PENERAPAN KRIPTOGRAFI ALGORITMA AES (*ADVANCED ENCRYPTION STANDARD*) SERTA KOMPRESI ALGORITMA *HUFFMAN* PADA APLIKASI *MESSAGE*

SKRIPSI

ELI PATIMA

1511500167

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

ATMA LUHUR

PANGKALPINANG

2018

PENERAPAN KRIPTOGRAFI ALGORITMA AES (*ADVANCED ENCRYPTION STANDARD*) SERTA KOMPRESI ALGORITMA *HUFFMAN* PADA APLIKASI *MESSAGE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

ELI PATIMA

1511500167

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER ATMA LUHUR

PANGKALPINANG

2018

LEMBAR PERNYATAAN

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

NIM : 1511500167

Nama : Eli Patima

Judul Skripsi : PENERAPAN KRIPTOGRAFI ALGORITMA AES (*ADVANCED ENCRYPTION STANDARD*) SERTA KOMPRESI ALGORITMA *HUFFMAN* PADA APLIKASI *MESSAGE*

Menyatakan bahwa Laporan Tugas Akhir saya adalah **HASIL KARYA SENDIRI, 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, 27 Juli 2018

Eli Patima

i

LEMBAR PENGESAHAN SKRIPSI

LEMBAR PENGESAHAN SKRIPSI

PENERAPAN KRIPTOGRAFI ALGORITMA AES SERTA KOMPRESI ALGORITMA HUFFMAN PADA APLIKASI MESSAGE

Yang dipersiapkan dan disusun oleh :

ELI PATIMA
1511500167

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 10 Agustus 2018

Susunan Dewan Penguji **Anggota**	**Dosen Pembimbing**
R. Burham Isnanto F., S.Si, M.Kom **NIDN. 0224048003**	**Laurentinus, M.Kom** **NIDN. 0201079201**
Kaprodi Teknik Informatika	**Ketua**
R. Burham Isnanto F., S.Si, M.Kom **NIDN. 0224048003**	**Dwi Yuny Sylfania, M.Kom** **NIDN. 0207069301**

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

ii

KATA PENGANTAR

Puji syukur kehadirat Tuhan YME yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi 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. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Ayah dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Kakak – kakakku tercinta yang telah memberikan bantuan baik spirit maupun materi untuk terus menyelesaikan skripsi ini.
4. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
5. Bapak Dr. Husni Teja Sukmana, S.T., M.sc, selaku Ketua STMIK Atma Luhur.
6. Bapak R. Burham Isnanto Farid, S.Si., M. Kom Selaku Kaprodi Teknik Informatika.
7. Bapak Laurentinus, M. Kom selaku dosen pembimbing, yang telah memberikan masukan yang sangat berarti dan membimbing penulis sehingga skripsi ini dapat terselesaikan.
8. Teman – teman seperjuangan yang telah membagi ilmu serta memberi warna dalam persahabatan dan kebersamaan yang telah terjalin selama kuliah di STMIK Atma Luhur Pangkalpinang
9. Saudara dan sahabat-sahabatku terutama Kawan-kawan Angkatan 2014 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

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

Pangkalpinang, 27 Juli 2018

Penulis

ABSTRACT

The development of information technology that increasingly rapidly give a very big influence on telecommunications, especially mobile phones. One feature of cellular telephones is SMS (Short Message Service), but this facility in the form of SMS (Short Message Service) has a vulnerability in the form of information leakage, therefore an encryption application is proposed using OOP (Object Oriented Programming) method with Waterfall's model and (Unified Modeling Language) as tools. To the maintain of the confidentiality a message, its required AES (Advanced Encryption Standard) cryptography. Cryptography AES (Advanced Encryption Standard) had functions to encode messages into the form of ciphertext. But the results of the characters from encryption will usually has more than before because there is an addition to the cipher on each encrypted data. Therefore, huffman algorithm compression is needed for text compression so that the results of encrypted messages become less. The purpose of this study is to maintain the confidentiality of messages. The results obtained in this study are differences in the number of text encryption characters AES (Advanced Encryption Standard) with the addition of huffman compression that is 17.35%. The implementation of this message application was successfully implemented using the AES algorithm and the huffman algorithm, then the message is not can be read by the service center and the number of characters sent messages can be compressed into fewer.

Keywords : SMS (Short Message Service), AES (Advanced Encryption Standard) Algorithm, Huffman Algorithm.

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat memberikan pengaruh yang sangat besar terhadap telekomunikasi khususnya telepon seluler. Salah satu fitur telepon seluler adalah SMS (*Short Message Service*), akan tetapi fasilitas berupa SMS (*Short Message Service*) ini memiliki kerentanan berupa kebocoran informasi, maka dari itu diusulkan aplikasi enkripsi menggunakan metode OOP (*Object Oriented Programming*) dengan model *Waterfall* dan *tools* UML (*Unified Modeling Language*). Untuk menjaga kerahasiaan dari sebuah pesan maka dibutuhkan kriptografi algortima AES (*Advanced Encryption Standard*). Kriptografi AES (*Advanced Encryption Standard*) berfungsi untuk menyandikan pesan kedalam bentuk ciphertext. Namun hasil karakter dari enkripsi biasanya akan semakin banyak dibandingkan sebelum dienkripsi, hal tersebut karena ada penambahan chiper pada setiap data yang dienkripsi. Oleh karena itu kompresi algoritma *huffman* dibutuhkan untuk kompresi teks sehingga hasil pesan yang dienkripsi menjadi lebih sedikit. Tujuan dari penelitian ini adalah untuk menjaga kerahasiaan pesan. Hasil yang didapat dalam penelitian ini yaitu perbedaan jumlah karakter *text* enkripsi AES (*Advanced Encryption Standard*) dengan penambahan kompresi *huffman* yaitu 17,35%. Implementasi pada aplikasi pesan ini berhasil diterapkan dengan menggunakan algoritma AES (*Advanced Encryption Standard*) dan algoritma *huffman* sehingga pesan tidak bisa dibaca oleh pihak layanan *center* dan jumlah karakter pesan yang dikirimkan bisa dikompresi menjadi lebih sedikit.

Kata Kunci : SMS (*Short Message Service*), Algoritma AES (*Advanced Encryption Standard*), Algortima *Huffman*.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SIMBOL

1. Simbol *Acivity Diagram*

Start Point (Initial Node)
Merupakan simbol untuk memulai *activity diagram.*

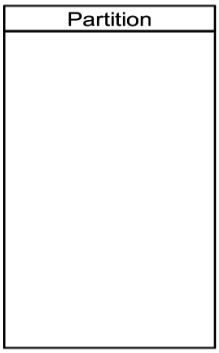
End Point (Activity Final Node)

*M*erupakan simbol untuk mengakhiri *activity diagram*

Transition
Menggambarkan aliran perpindahan kontrol antara *activity*.

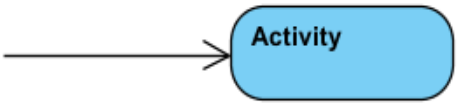
***Activity* (Aktivitas)**

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



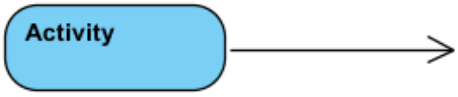
Swimline

Menggambarkan pemisahan atau pengelompokan aktivitas berdasarkan *actor*.



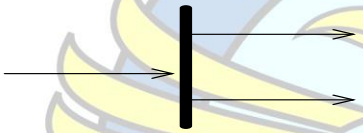
Black Hole Activities

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

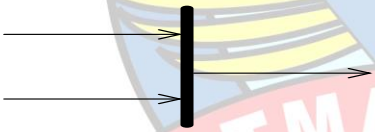


Miracle Activities

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.

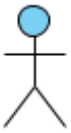


***Join* (Penggabungan)**
Mempunyai 2 atau lebih transisi masuk dan hanya 1 transisi keluar.

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

2. Simbol *Use Case Diagram*

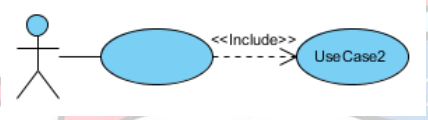
Use case
Gambaran fungsionalitas dari suatu sistem, sehingga pengguna sistem paham dan mengerti mengenai kegunaan sistem yang akan dibangun.



Actor

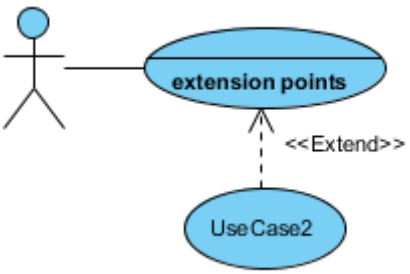
Sebuah sebuah entitas manusia atau mesin yang berinteraksi dengan sistem untuk melakukan pekerjaan-pekerjaan tertentu.

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



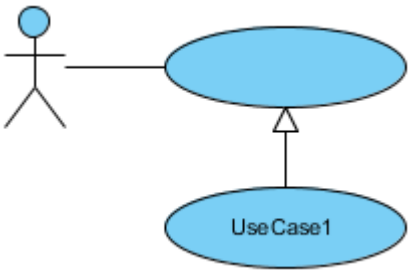
Include

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

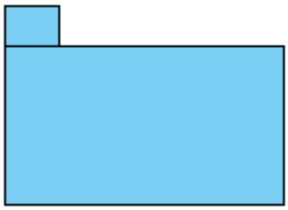


Extend

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 *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

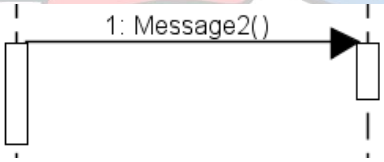
Menggambarkan informasi yang harus disimpan oleh sistem (struktur data dari sebuah sistem).

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.

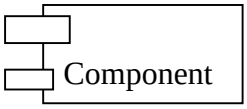


Object Message
Menggambarkan pesan/hubungan antar objek yang menunjukkan urutan kejadian yang terjadi.

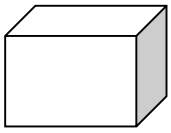
Looping logic

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

4. Simbol *Deployment Diagram*



Pada deployment diagram, komponen-komponen yang ada diletakkan didalam node untuk memastikan keberadaan posisi mereka.



Node mengambarkan bagian-bagian hardware dalam sebuah sistem. Notasi untuk node digambarkan sebagai sebuah kubus tiga dimensi.

Sebuah association digambarkan sebuah garis yang menghubungkan dua node yang mengindikasikan jalur komunikasi antara lement-element hardware


STMIK
ATMA LUHUR
PANGKAL PINANG