PEMANFAATAN ALGORITMA *BLOK CHIPER* DES (*DATA ENCRYPTION STANDARD*) UNTUK MENGENKRIPSI SMS (*SHORT MESSAGE SERVICES*) PADA PLATFORM ANDROID

SKRIPSI

CALVIN ADIANTO TAJIB

1411500029

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

ATMALUHUR

PANGKALPINANG

2017/2018

PEMANFAATAN ALGORITMA *BLOK CHIPER* DES (*DATA ENCRYPTION STANDARD*) UNTUK MENGENKRIPSI SMS (*SHORT MESSAGE SERVICES*) PADA PLATFORM ANDROID

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

CALVIN ADIANTO TAJIB
1411500029

PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMALUHUR
PANGKALPINANG
2017/2018

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

NIM	:	1411500029
Nama	:	CALVIN ADIANTO TAJIB
Judul Skripsi	:	PEMANFAATAN ALGORITMA *BLOK CHIPER DES* (*DATA ENCRYPTION STANDARD*) UNTUK MENGENKRIPSI SMS (*SHORT MESSAGE SERVICES*) PADA PLATFORM 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 diatas, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 23 Juli 2018

(Calvin Adianto Tajib)

LEMBAR PENGESAHAN SKRIPSI

PEMANFAATAN ALGORITMA *BLOK CHIPER* DES (*DATA ENCRYPTION STANDARD*) UNTUK MENGENKRIPSI SMS (*SHORT MESSAGE SERVICES*) PADA PLATFORM ANDROID

Yang dipersiapkan dan disusun oleh

Calvin Adianto Tajib
1411500029

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 01 Agustus 2018

Susunan Dewan Penguji
Anggota

Dwi Yuny Sylfania, M.Kom
NIDN. 0207069301

Dosen Pembimbing

Ari Amir Alkodri, M.Kom
NIDN. 0201038601

Kaprodi Teknik Informatika

R. Burham Isnanto F., S.Si, M.Kom
NIDN. 0224048003

Ketua

Rendy Rian Chrisna Putra, M.Kom
NIDN. 0221069201

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Agustus 2018

KETUA STMIK ATMA LUHUR PANGKALPINANG

Dr. Husni Teja Sukmana, S.T., M.Sc
NIP:197710302001121003

KATA PENGANTAR

Puji syukur atas Kehadirat Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (TI) pada Jurusan Teknik Informatika 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. Tuhan Yang Maha Esa yang telah menciptakan dan memberikan kehidupan di dunia
2. Bapak dan Ibu tercinta yang telah mendukung penulisan ini.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
4. Bapak Dr. Husni Teja Sukmana, S.T., M.Sc., selaku Ketua STMIK Atma Luhur.
5. Bapak R. Burham Isnanto F., S.Si, M.Kom Selaku Kaprodi Teknik Informatika.
6. Bapak Ari Amir Alkodri, M. Kom selaku dosen pembimbing.
7. Saudara dan teman-teman angkatan 2014 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

Semoga Tuhan membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Pangkalpinang, Agustus 2018

Penulis

ABSTRACT

Short Message Service (SMS) is a very popular communication technology revolution. By using SMS one can exchange messages with others. However, with the problem of SMS wiretapping, a person no longer has the right to privacy. So in this study, the authors develop an application on the Android-based mobile phone that will change the SMS message into codes so that the information content of the SMS is not known to others. Be aware of this issue required the security of the contents of the message to maintain the confidentiality of the message content. Safeguarding the contents of SMS messages through mobile applications by means of encryption (encryption) with DES (Data Encryption Standard) algorithm. With the application of encryption and decryption of this message is expected to maximize the security of the contents of the message against threats to read the contents of messages by people who do not want or have no right in reading the contents of the message. In this research use waterfall research model and Blackbox testing.

Keywords: Short Message Service Center, SMS, Short Message Service, Cryptography, DES, Data Encryption Standard

ABSTRAKSI

Short Message Service (SMS) merupakan sebuah revolusi teknologi komunikasi yang sangat popular. Dengan menggunakan SMS seseorang dapat saling bertukar pesan dengan orang lain. Namun, dengan adanya masalah penyadapan SMS, seseorang sudah tidak lagi mempunyai hak privasi. Sehingga pada penelitian ini, penulis mengembangkan sebuah aplikasi pada telepon selular berbasis Android yang akan merubah pesan SMS menjadi kode-kode agar isi informasi dari SMS tersebut tidak diketahui orang lain. Bersadarkan permasalahan ini diperlukan pengamanan isi pesan untuk menjaga kerahasiaan isi pesan. Pengamanan isi pesan SMS melalui aplikasi ponsel dengan cara melakukan penyandian (enkripsi) dengan algoritma DES (*Data Encryption Standard)*. Dengan aplikasi enkripsi dan dekripsi pesan ini diharapkan mampu memaksimalkan pengamanan isi pesan terhadap ancaman terhadap pembacaan isi pesan oleh orang yang tidak diinginkan atau tidak memiliki hak dalam pembacaan isi pesan. Pada penelitian ini menggunakan model penelitian *waterfall* dan pengujian *Blackbox*.

Kata Kunci : *Short Message Service Center*, SMS, *Short Message Service*, Kriptografi, DES, *Data Encryption Standard*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR SIMBOL

1. *Activity Diagram*

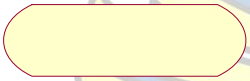
a. Start Point

Menggambarkan awal dari suatu aktivitas yang berjalan pada sistem.

b. End Point

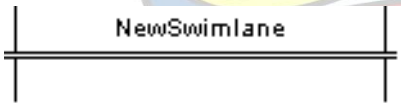
Menggambarkan akhir dari suatu aktivitas yang berjalan pada sistem.

c. Activity



Menggambarkan aktivitas yang dilakukan pada sistem.

d. Swimlane



Menggambarkan pembagian atau pengelompokkan berdasarkan tugas dan fungsi tersendiri.

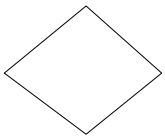
e. Transition State

Menggambarkan hubungan antara dua state, dua activity ataupun antara state dan activity.

f. Transition to self

Menggambarkan hubungan antara state atau activity yang kembali kepada state atau activity itu sendiri.

g. *Decision*

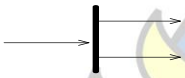


Menggambarkan kondisi dari sebuah aktivitas yang bernilai benar atau salah.

h. *State*

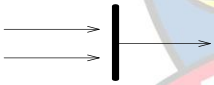
Menggambarkan kondisi, situasi ataupun tempat untuk beberapa aktivitas.

i. *Fork*



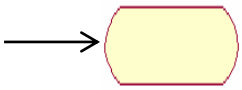
Menggambarkan aktivitas yang dimulai dengan sebuah aktivitas dan diikuti oleh dua atau lebih aktivitas yang harus dikerjakan.

j. *Join*



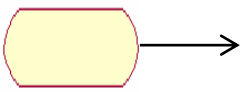
Menggambarkan aktivitas yang dimulai dengan dua atau lebih aktivitas yang sudah dilakukan dan menghasilkan sebuah aktivitas.

k. *Black Hole Activities*



Menggambarkan ada masukan tapi tidak ada keluaran.

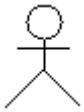
l. *Miracle Activities*



Menggambarkan tidak ada masukan tapi ada keluaran.

2. *Usecase Diagram*

a. Actor



Menggambarkan orang atau sistem yang menyediakan atau menerima informasi dari sistem atau menggambarkan pengguna software aplikasi (user).

b. *Use case*

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

c. Association

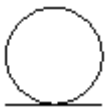
Menggambarkan hubungan antara actor dengan use case.

3. *Sequence Diagram*

a. Actor

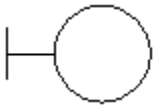
Menggambarkan orang yang sedang berinteraksi dengan sistem

b. Entity



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

c. Boundary

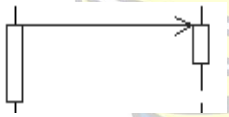


Menggambarkan interaksi antara satu atau lebih actor dengan sistem.

d. Control

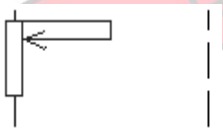
Menggambarkan "perilaku mengatur", mengkoordinasikan perilaku sistem dan dinamika dari suatu sistem, menangani tugas utama dan mengontrol alur kerja suatu sistem.

e. Object Messagee



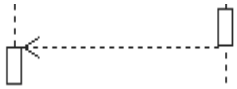
Menggambarkan pesan/hubungan antar objek, yang menunjukan urutan kejadian yang terjadi.

f. Message to self



Menggambarkan pesan/hubungan objek itu sendiri, yang menunjukan urutan kejadian yang terjadi.

g. Return Message



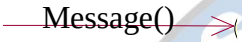
Menggambarkan pesan/hubungan antar objek, yang menunjukan urutan kejadian yang terjadi.

h. Object

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

i. Message

Menggambarkan pengiriman pesan.



j. Loop

Menggambarkan perulangan dalam sequence.