APLIKASI KRIPTOGRAFI PESAN SINGKAT DENGAN ALGORITMA *RIVEST CHIPER* 6 (RC6) DAN *BLOWFISH* BERBASIS ANDROID

SKRIPSI

Risky Maulana

1411500049

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

ATMA LUHUR

PANGKALPINANG

2018

APLIKASI KRIPTOGRAFI PESAN SINGKAT DENGAN ALGORITMA *RIVEST CHIPER* 6 (RC6) DAN *BLOWFISH* BERBASIS ANDROID

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Risky Maulana

1411500049

PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG
2018

LEMBAR PERYATAAN

Yang bertanda tangan dibawah ini:

NIM : 1411500049

Nama : Risky Maulana

Judul Skripsi : APLIKASI KRIPTOGRAFI PESAN SINGKAT DENGAN ALGORITMA *RIVEST CHIPER* 6 (RC6) DAN *BLOWFISH* BERBASIS ANDROID

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri 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

Risky Maulana

LEMBAR PENGESAHAN SKRIPSI

APLIKASI KRIPTOGRAFI PESAN SINGKAT DENGAN ALGORITMA *RIVEST CHIPER* 6 (RC6) DAN *BLOWFISH* BERBASIS ANDROID

Yang dipersiapkan dan disusun oleh

Risky Maulana
1411500049

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 2 Agustus 2018

Susunan Dewan Penguji
Anggota

Benny Wijaya, S.T., M.Kom
NIDN. 0202097902

Dosen Pembimbing

Ari Amir Alkodri, M.Kom
NIDN. 0201038601

Kaprodi Teknik Informatika

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

Ketua

Yohanes Setiawan, M.Kom
NIDN. 0219068501

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 Alhamdullillah penulis panjatkan kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunianNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang Strata Satu (S1) 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, pemimbing, dan dorongan berbagai pihak Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah meciptakan dan memberikan kehidupan di dunia.
2. Bapak dan Ibu tercinta atas doa-doanya, dan juga untuk Adik yang telah mendukung dan memberi semangat.
3. Bapak Drs. Djaetun HS yang telah mendirikan Atma Luhur.
4. Bapak Dr. Husni Teja Sukmana, ST., 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 pembimbing teori serta pembimbing aplikasi.
7. Sahabatterdekat dan teman seperjuangan penulis yang tidak bisa penulis sebutkan satu persatu yang selalu memberi semangat.

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

Pangkalpinang, 27 Juli 2018

Risky Maulana

ABSTRACT

Technological development for several years is very rapid, short message technology is still a lot of people who use it, but the security aspect is not guaranteed.People who exchange information are at risk of experiencing theft of information during the shipping process, for this reason it is necessary to have encryption before the message is sent and decryption is done to read so that it is not easily misused by people who do not have authority. With Rivest Chiper 6 and Blowfish cryptographic algorithms this model is one symmetric key algorithm in the form of block cipher that can answer message security, this method is suitable for maintaining message security. This paper will discuss a number of aspects of cryptography and the basic concepts of the Rivest Chiper 6 and Blowfish algorithms. An application designed to implement the Rivest Chiper 6 and Blowfish algorithms. Rivest Chiper 6 and Blowfish algorithms implemented on Android smartphones can encrypt messages before they are sent and decrypt messages when received. By using two encryption options, message security can differentiate the results of the two algorithms and become more secure, the process of encryption and decryption does not take a long time. This application can be used to secure the sending of text messages.

Keywords : Rivest Chiper 6, Blowfish, encryption, decryption, message security

ABSTRAK

Perkembangan teknologi untuk beberapa tahun ini sangat pesat, teknologi pesan singkat masih banyak masyarakat yang menggunakan, tetapi segi keamanan belum terjamin. Orang yang bertukar informasi beresiko mengalami pencurian isi informasi saat proses pengiriman, karena alasan tersebut perlu adanya enkripsi sebelum pesan tersebut dikirim dan dilakukan dekripsi untuk membaca agar tidak mudah disalahgunakan oleh orang yang tidak memiliki kewenangan. Dengan algoritma kriptografi *Rivest Chiper* 6 dan *Blowfish* model ini merupakan salah satu algoritma kunci simetris yang berbentuk *block chiper* yang dapat menjawab keamanan pesan, Metode tersebut cocok untuk menjaga keamanan pesan. Pada tulisan ini akan dibahas sejumlah aspek dari kriptografi serta konsep dasar dari algoritma *Rivest Chiper* 6 dan *Blowfish*. Sebuah aplikasi dirancang untuk dapat mengimplementasikan algoritma *Rivest Chiper* 6 dan *Blowfish*. Algoritma *Rivest Chiper* 6 dan *Blowfish* di Implementasikan pada *smartphone* android dapat mengenkripsi pesan sebelum dikirim dan mendekripsi pesan ketika diterima. Dengan menggunakan dua pilihan enkripsi keamanan pesan pengguna bisa membedakan hasil dua algoritma tersebut dan menjadi lebih terjamin, Proses enkripsi dan dekripsi tidak memakan waktu yang lama. Aplikasi ini dapat di manfaatkan untuk mengamankan pengiriman pesan teks.

Kata kunci :*Rivest Chiper* 6 (RC6), *Blowfish,* enkripsi, dekripsi, keamanan pesan

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR SIMBOL

1. Activity Diagram

Start Point

Mengambarkan awal dari suatu aktivitas yang berjalan pada sistem.

End Point

Menggambarkan akhir dari suatu aktivitas yang berjalan pada sistem.

Activity State

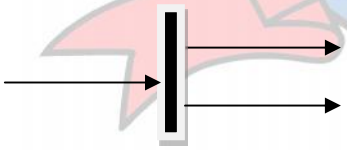
Menggambarkan suatu proses / kegiatan bisnis.

Swimlane

Menggambarkan pembagian / pengelompokkan berdasarkan tugas dan fungsi sendiri.

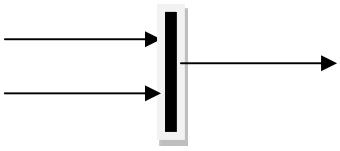
Decision Points

Menggambarkan pilihan untuk pengambilan keputusan, true atau false.



Fork

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



Join

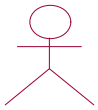
Menggambarkan aktivitas yang dimulai dengan dua atau lebih aktivitas yang sudah dilakukan dan menghasilkan sebuah aktivitas.

[….]	*Guards* Sebuah kondisi benar sewaktu melewati sebuah transisi, harus konsisten dan tidak overlap.
⟶	*Transition* Menggambarkan aliran perpindahan control antara state.

2. *Use Case* Diagram

	*Actor* Abstraksi dari orang atau sistem yang mengaktifkan fungsi dari use case.
	*Use Case* Menggambarkan proses sistem dari perpektif pengguna (user).
	Relasi/Asosiasi Menggambarkan hubungan antara actor dengan use case.
<< include >> ---------->	Assosiasi yang termasuk didalam *use case* lain, yang bersifat harus dilakukan bila *use case* lain tersebut dilakukan.
<<extend>> ---------->	Perluasan dari *use case* lain jika kondisi atau syarat terpenuhi dan tidak harus dilakukan.

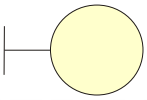
3. Sequence Diagram



Actor

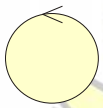
Menggambarkan seseorang atau sesuatu (seperti perangkat, sistem lain) yang berinteraksi dengan sistem.

.



Boundary

Sebuah obyek yang menjadi penghubung antara user dengan sitem.Contohnya window, dialogue box atau screen(tampilan layar).



Control

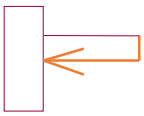
Suatu obyek yangberisi logika aplikasi yang tidak memiliki tanggung jawa kepada entitas.

Entity

Menggambarkan suatu objek yang berisi informasi kegiatan yang terkait yang tetap dan dsimpan kedalam suatu database.

Object Message

Menggambarkan pengiriman pesa dari sebuah objek ke objek lain.



Recursive

Sebuah obyek yang mempunyai sebuah operation kepada dirinya sendiri.

Return Message

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

Lifeline

Garis titiktitik yang terhubung dengan obyek, sepanjang lifeline terdapat activation.

Activation

Activation mewakili sebuah eksekusi operasi dari obyek, panjang kotak ini berbanding dengan durasi aktivasi sebuah operasi.

DAFTAR ISTILAH

1. SMSC = *Short Message Service Center*
2. SMS = *Short Message Service*
3. GSM = *Global Systema For Mobile Communication*
4. TDMA = *Time Division Multiple Access*
5. CDMA = *Code Division Multiple Access*
6. AES = *Advanced Encryption Standard*
7. RC6 = *Rivest Chiper 6*
8. UML = *Unified Modeling Language*