

**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**

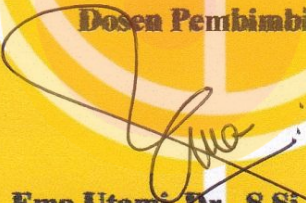
Yang dipersiapkan dan disusun oleh

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

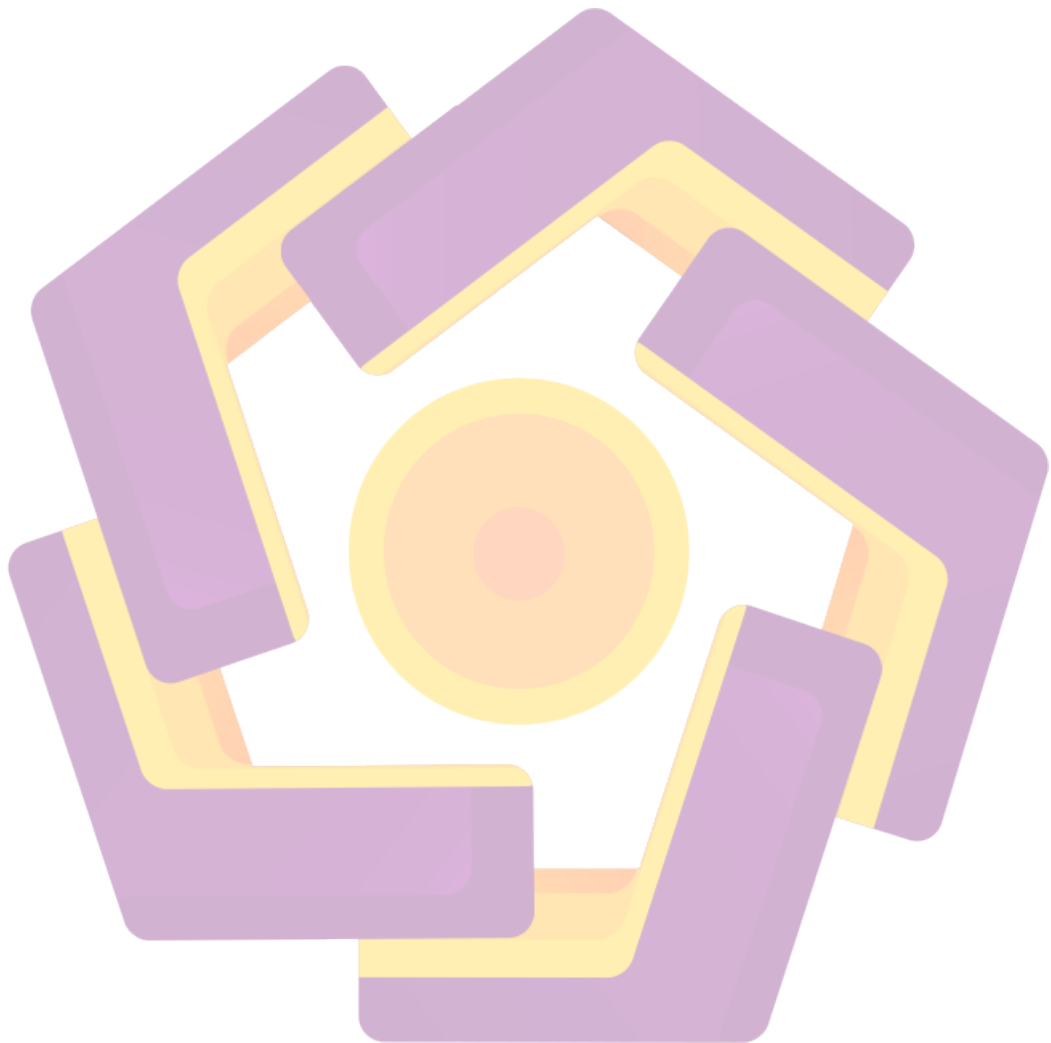
Ferry Wahyu Wibowo, S.Si., M.Cs
NIK. 190302207

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

KEPALA 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 di suatu 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 secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 7 Februari 2014

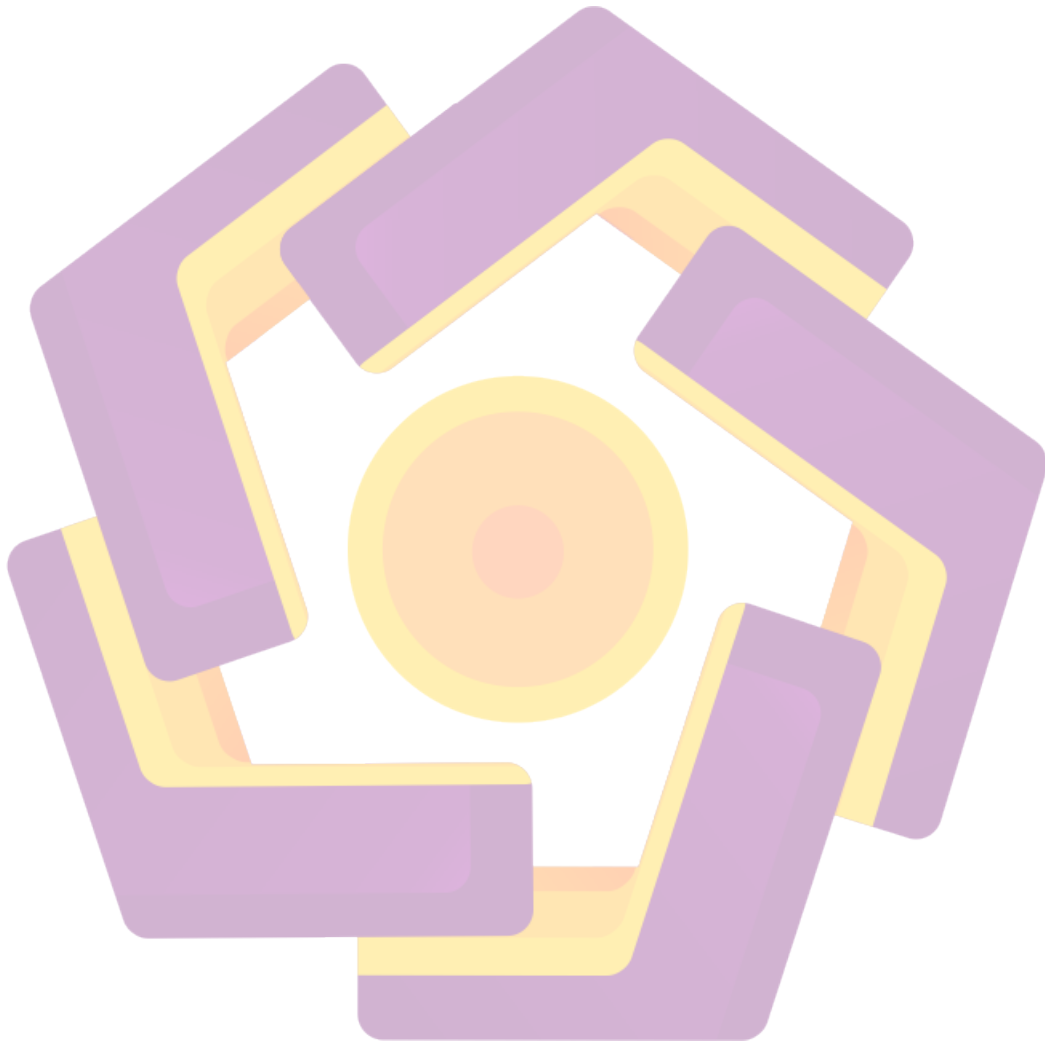
Joko Tri Susilo Widodo

10.11.3599

MOTTO

“Tidak ada cita-cita yang terlalu tinggi, namun yang ada adalah keasungguhan seseorang yang tidak terlalu tinggi untuk menggapainya”

(Joko Tri Susilo Widodo)



PERSEMBAHAN

Dengan mengucapkan 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 Romadhian., 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 Romadhian 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 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,

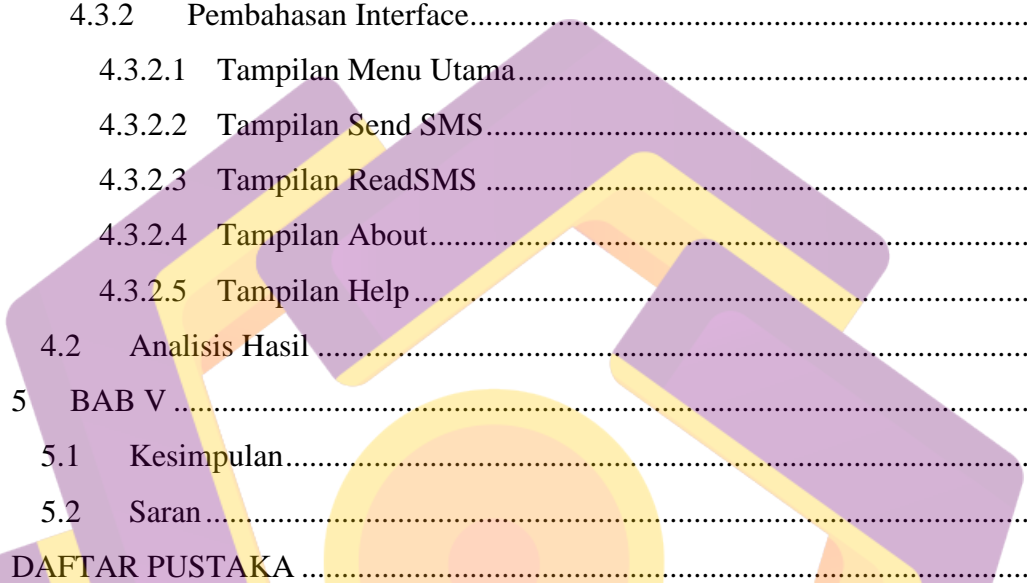
Joko Tri Susilo Widodo

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN	v
HALAMAN MOTTO	vi
HALAMAN PERSEMBAHAN	vii
HALAMAN KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR.....	xv
INTISARI.....	xvii
ABSTRACT.....	xviii
BAB I.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metodologi Penelitian.....	4
1.7 Sistematika Penulisan.....	5
BAB II.....	7
2.1 SMS (Short Message Service).....	7
2.1.1 Cara kerja SMS	7
2.1.2 Elemen Pendukung SMS	8
2.1.1 Keuntungan SMS	9
2.2 Kriptografi.....	10
2.2.1 Algoritma AES 128 bit	11
2.2.1.1 Key Schedule.....	12
2.2.1.2 Add Round Key.....	13
2.2.1.3 SubBytes.....	14

2.2.1.4	Shift Rows	15
2.2.1.5	MixColumns	16
2.3	Android.....	18
2.3.1	Arsitektur Android	18
2.3.1.1	Application dan Widgets	19
2.3.1.2	Application Frameworks	19
2.3.1.3	Libraries.....	20
2.3.1.4	Android Run Time.....	20
2.3.1.5	Linux Kernel.....	21
2.3.2	Fitur Android.....	21
2.3.3	Kronologis Perkembangan Versi Android dan Fitur	22
2.4	Eclipse	28
2.4.1	Android SDK (Software Development Kit).....	29
2.4.2	ADT (Android Delevopment Tools).....	29
2.4.3	Versi peluncuran Eclipse.....	30
BAB III	31
3.1	Analisis	31
3.1.1	Analisis SWOT	31
3.1.1.1	Strength	32
3.1.1.2	Weakness.....	32
3.1.1.3	Opportunity	32
3.1.1.4	Threats	32
3.1.2	Analisi Kebutuhan Awal.....	33
3.1.3	Analisis kelayakan sistem	33
3.1.3.1	Analisis Sistem Operasi.....	34
3.1.3.2	Analisis kelayakan teknik.....	34
3.1.3.3	Analisis Kelayakan Operasional.....	34
3.1.4	Analisis Kebutuhan Pengguna	35
3.1.5	Kebutuhan perangkat keras	35
3.1.6	Kebutuhan Perangkat Lunak	35
3.1.7	Kebutuhan Implementasi Sistem.....	36

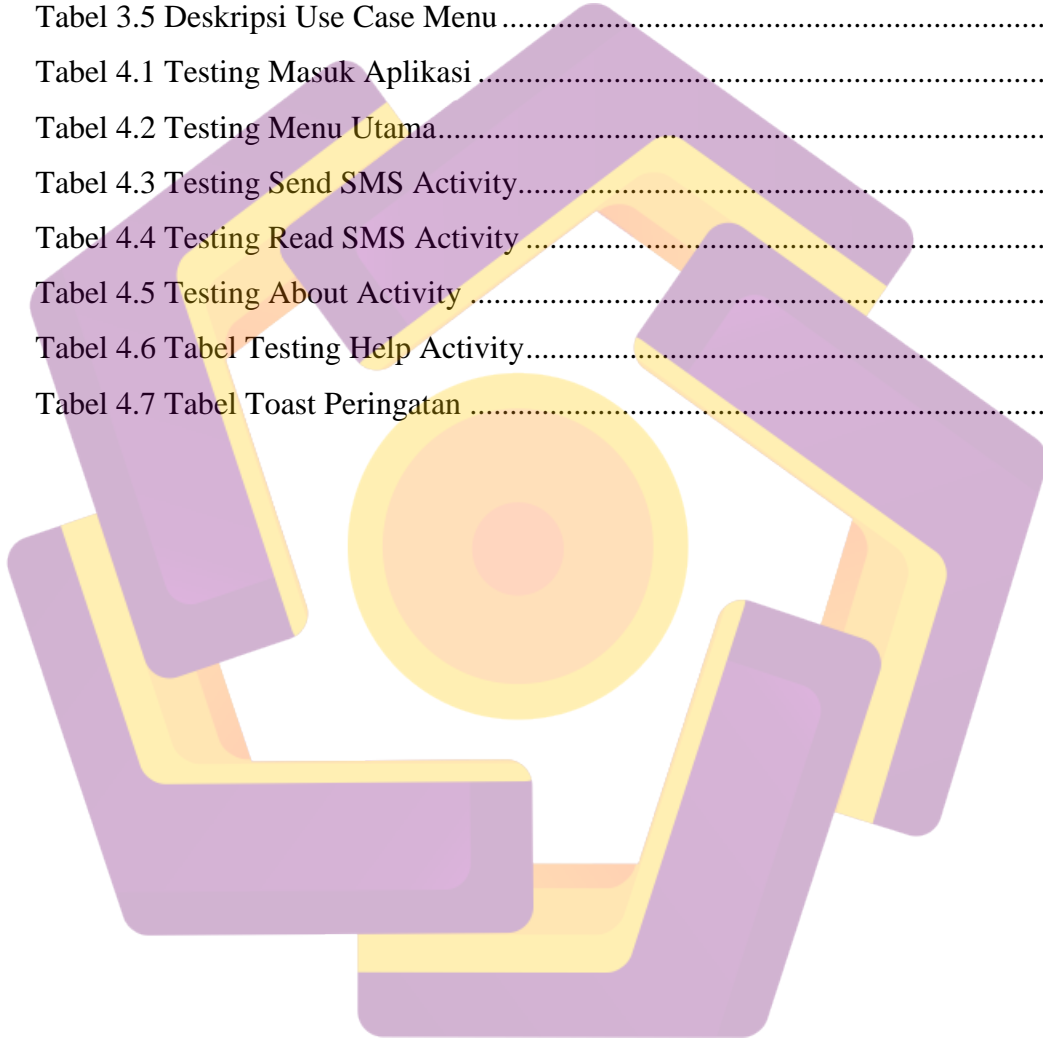
3.2	Perancangan sistem	36
3.2.1	Flowchart Sistem.....	36
3.2.2	Diagram arus data sistem /data flow diagram	39
3.2.3	Usecase Diagram.....	40
3.2.4	Class Diagram	44
3.2.5	Sequence Diagram	45
3.2.6	Activity Diagram.....	47
3.3	Perancangan antarmuka.....	49
3.3.1	Antarmuka Tampilan Utama.....	49
3.3.2	Rancangan Struktur Algoritma AES 128 bit.....	52
3.4	Skenario Pengujian.....	55
BAB IV	56
4.1	Implementasi	56
4.1.1	Manual Instalasi	56
4.2	Pengujian	56
4.2.1	lingkungan pengujian	57
4.2.1.1	Perangkat Lunak	57
4.2.1.2	Perangkat Keras	57
4.2.2	Uji Coba Program	58
4.2.2.1	Kesalahan Dalam Penulisan Program (Syntax Error)	58
4.2.2.2	Kesalahan Proses (Runtime Error)	59
4.2.2.3	Kesalahan Logika (Logic Error).....	60
4.2.2.4	White-box Testing	60
4.2.2.5	Black-box Testing	60
4.2.3	Manual Program.....	72
4.2.3.1	Menu Utama	72
4.2.3.2	Send SMS	72
4.2.3.3	Read SMS	73
4.2.3.4	About	74
4.2.3.5	Help	75
4.3	Pembahasan	75



4.3.1	Pembahasan Listing Program.....	75
4.3.1.1	Class SecureSMS.java.....	75
4.3.1.2	Class AES.java	77
4.3.1.3	Class SendSMS.java.....	79
4.3.1.4	Class InboxSMS.java	80
4.3.2	Pembahasan Interface.....	81
4.3.2.1	Tampilan Menu Utama.....	81
4.3.2.2	Tampilan Send SMS.....	82
4.3.2.3	Tampilan ReadSMS	83
4.3.2.4	Tampilan About.....	83
4.3.2.5	Tampilan Help.....	84
4.2	Analisis Hasil	84
5	BAB V	86
5.1	Kesimpulan.....	86
5.2	Saran.....	86
	DAFTAR PUSTAKA	88

DAFTAR TABEL

Tabel 3.1 Kesimpulan SWOT	33
Tabel 3.2 Deskripsi use case Enkripsi SMS	41
Tabel 3.3 Deskripsi use case Kirim SMS	42
Tabel 3.4 Deskripsi usecase Dekripsi SMS	43
Tabel 3.5 Deskripsi Use Case Menu	43
Tabel 4.1 Testing Masuk Aplikasi	61
Tabel 4.2 Testing Menu Utama.....	63
Tabel 4.3 Testing Send SMS Activity.....	64
Tabel 4.4 Testing Read SMS Activity	65
Tabel 4.5 Testing About Activity	66
Tabel 4.6 Tabel Testing Help Activity.....	67
Tabel 4.7 Tabel Toast Peringatan	70



DAFTAR GAMBAR

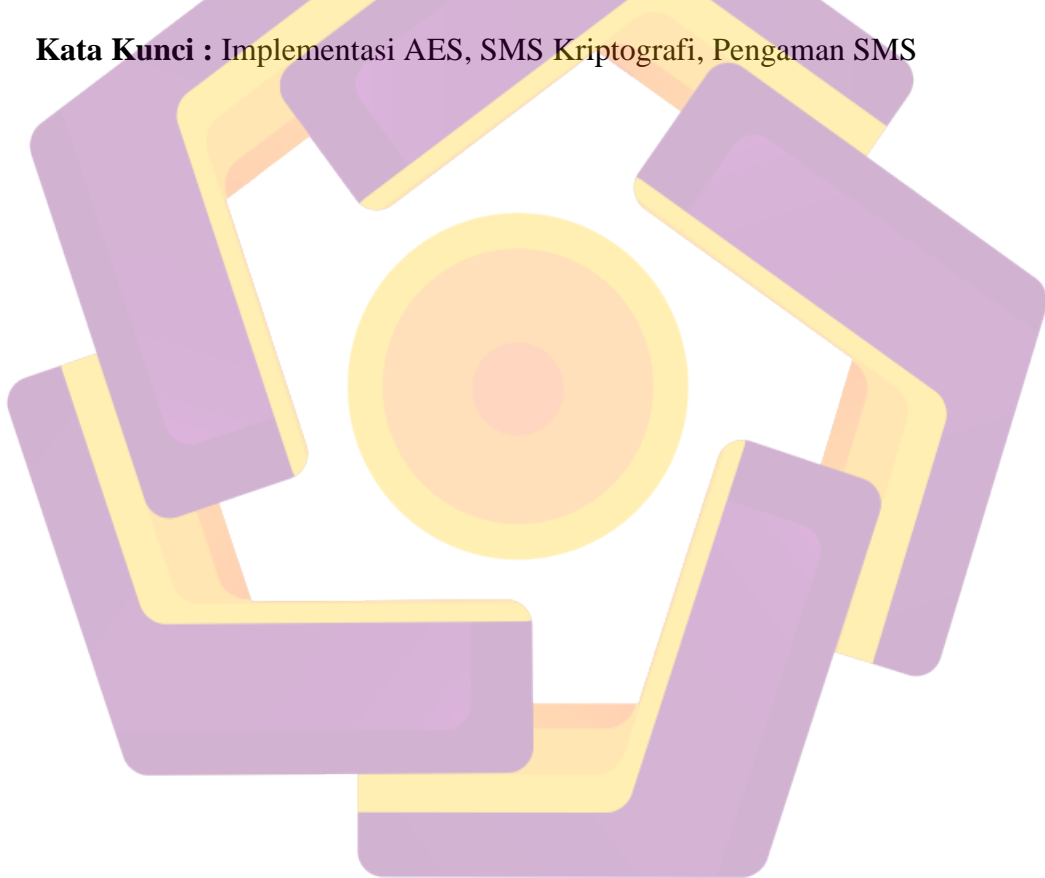
Gambar 2.1 Skema Kerja SMS	8
Gambar 2.2 Elemen jaringan penyusun layanan SMS.....	8
Gambar 2.3 Konsep Kriptografi Secara Umum.....	11
Gambar 2.4 Proses <i>add round key</i>	14
Gambar 2.5 S-Box.....	15
Gambar 2.6 Proses Sub-Bytes.....	15
Gambar 2.7 Proses <i>shift rows</i>	16
Gambar 2.8 Proses <i>mix columns</i>	17
Gambar 2.9 Arsitektur Android	19
Gambar 2.10 Logo Android 1.5 (Cupcake)	23
Gambar 2.11 Logo Android versi 1.6 (Donut).....	24
Gambar 2.12 Logo Android versi 2.0 (Eclair).....	24
Gambar 2.13 Logo Android 2.2 (Froyo).....	25
Gambar 2.14 Logo Android 2.3 (GingerBread).....	25
Gambar 2.15 Logo Android versi 3.0 (HoneyComb)	26
Gambar 2.16 Logo Android versi 4.0 (ICS/Ice Cream Sandwich).....	27
Gambar 2.17 Logo Android 4.1 (Jelly Bean).....	28
Gambar 3.1 Flowchart Aplikasi SMSKripto.....	37
Gambar 3.2 Flowchart Simulasi Pengguna Mengirim SMS.....	38
Gambar 3.3 Flowchart Simulasi Pengguna Membaca SMS	38
Gambar 3.4 Context Diagram	39
Gambar 3.5 DFD level 0	40
Gambar 3.6 Use case SMS Kripro	41
Gambar 3.7 Class Diagram	45
Gambar 3.8 Sequence Diagram Enkripsi SMS	46
Gambar 3.9 Sequence Diagram Dekripsi SMS.....	46
Gambar 3.10 Activity Diagram Secure SMS.....	48
Gambar 3.11 Rancangan form Utama.....	49
Gambar 3.12 Rancangan form Send Message	50
Gambar 3.13 Rancangan form Inbox(derypt) Messages.....	51

Gambar 3.14 Rancangan form About	51
Gambar 3.15 Rancangan form Help.....	52
Gambar 4.1 Syntax Error	59
Gambar 4.2 Runtime Error Force close	59
Gambar 4.3 Tampilan Awal Aplikasi	61
Gambar 4.4 Send SMS berhasil	62
Gambar 4.5 Read SMS berhasil	62
Gambar 4.6 About berhasil	63
Gambar 4.7 Help berhasil	63
Gambar 4.8 Look-up kontak berhasil	64
Gambar 4.9 Pesan ter-enkripsi dan berhasil.....	64
Gambar 4.10 Pesan berhasil di-dekripsi.....	65
Gambar 4.11 About berhasil tampil	66
Gambar 4.12 Help Berhasil Tampil	67
Gambar 4.13 Peringatan Pengisian Nomor Tujuan.....	68
Gambar 4.14 Peringatan Pengisian Pesan	68
Gambar 4.15 Peringatan Pengisian Key	69
Gambar 4.16 Pesan Peringatan Input Pesan Melebihi 80 Karakter	69
Gambar 4.17 Peringatan Key Melebihi 16 Karakter.....	70
Gambar 4.18 Tampilan Menu Utama.....	72
Gambar 4.19 Tampilan SendSMS Activity	73
Gambar 4.20 Tampilan InboxActivity	74
Gambar 4.21 Tampilan About Activity	74
Gambar 4.22 Tampilan About Activity	75
Gambar 4.23 Tampilan Menu Utama.....	82
Gambar 4.24 Tampilan Send SMS	82
Gambar 4.25 Tampilan Read SMS	83
Gambar 4.26 Tampilan About.....	83
Gambar 4.27 Tampilan Help.....	84
Gambar 4.28 Perbandingan kombinasi key	85
Gambar 4.29 Perbandingan kombinasi key dengan karakter yang lebih panjang	85

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*

