

**RANCANG BANGUN APLIKASI KONVERSI SMS KE DALAM BAHASA
KHEK DAN ENKRIPSI MENGGUNAKAN ALGORITMA AES
BERBASIS ANDROID**

SKRIPSI



Edi Sugianto
1311500005

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG
2017**

**RANCANG BANGUN APLIKASI KONVERSI SMS KE DALAM BAHASA
KHEK DAN ENKRIPSI MENGGUNAKAN ALGORITMA AES
BERBASIS ANDROID**

SKRIPSI

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



Oleh :

Edi Sugianto

1311500005

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG
2017**

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

NIM : 1311500005

Nama : Edi Sugianto

Judul Skripsi : RANCANG BANGUN APLIKASI KONVERSI SMS
KE DALAM BAHASA KHEK DAN ENKRIPSI
MENGUNAKAN ALGORITMA AES BERBASIS
ANDROID

Menyatakan bahwa Laporan Tugas Akhir saya adalah **HASIL KARYA SENDIRI, TIDAK MEMBELI, TIDAK MEMBAYAR PIHAK LAIN UNTUK MEMBUATKAN, DAN BUKAN PLAGIAT**, Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, Juli 2017



Edi Sugianto

LEMBAR PENGESAHAN SKRIPSI

**RANCANG BANGUN APLIKASI KONVERSI SMS KE DALAM BAHASA
KHEK DAN ENKRIPSI MENGGUNAKAN ALGORITMA AES
BERBASIS ANDROID**

Yang dipersiapkan dan disusun oleh

Edi Sugianto

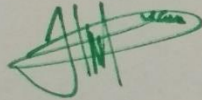
1311500005

Telah dipertahankan di depan Dewan Penguji

Pada Tanggal 07 Agustus 2017

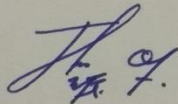
Susunan Dewan Penguji

Ketua



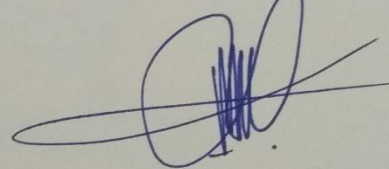
**Yohanes Setiawan, M.Kom.
NIDN 0219068501**

Anggota



**Hengki, M.Kom.
NIDN 0207049001**

Dosen Pembimbing



**Chandra Kirana, M.Kom
NIDN 0228108501**

Kaprodi Teknik Informatika



**R. Bambang Isnanto, F.Si, M.kom
NIDN 0224048003**

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 07 Agustus 2017

KETUA STMIK ATMA LUHUR PANGKALPINANG

Prof. Dr. Moedjiono, M.Sc

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk memperoleh gelar sarjana pada program studi Teknik Informatika pada STMIK ATMA LUHUR.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
4. Bapak Drs. Harry Sudjikianto, MM, MBA selaku Ketua Yayasan Atma Luhur.
5. Bapak Dr. Moedjiono, M.Sc selaku Ketua STMIK Atma Luhur.
6. Kakak yang telah memberikan bantuan baik spirit maupun materi.
7. Bapak R.Burham Isnanto Farid, S.Si., M. Kom Selaku Kaprodi Teknik Informatika.
8. Susan Suprawiro yang sebentar lagi S.Kom selalu memberikan spirit untuk saya terus menyelesaikan skripsi ini.
9. Bapak Chandra Kirana, M.Kom selaku dosen pembimbing dalam penyusunan skripsi ini, yang telah memberikan masukan yang sangat berarti dan membimbing penulis sehingga skripsi ini dapat terselesaikan.
10. Teman-teman senasib dan seperjuangan yang telah membagi ilmu serta memberi warna dalam persahabatan dan kebersamaan yang telah terjalin selama kuliah di STMIK Atma Luhur Pangkalpinang.
11. Saudara dan sahabat-sahabatku terutama Kawan-kawan Angkatan 2013 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

Semoga semua jasa yang telah diberikan mendapat balasan dari Tuhan Yang Maha Esa. Akhir kata penulis berharap semoga laporan skripsi ini berguna bagi para pembaca umumnya dan teman-teman mahasiswa STMIK Atma Luhur Pangkalpinang khususnya.

Pangkalpinang, Juli 2017

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke at the end.

Penulis

ABSTRACT

The mobile phone known as HP (hand phone) has many excellence and excess both in terms of facilities it is, one of the facilities that are widely used SMS. Besides the existing facilities SMS has a snippet of intercepts, therefore it is an application that uses the AES algorithm and khek language conversion. The Advanced Encryption Standard Algorithm (AES) is a modern cryptographic algorithm that assumes symmetry. In the key AES algorithm used has a variable length of 128,192,256 with a different number of rounds depending on the length of the key. Khek is a language spoken by Hakka people, has 9 dialect types, one of which is dialect of lufang. By applying the AES algorithm and the khek language conversion to the encryption application, securing the messages sent will be assured of its secrecy, so that the unauthorized parties, can not get free message information.

Keywords :AES Algorithm, SMS, Cryptography, Khek Language, Mobile Phone

ABSTRAK

Telepon Selular (ponsel) atau dikenal dengan nama HP (*handphone*) memiliki banyak keunggulan dan kelebihan baik dari segi fasilitas yang dimilikinya, salah satu fasilitas yang banyak digunakan berupa SMS. Akan tetapi fasilitas yang berupa SMS ini memiliki kerentanan berupa penyadapan, maka dari itu diusulkan sebuah aplikasi enkripsi menggunakan algoritma AES dan konversi bahasa khek. Algoritma *Advanced Encryption Standard* (AES) merupakan algoritma kriptografi modern yang bersifat simetris. Pada algoritma AES kunci yang dipakai memiliki panjang bervariasi yaitu 128,192,256 dengan memiliki jumlah ronde yang berbeda pula tergantung panjang kunci-nya. Bahasa Khek adalah bahasa yang dituturkan oleh orang Hakka, memiliki 9 jenis dialek, salah yang digunakan adalah dialek lufang. Dengan menerapkan algoritma AES dan konversi bahasa khek pada aplikasi enkripsi, pengamanan pesan yang dikirim akan terjamin kerahasiaannya, sehingga pihak yang tidak berwenang, tidak dapat mendapatkan informasi pesan yang dikirimkan.

Kata kunci : Algoritma AES, SMS , Kriptografi, Bahasa khek, *Handphone*

DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	i
LEMBAR PERSETUJUAN SIDANG	ii
LEMBAR PENGESAHAN SKRIPSI	iii
KATA PENGANTAR.....	iv
ABSTRACT	vi
ABSTRAK	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiv
DAFTAR SIMBOL	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah.....	3
1.4 Metodologi Penelitian	3
1.5 Tujuan dan Manfaat	4
1.5.1 Tujuan Penelitian	4
1.5.2 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
BAB II LANDASAN TEORI	6
2.1 Aplikasi <i>Mobile</i>	6
2.2 <i>Android</i>	7
2.2.1 Arsitektur <i>Android</i>	8
2.2.2 Aplikasi <i>Android</i>	10
2.2.3 Kelebihan dan Kekurangan <i>Android</i>	12
2.3 <i>Java</i>	13

2.4 <i>Eclipse</i> IDE.....	14
2.4.1 Arsitektur <i>Eclipse</i>	14
2.4.2 <i>Android</i> SDK.....	15
2.4.3 ADT <i>Plugin for Eclipse</i>	16
2.4.4 <i>Java Development Kit</i> (JDK)	17
2.5 Model Perangkat Lunak	17
2.6 UML (<i>Unified Modelling Language</i>).....	18
2.6.1 Diagram UML.....	19
2.7 <i>Black Box Testing</i>	21
2.8 <i>Redkoda</i>	22
2.9 Kriptografi	22
2.9.1 Tujuan Kriptografi	23
2.9.2 Jenis – Jenis Kriptografi.....	23
2.9.3 Enkripsi Simetris.....	23
2.9.4 Kunci Enkripsi dan Fungsi Hash	26
2.9.5 Daftar Istilah System Security	26
2.9.6 Perbandingan Algoritma Enkripsi Simetris.....	27
2.10 Kode ASCII.....	27
2.11 Algoritma Rijndael / <i>Advanced Encryption System</i>	29
2.12 Bahasa Hakka /Khek	32
2.12.1 Sejarah.....	32
2.12.2 Penutur Bahasa Hakka Di Indonesia.....	33
2.12.3 Dialek Hakka.....	33
2.13 Penelitian Terdahulu	34
BAB III METODOLOGI PENELITIAN	40
3.1 Model Pengembangan Sistem	40
3.2 Metode Pengembangan Sistem	41
3.3 Tools Pengembangan Sistem	42
3.4 AES	42

BAB IV HASIL DAN PEMBAHASAN	43
4.1 Analisis.....	43
4.1.1 Analisis Sistem Berjalan	43
4.1.2 Analisis Sistem Usulan	44
4.1.3 Analisis Kebutuhan	45
4.1.4 Analisis Proses	48
4.2 Perancangan	56
4.2.1 Perancangan Aplikasi.....	56
4.2.2 Algoritma Pada Sistem.....	69
4.2.3 Perancangan <i>Interface</i> Aplikasi	70
4.2.4 <i>Sequence</i> Diagram Aplikasi Enkripsi.....	74
4.3 Implementasi	78
4.4 Pengujian.....	86
BAB V PENUTUP	89
5.1 Kesimpulan	89
5.2 Saran.....	89
DAFTAR PUSTAKA	86
LAMPIRAN.....	89

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Arsitektur <i>Android</i>	28
Gambar 2.2 Tahap <i>Model Waterfall</i>	37
Gambar 2.3 Contoh Diagram <i>Use Case</i>	40
Gambar 2.4 Contoh Diagram <i>Activity Diagram</i>	41
Gambar 2.5 Skema dari <i>Symmetric Chiphers Models</i>	44
Gambar 2.6 Perbandingan Algoritma Simetris ^[22]	47
Gambar 2.7 Karakter Kontrol ASCII 0 – 127	48
Gambar 2.8 Karakter Kontrol ASCII 128 – 255	49
Gambar 2.9 Proses Enkripsi dan Dekripsi AES	51
Gambar 4.1 <i>Activity Diagram</i> Penyampaian Informasi	64
Gambar 4.2 <i>Activity Diagram</i> Sistem Usulan Penyampain Informasi	65
Gambar 4.3 Proses Enkripsi AES	69
Gambar 4.4 Operasi Xor St1 dan St2	69
Gambar 4.5 <i>S-box</i>	70
Gambar 4.6 <i>Shiftrows</i>	70
Gambar 4.7 Hasil <i>Shiftrows</i>	70
Gambar 4.8 <i>Mixcolumn()</i>	71
Gambar 4.9 Dekripsi AES	73
Gambar 4.10 <i>Invers Shift Rows</i>	73
Gambar 4.11 <i>S-box</i> ⁻¹	74
Gambar 4.12 Operasi <i>Add Round Key</i>	74
Gambar 4.13 <i>Use Case Diagram</i> Aplikasi Pengaman SMS	77
Gambar 4.14 <i>Activity Diagram</i> Membuat Pesan	83
Gambar 4.15 <i>Activity Diagram</i> Terjemah Pesan Masuk	83
Gambar 4.16 <i>Activity Diagram</i> Terjemah Pesan Keluar	84
Gambar 4.17 <i>Activity Diagram</i> Teruskan Pesan Keluar	84

Gambar 4.18 <i>Activity Diagram</i> Teruskan Pesan Keluar.....	85
Gambar 4.19 <i>Activity Diagram</i> Hapus Pesan Masuk	85
Gambar 4.20 <i>Activity Diagram</i> Hapus Pesan Keluar	86
Gambar 4.21 <i>Activity Diagram</i> Bantuan	86
Gambar 4.22 <i>Activity Diagram</i> Tentang.....	87
Gambar 4.23 Diagram Keluar	87
Gambar 4.24 <i>Class Diagram</i>	88
Gambar 4.25 Rancangan Layar Utama	90
Gambar 4.26 Rancangan Layar List Pesan	91
Gambar 4.27 Rancangan Layar Pesan	91
Gambar 4.28 Rancangan Layar Buat Pesan	92
Gambar 4.29 Rancangan Layar Terjemahan.....	92
Gambar 4.30 Rancangan Layar Bantuan	93
Gambar 4.31 Rancangan Layar Tentang.....	93
Gambar 4.32 <i>Sequence Diagram</i> Buat Pesan.....	94
Gambar 4.33 <i>Sequence Diagram</i> Pesan Masuk.....	95
Gambar 4.34 <i>Sequence Diagram</i> Pesan Keluar.....	96
Gambar 4.35 <i>Sequence Diagram</i> Bantuan	97
Gambar 4.36 <i>Sequence Diagram</i> Tentang.....	97
Gambar 4.37 <i>Sequence Diagram</i> Keluar	98
Gambar 4.38 Penginstalan Aplikasi	99
Gambar 4.39 Penginstalan Aplikasi.....	99
Gambar 4.40 Penginstalan Aplikasi.....	100
Gambar 4.41 Penginstalan Aplikasi.....	100
Gambar 4.42 Tampilan Layar Utama.....	101
Gambar 4.43 Tampilan List Pesan	101
Gambar 4.44 Tampilan Layar Pesan	102
Gambar 4.45 Tampilan Layar Buat Pesan	102

Gambar 4.46 Tampilan Layar Terjemah Pesan.....	103
Gambar 4.47 Tampilan Layar Bantuan	103
Gambar 4.48 Tampilan Layar Tentang	104
Gambar 4.49 Tampilan Enkripsi Pesan.....	105
Gambar 4.50 Tampilan Dekripsi Pesan	106

DAFTAR TABEL

	Halaman
Tabel 2.1 Istilah <i>System Security</i>	46
Tabel 2.2 Penelitian Terdahulu	57
Tabel 4.1 Kamus bahasa Indonesia dan khek	68
Tabel 4.2 Spesifikasi Basis Data Admin.....	88
Tabel 4.3 <i>Blackbox Testing</i>	106

DAFTAR SIMBOL

1. Simbol *Activity Diagram*



Start Point (Initial Node)

Merupakan simbol untuk memulai *activity diagram*.



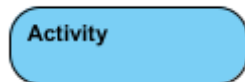
End Point (Activity Final Node)

Merupakan simbol untuk mengakhiri *activity diagram*



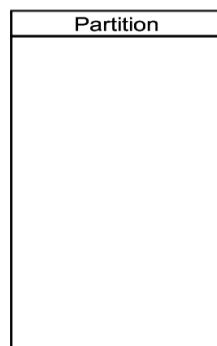
Transition

Menggambarkan aliran perpindahan kontrol antara *activity*.



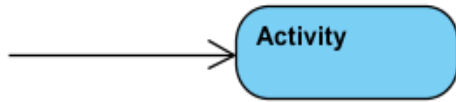
Activity (Aktivitas)

Menggambarkan proses bisnis dan dikenal sebagai *activity state*. *Activity* juga merupakan proses komputasi atau perubahan kondisi yang bisa berupa kata kerja atau ekspresi.



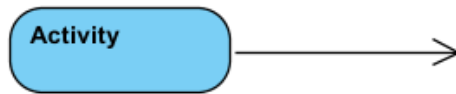
Swimlane

Menggambarkan pemisahan atau pengelompokan aktivitas berdasarkan *actor*.



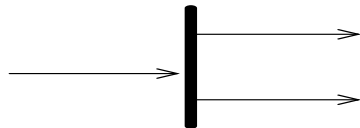
Black Hole Activities

Adanya masukan dan tidak ada keluaran, biasanya digunakan jika dikehendaki ada 1 atau lebih transisi.



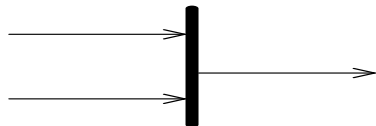
Miracle Activities

Tidak ada masukan dan ada keluaran, biasanya dipakai pada waktu *start point* dan dikehendaki ada 1 atau lebih transisi.



Fork (Percabangan)

Mempunyai 1 transisi masuk dan 2 atau lebih transisi keluar.



Join (Penggabungan)

Mempunyai 2 atau lebih transisi masuk dan hanya 1 transisi keluar.



Decision

Merupakan cara untuk menggabungkan ketika ada lebih dari 1 transisi yang masuk atau pilihan untuk mengambil keputusan.

2. Simbol Use Case Diagram



Use case

Gambaran fungsionalitas dari suatu sistem, sehingga pengguna sistem paham dan mengerti mengenai kegunaan sistem yang akan dibangun.



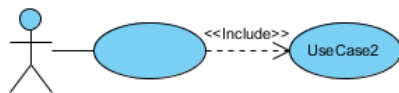
Actor

Sebuah entitas manusia atau mesin yang berinteraksi dengan sistem untuk melakukan pekerjaan-pekerjaan tertentu.



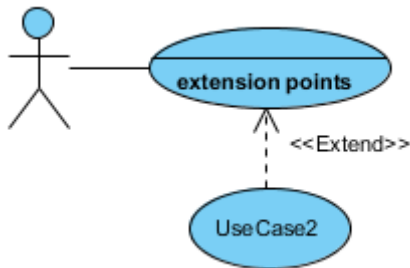
Association

Merupakan abstraksi berupa garis tanpa panah yang menghubungkan antara aktor dan *use case*.



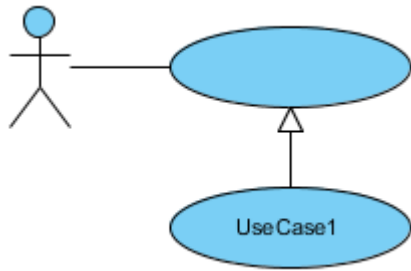
Include

Menunjukkan bahwa suatu *use case* seluruhnya merupakan fungsionalitas dari *use case* lainnya.



Extend

Menunjukkan suatu *use case* merupakan tambahan fungsional dari *use case* lainnya jika suatu kondisi terpenuhi.

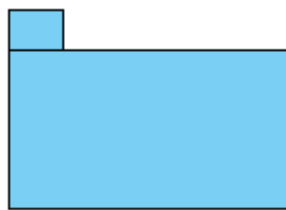


Generalization

Disebut juga *inheritance* (pewarisan), sebuah elemen dapat merupakan spesialisasi dari elemen lainnya.

Packages

Digambarkan sebagai sebuah direktori yang berisikan model-model elemen. *Packages* digunakan untuk mengorganisasikan sebuah diagram yang besar menjadi beberapa diagram kecil.



3. Simbol Entity Relationship Diagram (ERD)

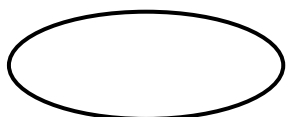
Entity

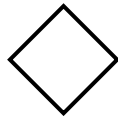
Dapat berupa orang, tempat, objek, atau kejadian yang dianggap penting bagi perusahaan atau instansi, sehingga segala atributnya harus dicatat dan disimpan dalam basis data.



Attribute

Elemen data yang dimiliki sebuah entitas. Atribut berfungsi mendeskripsikan karakteristik entitas (atribut yang berfungsi sebagai *key* diberi garis bawah).





Relasi

Menggambarkan hubungan yang ada diantara himpunan entitas

4. Simbol *Sequence Diagram*



Actor

Menggambarkan seseorang atau sesuatu (seperti perangkat, sistem lain) yang berinteraksi dengan sistem.



Boundary

Menggambarkan interaksi antara satu atau lebih *actor* dengan sistem, memodelkan bagian dari sistem yang bergantung pada pihak lain disekitarnya dan merupakan pembatas sistem dengan dunia luar.



Control

Menggambarkan “perilaku untuk mengatur atau kegiatan mengontrol”, mengkoordinasikan perilaku sistem dan dinamika dari suatu sistem, menangani tugas utama dan mengontrol alur kerja suatu sistem.



Entity

Menggambarkan informasi yang harus disimpan oleh sistem (struktur data dari sebuah sistem).



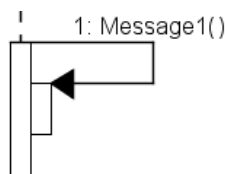
Object

Menggambarkan abstraksi dari sebuah entitas nyata/tidak nyata yang informasinya harus disimpan.



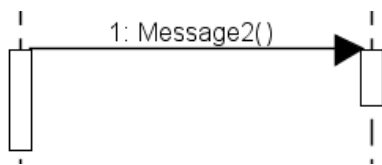
Activation

Menunjukkan periode selama suatu *object* atau *actor* sedang melakukan suatu tindakan.



Message

Pesan yang dikirim untuk dirinya sendiri.



Object Message

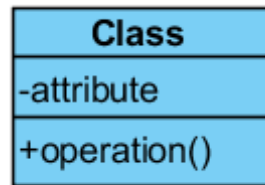
Menggambarkan pesan/hubungan antar objek yang menunjukkan urutan kejadian yang terjadi.



Looping logic

Menggambarkan dengan sebuah *frame* dengan label *loop* dan sebuah kalimat yang mengindikasikan pengulangan dan *interaction operator loop*.

5. Simbol *Class Diagram*



Class

Himpunan objek-objek dengan *attribute* dan *operation* yang sama dan saling keterkaitan.

Association

Menggambarkan hubungan antara *class* dengan *class* lainnya.