehingga Algoritma ini tergolong sangat aman dan saat ini masih belum terpecahkan oleh para kriptanalis. Implementasi aplikasi ini direalisasikan dengan menggunakan Eclipse SDK 4.2. Aplikasi yang diterapkan pada Smart Phone Berbasis Android ini diharapkan mampu menjadi salah satu solusi dari kasus tersebut.

Kata Kunci : Implementasi AES, SMS Kriptografi, Pengaman SMS

ABSTRACT

Today wiretapping case sms increasing in Indonesia. In the discussion of this study, the authors build an SMS application design security using 128-bit AES cryptography algorithm is applied to the Smart Phone based on Android. The authors chose 128 bit AES algorithm for AES algorithm using substitution, permutation, and a number of rounds imposed on each block to be encrypted or decrypted, than for every revolution, AES uses a different key, so the algorithm is classified as very secure and is currently still unresolved for cryptanalyst. The implementation of this application realized using Eclipse SDK 4.2. Applications that apply to Android-Based Smart Phone is expected to be one of the solution of the case.

Keyword : *AES Implementation, SMS Cryptography, Secure SMS*