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 MENGGUNAKAN 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. Burham Isnanto F.,S.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

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 Algortima (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 Langguage, 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. Algortima *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 kerahasiaan nya, sehingga pihak yang tidak berwenang, tidak dapat mendapatkan informasi pesan yang dikirimkan.

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Halaman

DAFTAR SIMBOL

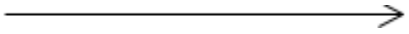
1. Simbol *Acivity Diagram*

Start Point (Initial Node)

Merupakan simbol untuk memulai *activity diagram.*

End Point (Activity Final Node)

*M*erupakan simbol untuk mengakhiri *activity diagram*

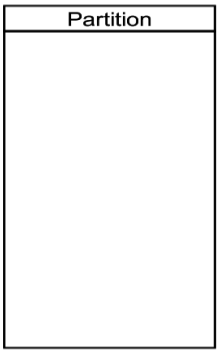


Transition

Menggambarkan aliran perpindahan kontrol antara *activity*.

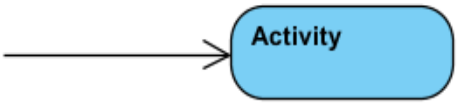
***Activity* (Aktivitas)**

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



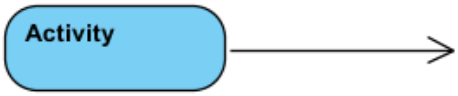
Swimline

Menggambarkan pemisahan atau pengelompokan aktivitas berdasarkan *actor*.



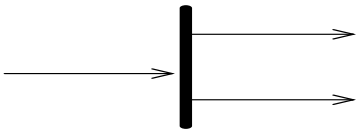
Black Hole Activities

*A*danya masukan dan tidak ada keluaran, biasanya digunakan jika dikehendaki ada 1 atau lebih transisi.



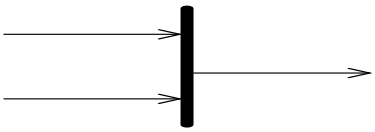
Miracle Activities

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.

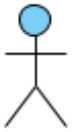
Decision

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.

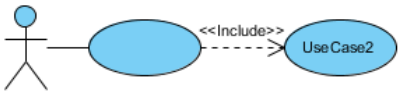


Actor

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

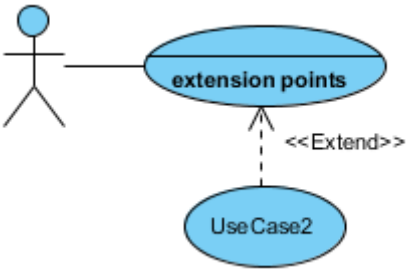
Association

Merupakan abtraksi berupa garis tanpa panah yang menghubung antara aktor dan *use case*.



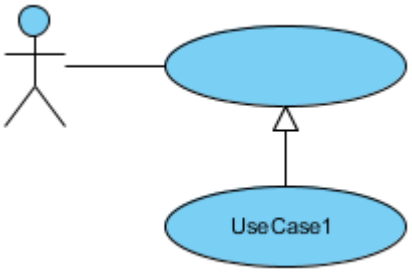
Include

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



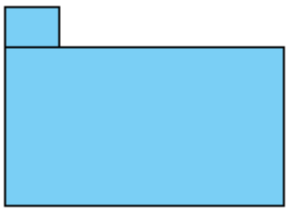
Extend

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.



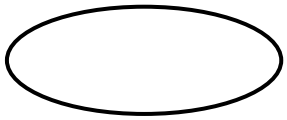
Packages

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)*

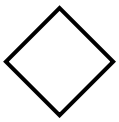
Entity

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

Mengambarkan 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

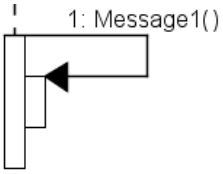
Menggambarkan informasi yang harus disimpan oleh sistem (struktur data dari sebuah sistem).

Object

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

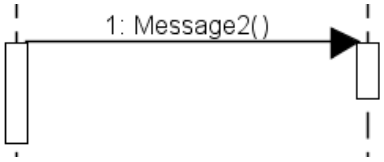
Activation

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



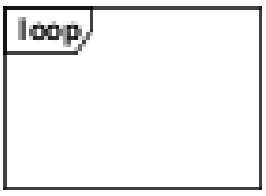
Message

Pesan yang dikirim untuk dirinya sendiri.



Object Message

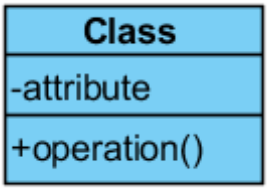
Menggambarkan pesan/hubungan antar objek yang menunjukkan urutan kejadian yang terjadi.



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.