

**IMPLEMENTASI ALGORITMA ENKRIPSI AES PADA APLIKASI SMS
(SHORT MESSAGE SERVICE) BERBASIS ANDROID**

SKRIPSI



disusun oleh

Noni Endriani

10.11.3926

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

**IMPLEMENTASI ALGORITMA ENKRIPSI AES PADA APLIKASI SMS
(SHORT MESSAGE SERVICE) BERBASIS ANDROID**

SKRIPSI

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



disusun oleh

Noni Endriani

10.11.3926

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

PERSETUJUAN

SKRIPSI

IMPLEMENTASI ALGORITMA ENKRIPSI AES PADA APLIKASI SMS (SHORT MESSAGE SERVICE) BERBASIS ANDROID

yang dipersiapkan dan disusun oleh

Noni Endriani

10.11.3926

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 11 November 2013

Dosen Pembimbing,


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

PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA ENKRIPSI AES PADA APLIKASI SMS (SHORT MESSAGE SERVICE) BERBASIS ANDROID

yang dipersiapkan dan disusun oleh

Noni Endriani

10.11.3926

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 April 2014

Susunan Dewan Penguji


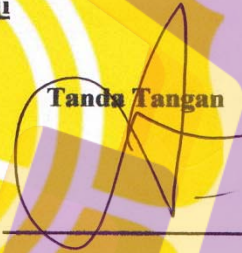
Nama Penguji

Armadyah Amborowati, S.Kom, M.Eng
NIK. 190302063

Ferry Wahyu Wibowo, S.Si., M.Cs
NIK. 190302207

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

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 April 2014

KEPUA STM IK AMIKOM YOGYAKARTA



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

PERNYATAAN

Saya yang bertanda tangan 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 oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 22 April 2014

Noni Endriani

10.11.3926

MOTTO

الله أكبر



HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan kepada :

1. Allah S.W.T yang telah memberi anugerah dan nikmat yang luar biasa tak terhitung kepada hamba-hambanya, Syukur Alhamdulillah. Serta Junjungan Nabi besar Muhammad S.A.W yang membimbing umatnya hingga ke zaman yang penuh berkah ini.
2. Orang tuaku, bapak Andriono & ibu Rochmawati, adekku Nina Agustina dan Erwin Yoga Ardiansyah, dan seluruh keluarga, yang memberi do'a, motivasi dan dukungan dalam bentuk apapun itu. Terima kasih sekali ☺
3. Seluruh civitas akademika STMIK AMIKOM Yogyakarta tanpa terkecuali
4. Ibu dosbing saya Ema Utami Dr, S.Si, M.Kom yang baik hati, yang telah membimbing dan membantu saya hingga pendadaran. Terimakasih ibu ☺
5. Kerabat saya, seluruh anggota keluarga besar S1TI-F & 10-S1TI-05 big thanks for everything, miss you guys ♥
6. Seluruh keluarga besar Teater "MANGGAR" & "AGD", kawan-kawan belajar bareng dan menggila bareng saat seneng, biasa aja, sampe pas lagi stress :D thank you for a wonderful experience :*
7. Keluarga kedua saya di jogja "Kost Flowers 70" Bapak kost: pak Ranto, Ayah: Eka Yuliana, Bunda; Sri Wina, Bungsu: Dina Napita, Primita Medariska, Rasyida Nurul Kamilah, Winarti Riatdiana, Widi. Arigato minasan, untuk pengalaman yang luar biasa, bantuan dan dukungan kalian dalam bentuk apapun, makasih juga printernya hehehe *Hugs :* ☺
8. Kawan-kawan sekolah di Lampung. Kawan-kawan main & ngecamp di Jogja mpok Susi, Louis, Kentang, Wahid em en, mas Dika, Garil Ega dan Iwul yang juga memberi hiburan hihhi kalian luar biasa, makasih ^o^ *ThumbUp
9. Dan untuk yang sudah jadi tempat konsultasiku: Dwi ari, Cahyo, Thanks a lot ^^ juga untuk Stackoverflow.com mhihihi

KATA PENGANTAR



Assalamu'alaikum Wr. Wb.

Alhamdulillah puji syukur kita panjatkan kehadirat Allah SWT yang telah senantiasa melimpahkan rahmat dan anugerah kepada setiap hamba-Nya yang beriman, bertaqwa, dan berikhtiar. Sholawat serta salam senantiasa dilimpahkan kepada junjungan Nabi besar kita Muhammad SAW.

Berkat bimbingan dan pertolongan Allah SWT, maka Skripsi dengan judul “Implementasi Algoritma Enkripsi AES Pada Aplikasi SMS(Short Message Service) Berbasis Android” ini dapat terselesaikan. Banyak hambatan dan kesulitan yang penulis alami dalam penyelesaian skripsi ini, tetapi berkat bimbingan dari berbagai pihak, baik yang bersifat langsung dan tidak langsung, akhirnya penulis dapat menyelesaikan skripsi ini.

Laporan skripsi ini tidak akan terlaksana dengan baik tanpa bantuan dari berbagai pihak. Oleh karena itu, dalam kesempatan ini penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. M Suyanto, MM, Ph.D selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer “Amikom” Yogyakarta

2. Ibu Ema Utami, Dr, S.Si, M.Kom. Selaku dosen pembimbing yang telah memberikan banyak arahan dan masukan kepada penulis
3. Bapak Sudarmawan, M.T selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
4. Tim Penguji, Seluruh dosen dan staf karyawan STMIK AMIKOM Yogyakarta yang telah memberikan ilmu dan bantuannya selama di bangku perkuliahan.
5. Kedua orang tua & keluarga besar, yang sudah mendo'akan serta memberi dukungan moril dan materi.
6. Saudara, kerabat dan seluruh kawan-kawan semua yang sudah memberikan do'a dan dukungannya. Semoga semua bantuan yang diberikan mendapat balasan dari Allah SWT, aamiin.

Penulis menyadari bahwa laporan skripsi ini masih memiliki kekurangan. Penulis mengharapkan kritik dan saran untuk perbaikan skripsi ini. Semoga laporan skripsi ini bermanfaat untuk orang lain.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 22 April 2014

Penulis

DAFTAR ISI

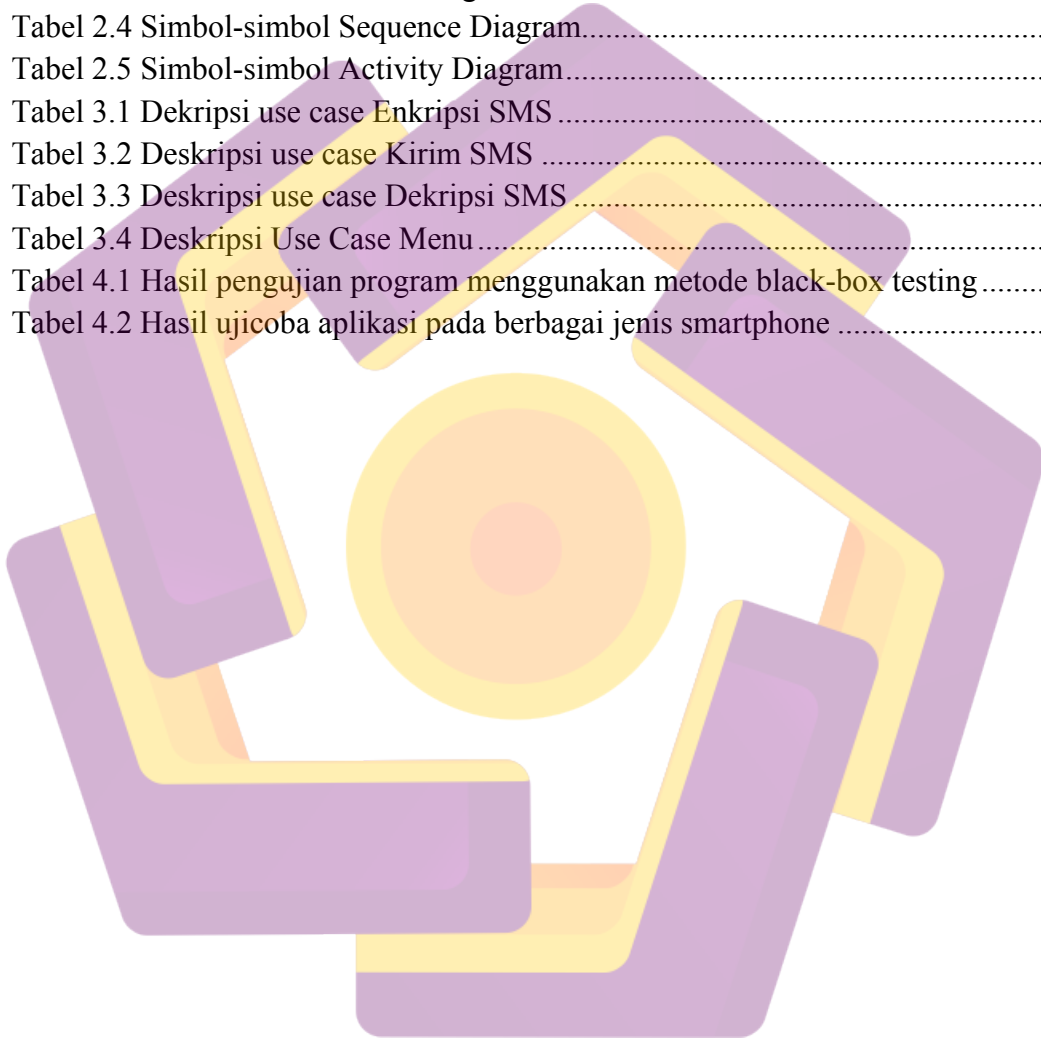
HALAMAN UTAMA.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PENYATAAN.....	iv
HALAMAN MOTTO.....	v
HALAMAN PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
INTISARI.....	xv
ABSTRACT.....	xvi
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat Penelitian.....	4
1.5 Metode Penelitian.....	5
1.6 Sistematika Penulisan.....	6
BAB II LANDASAN TEORI.....	8
2.1 Short Message Service (SMS).....	8
2.1.1 Pengertian Short Message Service (SMS).....	8
2.1.2 Arsitektur Short Message Service (SMS).....	9
2.2 Konsep Dasar Kriptografi.....	12
2.2.1 Pengertian Kriptografi.....	12
2.2.2 Tujuan Kriptografi.....	16

2.2.3	Keamanan Algoritma Kriptografi.....	18
2.3	Algoritma Kriptografi.....	18
2.3.1	Advanced Encryption Standard (AES).....	18
2.4	Android.....	22
2.4.1	Pengertian Android.....	22
2.4.2	Aplikasi.....	23
2.5	Eclipse.....	23
2.5.1	Tentang Eclipse IDE.....	23
2.6	UML.....	24
2.6.1	Use Case.....	25
2.6.2	Class Diagram.....	25
2.6.3	Sequence Diagram.....	26
2.6.4	Activity Diagram.....	27
BAB III	ANALISIS DAN PERANCANGAN SISTEM.....	28
3.1	Analisis.....	28
3.1.1	Analisis SWOT.....	28
3.1.2	Analisis Kebutuhan Awal.....	30
3.1.3	Analisis Kelayakan Sistem.....	31
3.1.4	Analisis Kebutuhan Pengguna.....	32
3.1.5	Kebutuhan Perangkat Keras.....	32
3.1.6	Kebutuhan Perangkat Lunak.....	32
3.1.7	Kebutuhan Implementasi Sistem.....	33
3.2	Perancangan Sistem.....	33
3.2.1	Flowchart Sistem.....	33
3.2.2	Diagram Arus Data Sistem/Data Flow Diagram.....	35
3.2.3	Use Case Diagram.....	36
3.2.4	Class Diagram.....	40
3.2.5	Sequence Diagram.....	41

3.2.6	Activity Diagram	43
3.2.7	Perancangan Antarmuka	45
3.3	Skenario Pengujian	47
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	49
4.1	Implementasi	49
4.1.1	Implementasi Desain	49
4.2	Pembahasan	54
4.2.1	Form Splash Screen	54
4.2.2	Form Tampilan Menu Utama	55
4.2.3	Form Tampilan Create Message	56
4.2.4	Form Tampilan Inbox / Decrypt Message	60
4.2.5	Form Tampilan Menu Help	64
4.2.6	Form Tampilan Menu About	64
4.2.7	Form Tampilan Menu Feedback	65
4.2.8	Kode Pendukung AES	66
4.3	Manual Instalasi	67
4.4	Uji Coba	69
4.4.1	Uji Coba Program	69
4.4.2	Uji Coba Sistem	70
4.5	Pemeliharaan Sistem	72
BAB V	KESIMPULAN DAN SARAN	73
5.1	Kesimpulan	73
5.2	Saran	74
DAFTAR PUSTAKA		75

DAFTAR TABEL

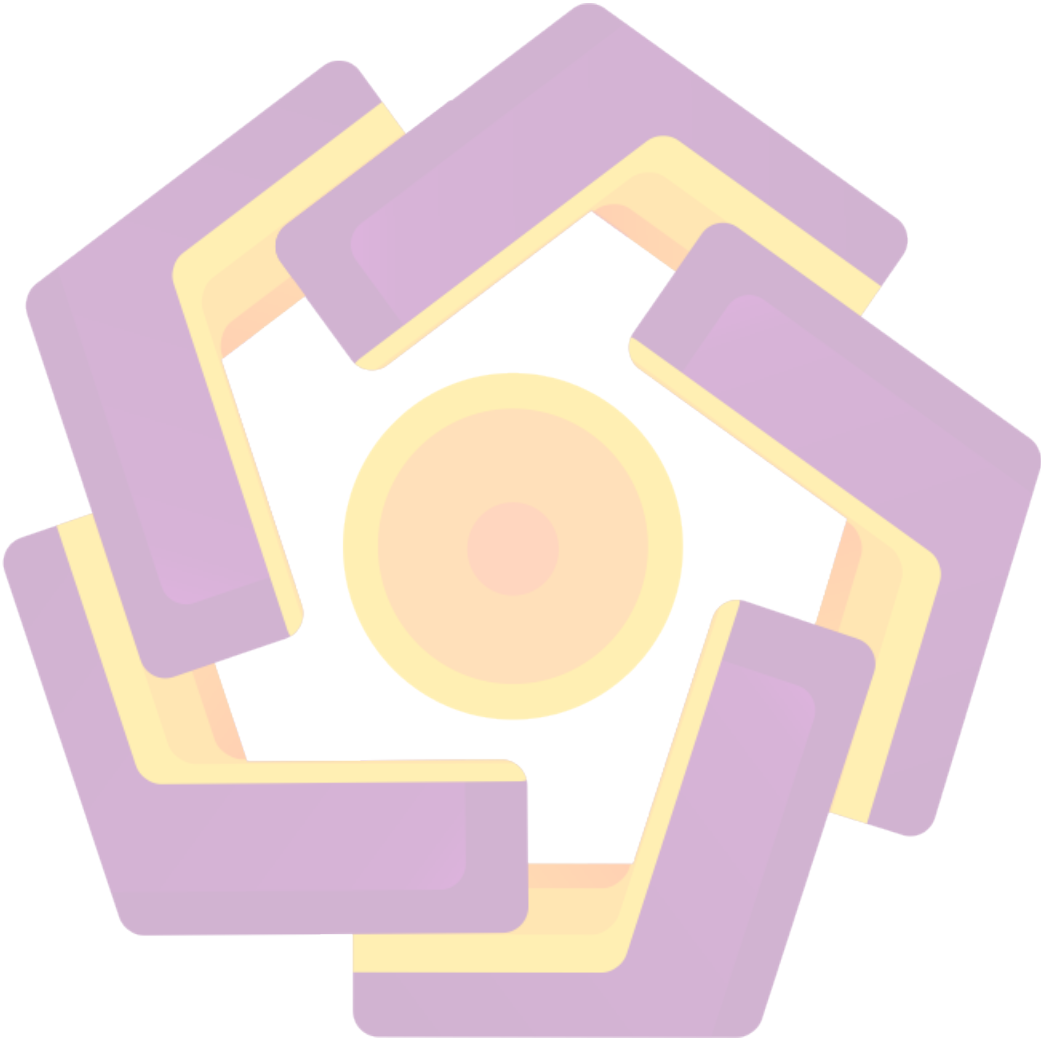
Tabel 2.1 Perbandingan jumlah round dan key.....	19
Tabel 2.2 Simbol-simbol use case diagram.....	25
Tabel 2.3 Simbol-simbol Class Diagram	26
Tabel 2.4 Simbol-simbol Sequence Diagram.....	26
Tabel 2.5 Simbol-simbol Activity Diagram.....	27
Tabel 3.1 Dekripsi use case Enkripsi SMS	37
Tabel 3.2 Deskripsi use case Kirim SMS	38
Tabel 3.3 Deskripsi use case Dekripsi SMS	38
Tabel 3.4 Deskripsi Use Case Menu	39
Tabel 4.1 Hasil pengujian program menggunakan metode black-box testing.....	69
Tabel 4.2 Hasil ujicoba aplikasi pada berbagai jenis smartphone	71



DAFTAR GAMBAR

Gambar 2.1 Struktur SMS.....	8
Gambar 2.2 Arsitektur SMS.....	9
Gambar 2.3 Skema enkripsi dan dekripsi dengan menggunakan kunci.....	15
Gambar 2.4 Skema Ilmu Kriptografi	16
Gambar 2.5 Proses input bytes, state array, dan output bytes.....	20
Gambar 2.6 Ilustrasi proses enkripsi AES	21
Gambar 3.1 Flowchart Aplikasi	34
Gambar 3.2 DFD Level 0 Aplikasi SMS Encryption	35
Gambar 3.3 DFD Level 1 SMS Encryption.....	35
Gambar 3.4 Use case SMS Encryption.....	36
Gambar 3.5 Class diagram SMS Encryption	41
Gambar 3.6 Sequence Diagram use case Mengirim SMS	42
Gambar 3.7 Sequence Diagram use case Terima SMS.....	42
Gambar 3.8 Activity diagram SMS Encryption.....	44
Gambar 3.9 Rancangan form Splash.....	45
Gambar 3.10 Rancangan form Create message	45
Gambar 3.11 Rancangan menu Inbox/decrypt message	46
Gambar 3.12 Rancangan menu aplikasi.....	46
Gambar 3.13 Rancangan menu Help	47
Gambar 3.14 Rancangan menu feedback.....	47
Gambar 4.1 Tampilan splash screen	50
Gambar 4.2 Tampilan Menu Utama.....	50
Gambar 4.3 Tampilan menu Create Message	51
Gambar 4.4 Tampilan menu List Inbox	51
Gambar 4.5 Tampilan menu Inbox	52
Gambar 4.6 Tampilan menu Help.....	52
Gambar 4.7 Tampilan menu About.....	53
Gambar 4.8 Tampilan menu Feedback	53
Gambar 4.9 Kode Form Splash Screen.....	54
Gambar 4.10 Kode Tampilan Menu Utama	56
Gambar 4.11 Kode Tampilan Menu Create message.....	59
Gambar 4.12 Kode Tampilan List Inbox/Form Decrypt.....	63
Gambar 4.13 Kode Tampilan Menu Help.....	64
Gambar 4.14 Kode Tampilan Menu About.....	64

Gambar 4.15 Kode Tampilan Menu Feedback 65
Gambar 4.16 Kode AES..... 67
Gambar 4.17 Tampilan konfirmasi install 68
Gambar 4.18 Aplikasi sukses diinstall..... 68



INTISARI

Pesan singkat atau SMS (*Short Message Service*) merupakan salah satu media komunikasi pertukaran pesan yang masih sangat populer digunakan, meski banyaknya aplikasi pertukaran pesan berbasis internet yang cenderung lebih hemat dan mudah namun masih terhalang pada jaringan kurang stabil.

Android kini menjadi sistem operasi dengan perkembangan paling maju, jumlah perangkat yang menawarkan sistem operasi ini meningkat pesat seiring dengan melonjaknya jumlah pengguna, diiringi dengan kemudahan teknologi komunikasi seharusnya diikuti dengan meningkatnya keamanan, terutama keamanan dalam bertukar informasi, salah satu cara termudah dan terpopuler dalam pertukaran informasi adalah melalui pengiriman pesan singkat (SMS). Umumnya, SMS pada telepon seluler, terutama di Android, sangat rentan terhadap resiko pencurian informasi, penyadapan dan bahkan kehilangan informasi yang penting, karena seringkali pesan yang dikirim bersifat personal dan rahasia. Sehingga, dapat disimpulkan bahwa perlu adanya sebuah aplikasi kriptografi di Android agar pengiriman SMS yang bersifat penting dan rahasia diharapkan dapat dengan aman sampai ke penerima, tanpa khawatir terhadap kebocoran informasi.

Implementasi algoritma enkripsi AES (Advanced Encryption Standard) untuk pengiriman pesan di Android bisa menjadi salah satu solusi untuk masalah diatas, aplikasi ini memiliki tampilan yang simpel dan menarik, sehingga aplikasi ini mudah digunakan dan bisa menjadi solusi keamanan dalam bertukar informasi.

Kata kunci: SMS, Encryption, Decryption, Android, AES

ABSTRACT

Short message service (SMS) is one of the popularly used message exchange communication medias although many internet based message exchange application tend to be more thrifty and easy but still obstructed by unstable networks.

Android is now the operating system with the most advanced developments, the number of devices that offer this operating system increasing rapidly due to the growing number of users, followed by ease of communication technology should be accompanied by increased security, especially security in the exchange of information, one of the easiest and most popular way to exchange information is through short message services (SMS). In general, SMS on mobile phones, especially Android, are particularly vulnerable to the risk of information theft, interception, and even the loss of important information, because frequently sent messages are personal and confidential. So, it can be concluded that it is necessary a cryptographic application in Android that important and confidential SMS delivery is expected can be safely delivered to the recipient, without fear of information leakage.

Advanced encryption standard (AES) algorithm implementation for message delivery in Android could be one solution to the problem above, this application has a simple and attractive appearance, so the application is user friendly and can be a secure solution in exchange of information through SMS.

Keywords: SMS, Encryption, Decryption, Android, AES