

**ANALISIS DAN PERANCANGAN APLIKASI ENKRIPSI SMS DENGAN
KOMBINASI METODE SUBSTITUSI DAN AES BERBASIS ANDROID
DI KALANGAN MAHASISWASTMIK “AMIKOM” YOGYAKARTA**

SKRIPSI



disusun oleh

Mimbar Sutisna Wangsadiria

09.11.3134

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

**ANALISIS DAN PERANCANGAN APLIKASI ENKRIPSI SMS DENGAN
KOMBINASI METODE SUBSTITUSI DAN AES BERBASIS ANDROID
DI KALANGAN MAHASISWA STMIK “AMIKOM” YOGYAKARTA**

SKRIPSI

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



disusun oleh

Mimbar Sutisna Wangsadiria

09.11.3134

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

PERSETUJUAN

SKRIPSI

**ANALISIS DAN PERANCANGAN APLIKASI ENKRIPSI SMS DENGAN
KOMBINASI METODE SUBSTITUSI DAN AES BERBASIS ANDROID
DI KALANGAN MAHASISWA STMIK "AMIKOM" YOGYAKARTA**

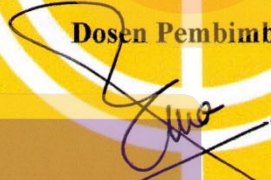
yang dipersiapkan dan disusun oleh

Mimbar Sutisna Wangsadiria

09.11.3134

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 30 Oktober 2012

Dosen Pembimbing,


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

PENGESAHAN

SKRIPSI

ANALISIS DAN PERANCANGAN APLIKASI ENKRIPSI SMS DENGAN KOMBINASI METODE SUBSTITUSI DAN AES BERBASIS ANDROID DI KALANGAN MAHASISWA STMIK "AMIKOM" YOGYAKARTA

yang dipersiapkan dan disusun oleh

Mimbar Sutisna Wangsadiria

09.11.3134

telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Juni 2013

Susunan Dewan Penguji

Nama Penguji

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

Emha Taufiq Luthfi, ST, M.Kom
NIK. 190302125

Joko Dwi Santoso, M.Kom
NIK. 190302181

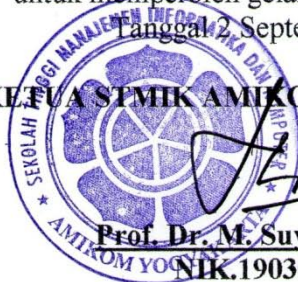
Fanda Tangan



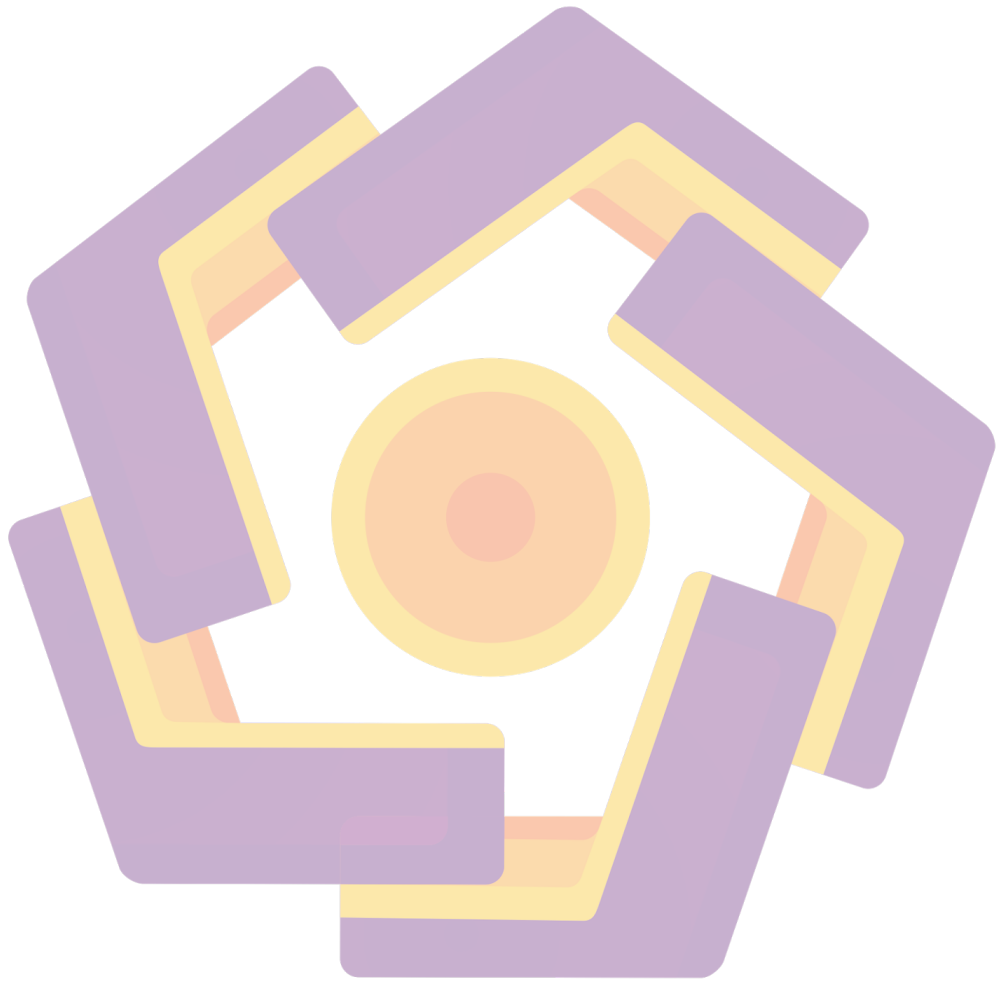


Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 2 September 2013

KETUA STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suvanto, M.M.
NIK.190302001



PERNYATAAN

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

Yogyakarta, 24 Juni 2013

Mimbar Sutisna Wangsadiria

09.11.3134



MOTTO

- ✚ Sesungguhnya Allah tidak merubah keadaan suatu kaum sehingga mereka merubah keadaan yang ada pada diri mereka sendiri (Q.S. Ar Ra'd : 11).
- ✚ Harapan adalah tiang yang menyangga dunia (Gaius Plinius Secundus/ Pliny the Elder).
- ✚ Pendidikan memiliki akar yang pahit, namun buahnya manis (Aritoteles).
- ✚ Jangan takut untuk mencoba, karena ketakutan itulah hambatan sesungguhnya dari sebuah kesuksesan kita (Mario Teguh).
- ✚ Rasa malas adalah cara Setan mencegahmu mencapai keberhasilanmu. Jika engkau bukan orang yang penting di masa depan, Setan tak akan berletih-letih menggangumu dengan rasa malas dan pesimisme hari ini. Setan hanya mengganggu orang yang sejatinya hebat (Mario Teguh).
- ✚ Saya hanyalah seorang manusia, tetapi saya adalah seseorang. Saya tidak dapat melakukan segalanya, tetapi saya dapat melakukan sesuatu. Saya tidak akan menolak melakukan sesuatu yang dapat saya lakukan (Helen Keller).
- ✚ Siapapun yang belum pernah melakukan kesalahan, tidak pernah mencoba sesuatu yang baru (Albert Einstein).

HALAMAN PERSEMBAHAN

Skripsi ini dipersembahkan untuk :

1. Allah SWT, atas berkat Rahmat dan Hidayah-Nya yang luar biasa sehingga skripsi ini dapat terselesaikan.
2. Papah dan Mamah tercinta yang senantiasa mendoakan, memotivasi serta memberikan semangat yang tiada henti.
3. Adik – adikku tercinta, Lia, Mitha, dan Wulan yang senantiasa mendoakan dan memberikan semangat selama ini.
4. Keluarga besar yang senantiasa mendoakan dan memberikan semangat.
5. Mas Joy yang telah banyak memberikan motivasi, inspirasi, dan ilmu yang bermanfaat.
6. Teman – teman kontrak yang telah memberikan banyak bantuan selama ini.
7. Teman – teman SMA Negeri 9 Yogyakarta angkatan 08.
8. Teman – teman PD FEB UGM angkatan 2008.
9. Kampus STMIK AMIKOM Yogyakarta tercinta yang telah memberikan kesempatan untuk menimba ilmu.

KATA PENGANTAR

Puji dan syukur penulis persembahkan untuk Allah SWT yang telah memberikan Rahmat dan Hidayah-Nya yang luar biasa sehingga penulis dapat menyelesaikan skripsi yang berjudul “ANALISIS DAN PERANCANGAN APLIKASI ENKRIPSI SMS DENGAN KOMBINASI METODE SUBSTITUSI DAN AES BERBASIS ANDROID DI KALANGAN MAHASISWA STMIK “AMIKOM” YOGYAKARTA”. Tidak lupa shalawat dan salam penulis haturkan kepada Nabi Muhammad SAW yang telah menyebarkan agama Islam dan membebaskan umat manusia dari belenggu kebodohan.

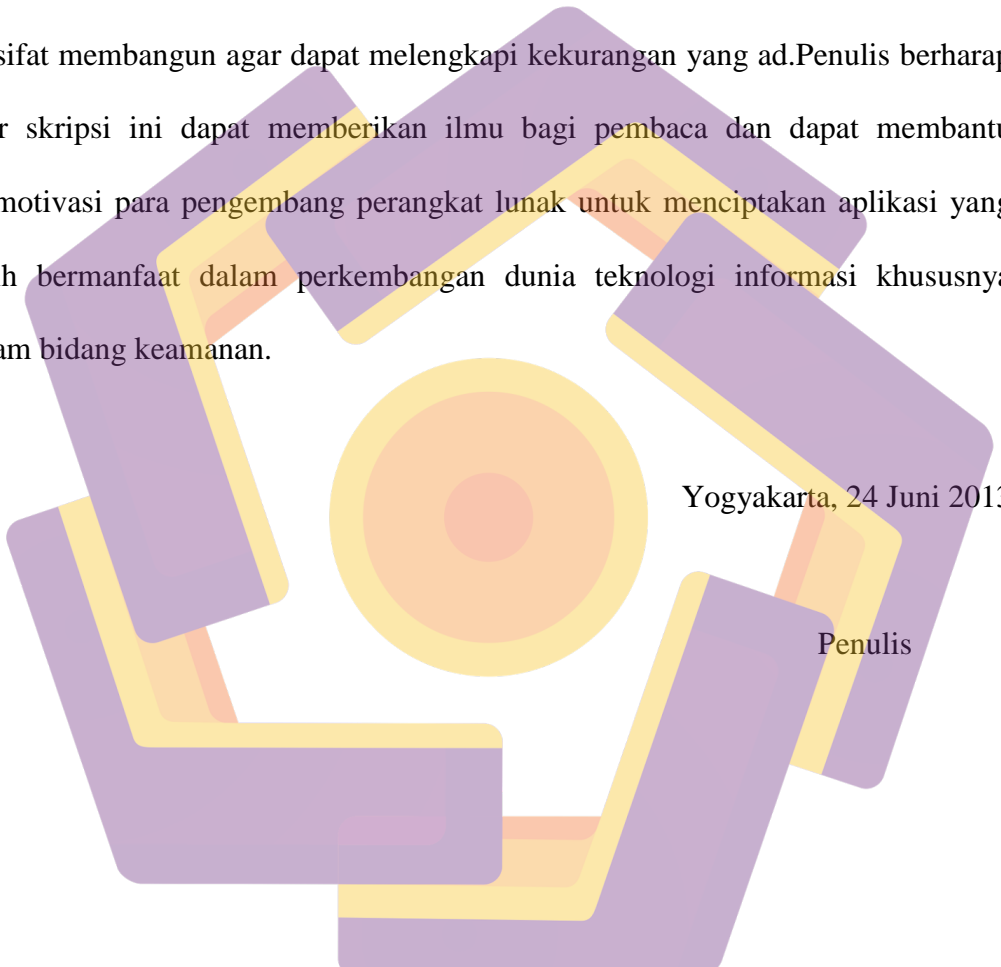
Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK AMIKOM Yogyakarta. Selain itu skripsi juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komputer.

Pada kesempatan ini, penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT selaku Ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, Dr., S.Si, M.Kom selaku dosen pembimbing yang telah memberikan bimbingan serta saran yang sangat membangun dalam proses pengerjaan skripsi.
4. Kedua Orang Tua penulis.

5. Seluruh pihak yang berperan serta dalam proses pengerjaan skripsi baik secara moril maupun materiil.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan, oleh karena itu penulis sangat mengharapkan saran dan kritik yang bersifat membangun agar dapat melengkapi kekurangan yang ada. Penulis berharap agar skripsi ini dapat memberikan ilmu bagi pembaca dan dapat membantu memotivasi para pengembang perangkat lunak untuk menciptakan aplikasi yang lebih bermanfaat dalam perkembangan dunia teknologi informasi khususnya dalam bidang keamanan.



Yogyakarta, 24 Juni 2013

Penulis

DAFTAR ISI

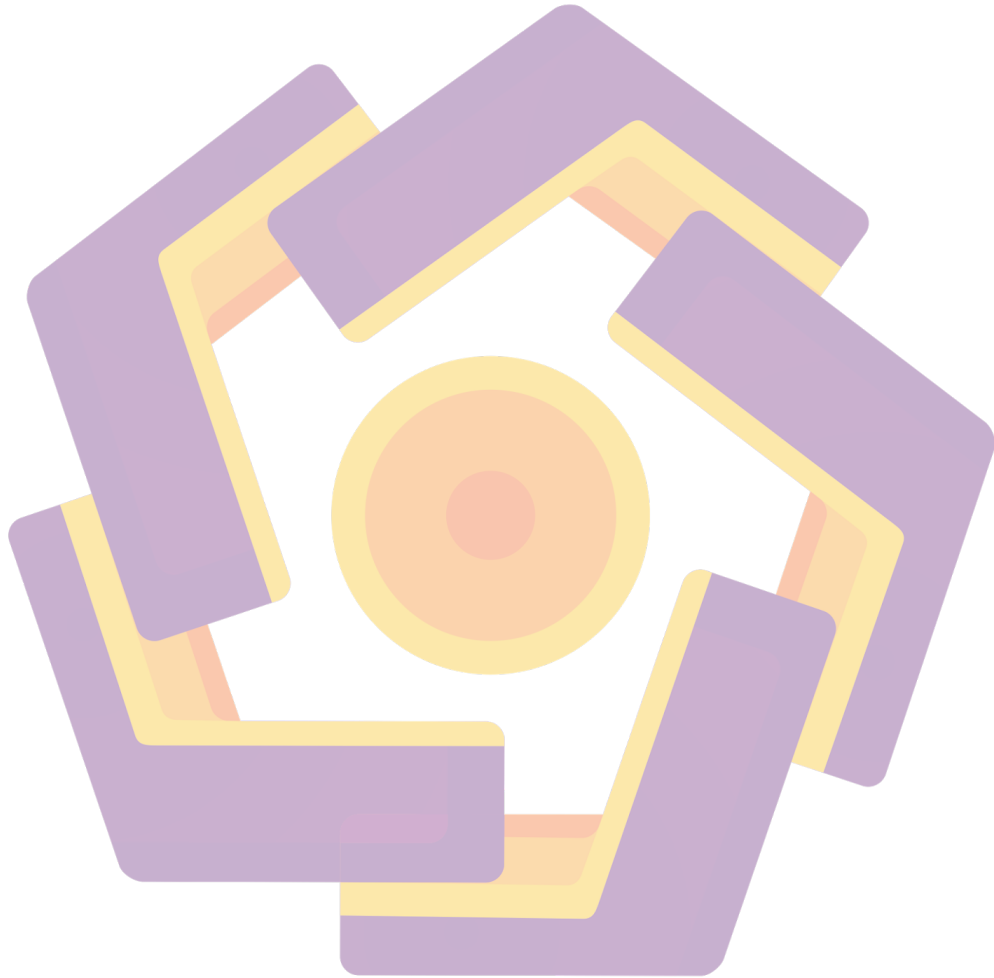
HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN.....	iv
HALAMAN MOTTO.....	v
HALAMAN PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
INTISARI.....	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Metode Penelitian.....	4
1.7 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI.....	7
2.1 Short Message Service (SMS).....	7
2.1.1 Pengertian Short Message Service (SMS).....	7
2.1.2 Arsitektur Short Message Service (SMS).....	8
2.2 Eclipse Intergrated Development Environment (Eclipse IDE).....	11
2.3 Android.....	12
2.3.1 Sejarah Android.....	12
2.3.2 Dalvik Virtual Machine (DVM).....	12

2.3.3	Android SDK (Software Development Kit)	13
2.3.4	Arsitektur Android.....	14
2.3.5	Fundamental Aplikasi.....	17
2.4	SQLite	19
2.5	Kriptografi.....	20
2.5.1	Sejarah Kriptografi	20
2.5.2	Komponen Kriptografi.....	20
2.5.3	Kode Geser	21
2.5.4	Kode Vigènere	22
2.5.5	Advanced Encryption Standard (AES).....	23
2.6	Data Flow Diagram (DFD)	24
2.6.1	Pengertian DFD	24
2.6.2	Elemen DFD.....	24
BAB III ANALISIS DAN PERANCANGAN SISTEM.....		26
3.1	Analisis Kebutuhan	26
3.2	Software Requirement Spesifitcation (SRS).....	28
3.3	Rancangan Digram Hierarki.....	29
3.4	Rancangan Flowchart.....	29
3.5	Rancangan Sistem	30
3.5.1	Arsitektur Sistem.....	30
3.5.1.1	Arsitektur Aliran Pesan Secara Umum (GSM)	30
3.5.1.2	Arsitektur Sistem Aplikasi.....	32
3.5.2	Perancangan Pemodelan Funsional.....	32
3.5.2.1	Context Diagram.....	32
3.5.2.2	Data Flow Diagram (DFD).....	33
3.5.3	Perancangan Sistem.....	36
3.6	Perancangan User Interface.....	37
3.6.1	Rancangan Splash Screen	37
3.6.2	Rancangan Form Tab Tulis Pesan	38
3.6.3	Rancangan Form Tab Kotak Masuk Pesan.....	38
3.6.4	Rancangan Form Tab Kotak Keluar Pesan.....	39

3.6.5 Rancangan Form Bantuan.....	39
BAB IV IMPLEMENTASI DAN PEMBAHASAN	40
4.1 Implementasi	40
4.1.1 Splash Screen.....	41
4.1.2 Form Tulis Pesan	41
4.1.3 Form Kotak Masuk Pesan.....	42
4.1.4 Form Kotak Keluar Pesan.....	43
4.1.5 Form Bantuan	44
4.2 Pengujian	45
4.2.1 Lingkungan Pengujian.....	45
4.2.1.1 Perangkat Lunak.....	45
4.2.1.2 Perangkat Keras.....	46
4.2.2 Material Pengujian	46
4.2.3 Pelaksanaan Pengujian	47
4.3 Analisis Hasil	55
4.4 Koversi File .apk	59
BAB V PENUTUP.....	64
5.1 Kesimpulan.....	64
5.2 Saran.....	65
DAFTAR PUSTAKA	66

DAFTAR TABEL

Tabel 3.1 Spesifikasi Kebutuhan Perangkat Lunak	28
Tabel 4.1 Hasil Pengujian	94



DAFTAR GAMBAR

Gambar 2.1 Struktur SMS.....	7
Gambar 2.2 Arsitektur SMS.....	8
Gambar 2.3 Arsitektur Android	17
Gambar 2.4 Tabula Recta.....	22
Gambar 2.5 Proses Umum Enkripsi dan Dekripsi AES.....	23
Gambar 2.6 Simbol Proses.....	24
Gambar 2.7 Simbol Data Flow	25
Gambar 2.8 Simbol Data Store	25
Gambar 2.9 Simbol External Entity	25
Gambar 3.1 Diagram Hierarki.....	29
Gambar 3.2 Flowchart Sistem.....	30
Gambar 3.3 Susunan Jaringan dan Aliran SMS.....	31
Gambar 3.4 Arsitektur Sistem Aplikasi	32
Gambar 3.5 Context Diagram	33
Gambar 3.6 DFD Level 1.....	34
Gambar 3.7 Rancangan Splash Screen.....	37
Gambar 3.8 Rancangan Form Tab Tulis Pesan.....	38
Gambar 3.9 Rancangan Form Tab Kotak Masuk Pesan	38
Gambar 3.10 Rancangan Form Tab Kotak Keluar Pesan	39
Gambar 3.11 Rancangan Form Tab Bantuan.....	39
Gambar 4.1 Form Splash Screen.....	41
Gambar 4.2 Form Tulis Pesan.....	42
Gambar 4.3 Form Kotak Masuk Pesan	43
Gambar 4.4 Form Kotak Keluar Pesan	44
Gambar 4.5 Form Bantuan.....	45
Gambar 4.6 Peringatan Nomor Tujuan Belum Diisi.....	48
Gambar 4.7 Peringatan Pesan Belum Diisi	49
Gambar 4.8 Peringatan Kunci Belum Diisi.....	49

Gambar 4.9 Penerimaan Pesan.....	50
Gambar 4.10 Fungsi Longpress	50
Gambar 4.11 Laporan Pesan Terkirim	51
Gambar 4.12 Laporan Pesan Terdekripsi.....	52
Gambar 4.13 Laporan Pesan Gagal Terdekripsi	52
Gambar 4.14 Menu Bantuan	53
Gambar 4.15 Menu Help.....	53
Gambar 4.16 Menu About	54
Gambar 4.17 Header Inbox	54
Gambar 4.18 Header Outbox	55
Gambar 4.19 Open Project.....	60
Gambar 4.20 Export .apk	61
Gambar 4.21 Pengecekan Project	61
Gambar 4.22 Pembuatan Keystore.....	62
Gambar 4.23 Pengisian Data Keystore	62
Gambar 4.24 Pengisian Nama File & Direktori.....	63

INTISARI

Beberapa tahun terakhir terjadi perkembangan yang pesat pada bidang teknologi, salah satunya adalah perkembangan teknologi telekomunikasi yang telah membantu mengurangi kendala kita dalam berkomunikasi yang dibatasi oleh jarak dan waktu. Perkembangan tersebut dapat kita cermati seiring dengan perkembangan berbagai macam ponsel pintar dengan fitur – fitur yang canggih. Salah satu fitur yang disediakan adalah *Short Message Service* (SMS). Fitur ini sangat *familiar* dikalangan pengguna ponsel pintar, dengan menggunakan SMS, pengguna dapat berkomunikasi melalui pesan teks.

Pada tugas akhir ini dibangun suatu perangkat lunak pada ponsel pintar yang digunakan untuk meningkatkan keamanan pesan yang akan dilakukan melalui SMS. Perangkat lunak yang ditujukan untuk meningkatkan keamanan isi pesan tersebut dengan cara melakukan enkripsi terhadap pesan yang dikirim dan melakukan dekripsi terhadap pesan yang diterima. Aplikasi ini dapat digunakan untuk mengirimkan suatu informasi yang bersifat rahasia dengan aman kepada orang lain melalui SMS.

Perangkat lunak yang dibangun menggunakan gabungan dari beberapa algoritma kriptografi klasik dan algoritma kriptografi modern untuk melakukan enkripsi SMS. Tujuan dari penggunaan beberapa metode adalah untuk mendapatkan suatu algoritma yang andal dan diimplementasikan menggunakan teknologi Android.

Kata kunci : SMS, enkripsi, dekripsi, teknik substitusi, AES, android.

ABSTRACT

Last few years occurred rapid development in technology, one of which is the development of telecommunications technology that has helped us reducing the obstacles in communication limited by distance and time. These developments can we look along in wide range of smart phone developments with sophisticated features. One of the provided features is Short Message Service (SMS). This feature is veru familiar among users of smart phones, using SMS, users can communicate via text messages.

In this final project, a software built on the smart phone that are used to enhance the security of the message that will be done through SMS. The software intended to enhance the security of message contents by encrypting sent messages and decrypt received messages. This application can be used to transmit a confidential information securely to others through SMS.

This software was built by using a combination of classical cryptographic algorithms and modern cryptographic algorithms to encrypt SMS. The purpose of using this multiple methods is to obtain an reliably algorithm and can be implemented using Android technology.

Keywords : *SMS, encryption, decryption, substitution technique, AES, android.*