ANALISA KINERJA ALGORITMA RIJNDAEL DAN RC4 DENGAN INPUTAN TEKS DAN FILE TEKS

SKRIPSI

Disusun Sebagai Salah Satu Syarat

Untuk Memperoleh Gelar Sarjana Komputer

pada Departemen Ilmu Komputer / Informatika

Disusun Oleh :

REZA GALIH IMAM PRAKOSO

24010311140092

DEPARTEMEN ILMU KOMPUTER / INFORMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

2016

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini,

Nama : Reza Galih Imam Prakoso
NIM :24010311140092
Judul : Analisa Kinerja Algoritma *Rijndael* dan *RC4* dengan Inputan Teks dan *File* Teks

Dengan ini saya menyatakan bahwa dalam tugas akhir / skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

HALAMAN PENGESAHAN

Judul : Analisa Kinerja Algoritma *Rijndael* dan *RC4* dengan Inputan Teks dan *File* Teks

Nama : Reza Galih Imam Prakoso

NIM : 24010311140092

Telah diujikan pada sidang tugas akhir pada tanggal 18 November 2016 dan dinyatakan lulus pada tanggal **1 Desember 2016**

Semarang, 14 Desember 2016

Mengetahui,
Ketua Departemen Ilmu Komputer/Informatika
FSM UNDIP

Rugil Saputra, S. Si, M. Cs
NIP. 198010212005011003

Mengetahui,
Panitia Penguji Tugas Akhir
Ketua,

Drs. Eko Adi Sarwoko, M.Kom
NIP. 196511071992031003

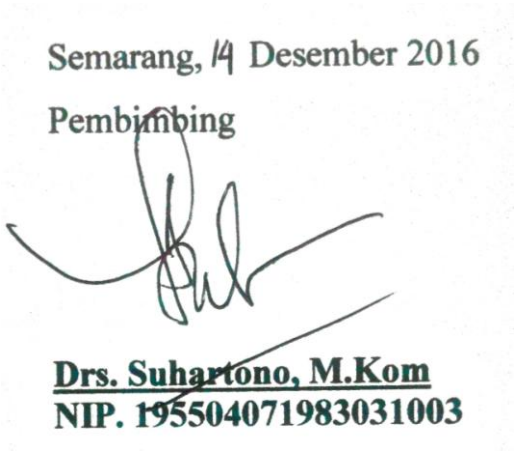
HALAMAN PENGESAHAN

Judul : Analisa Kinerja Algoritma *Rijndael* dan *RC4* dengan Inputan Teks dan *File* Teks

Nama : Reza Galih Imam Prakoso

NIM :24010311140092

Telah diujikan pada sidang tugas akhir pada tanggal 18 November 2016.



ABSTRAK

Kriptografi kerap digunakan dalam pertukaran informasi berupa teks dan berkas digital teks. Informasi yang ada terkandung pada teks atau berkas digital perlu dijaga kerahasiaannya supaya pihak-pihak yang tidak berkepentingan tidak dapat mengetahui informasi tersebut. Untuk melindungi kerahasiaan informasi tersebut, maka teks atau file digital tersebut dienkripsi menggunakan suatu algoritma. Suatu algoritma harus memiliki performa yang baik pada penerapannya di suatu program. Pada penelitian ini dilakukan pengujian kinerja dari algoritma *Rijndael* dan *RC4* pada program berbasis Java dengan tujuan untuk menentukan algoritma mana yang lebih unggul dalam hal kecepatan enkripsi dan dekripsi dan panjang *ciphertext*. Keluaran yang dihasilkan adalah *ciphertext*, jumlah karakter pada *ciphertext* dan waktu hasil enkripsi dari masing-masing algoritma.

Kata Kunci : Teks, Berkas Digital Teks, Algoritma *RC4*, Algoritma *Rijndael*, Kriptografi, Program Berbasis Java.

ABSTRACT

Cryptography is often used in the exchange of information in the form of text and digital text file. The information that is contained in the text or digital files need to be kept confidential so that the parties who are not interested can not know that information. To protect the confidentiality of such information, then the text or digital files are encrypted using an algorithm. An algorithm must have performed well in its application in a program. In this research, testing and performance of the Rijndael algorithm RC4 on a Java-based program with the aim to determine which algorithm is superior in terms of speed and length of encryption and decryption of ciphertext. The output is a ciphertext, the number of characters in the encrypted ciphertext and time of each algorithm.

Keywords: Text, Digital Text File, RC4 Algorithm, Rijndael Algorithm, Cryptography, Java-Based Program.

KATA PENGANTAR

Segala puji bagi Tuhan Yang Maha Kuasa atas karunia-Nya yang diberikan kepada penulis sehinggapenulis dapat menyelesaikan tugas akhir ini. Tugas akhir yang berjudul "Analisa Kinerja Algoritma *Rijndael* dan *RC4* dengan Inputan Teks dan *File* Teks" ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Departemen Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas DiponegoroSemarang.

Dalam penyusunan laporan ini tentulah banyak mendapat bantuan dan dukungan dariberbagai pihak. Untuk itu pada kesempatan ini penulis mengucapkan rasa hormat dan terimakasih kepada :

1. Ragil Saputra, S.Si, M.Cs. selaku Ketua Departemen Ilmu Komputer / Informatika FSM Universitas Diponegoro.
2. Helmi Arif Wibawa, S.Si, M.Cs. selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika FSM Universitas Diponegoro.
3. Drs. Suhartono, M.Kom selaku dosen Pembimbing.
4. Semua pihak yang telah membantu kelancaran dalam pelaksanaan tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materi ataupun dalam penyajiannya karena keterbatasan kemampuan dan pengetahuan penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan. Semoga laporan ini dapat bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya.

Semarang, Desember 2016

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, serta ruang lingkup penelitian.

1.1. Latar Belakang

Masalah keamanan merupakan suatu aspek penting dalam pengiriman data maupun komunikasi melalui jaringan. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi guna membuat pesan, data, maupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak (Tjiharjadi & Wijaya, 2009).

Kriptografi adalah ilmu yang mempelajari mengenai cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan melakukan enkripsi dan dekripsi pada informasi tersebut dengan suatu kunci khusus. Informasi yang belum mengalami proses enkripsi disebut *plaintext*, sedangkan informasi yang telah mengalami proses enkripsi disebut *ciphertext*. Berbagai algoritma kriptografi telah diciptakan oleh para ahli kriptografi, namun sudah banyak yang dapat memecahkannya. Hal ini mendorong para ahli kriptografi untuk menciptakan algoritma-algoritma baru yang lebih aman. Pada bulan Oktober 2000, algoritma *Rijndael* terpilih sebagai AES, dan pada bulan November 2001, algoritma *Rijndael* ditetapkan sebagai AES, dan diharapkan algoritma *Rijndael* menjadi standar kriptografi yang unggul selama 10 tahun (Surian, 2006).

Salah satu teknik pengamanan data dalam kriptografi adalah teknik kriptografi modern, dengan dua teknik dasar yang digunakan yaitu teknik substitusi dan teknik transposisi. Perkembangan algoritma kriptografi modern didorong oleh penggunaan komputer digital untuk keamanan pesan dengan menggunakan data biner. Ada beberapa contoh kriptografi modern yaitu algoritma *Rijndael* dan *RC4*. Algoritma *RC4* merupakan salah satu algoritma kunci simetris berbentuk *stream cipher* yang memproses unit atau *input* data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan *bit* (*byte* dalam hal *RC4*). Algoritma ini tidak harus menunggu

sejumlah *input* data, pesan atau informasi tertentu sebelum diproses atau menambahkan *byte* tambahan untuk mengenkripsi (Sukmawan, 1998).

Algoritma *Rijndael* menggunakan kunci yang sama saat enkripsi dan deskripsi serta memasukkan dan keluarannya berupa blok dengan jumlah *bit* sebesar 128, 196, dan 256 *bit*. Pemilihan ukuran block data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan deskripsi.

Pada penelitian sebelumnya Algoritma *Rijndael* digunakan dalam proses enkripsi dan dekripsi file untuk membantu mengamankan file dan membandingkan library yang terbaik untuk diimplementasi pada sistem operasi android (Langit Da Silva P & Dessyanto & Heriyanto, 2013 : 33-42). Pada penelitian sebelumnya juga algoritma *RC4* digunakan untuk mengenkripsi sebuah data dan disimpan dalam sebuah basis data dengan tujuan untuk menjaga keamanan dan kerahasiaan data (Wachyu & Slamet, 2013).

Tiap-tiap algoritma memiliki perbedaan dalam tingkat kerumitan dan proses perhitungannya, maka dari itu dalam penelitian ini akan dibuat sebuah aplikasi *dekstop* dengan bahasa pemograman *java* untuk membandingkan algoritma *Rijndael* dan *RC4* dengan kunci yang sama yaitu 128 *bit.* Pada dasarnya algoritma *Rijndael* dan *RC4* sama-sama dapat diproses dengan kunci 128 *bit* maka dari itu pada penelitian ini menggunakan kunci 128 *bit* . Dalam penelitian ini menggunakan dua algoritma dengan tujuan untuk menganalisa kinerja dari masing-masing algoritma tersebut bagaimana cara kerjanya dan hasil dari algoritma tersebut serta mengetahui algoritma mana yang lebih unggul baik dalam hal kecepatan enkripsi dan dekripsi dan ukuran *ciphertext* dari kedua algoritma tersebut.

1.2. Rumusan Masalah

Berdasarkan uraian pada latar belakang yang sudah disebutkan, maka dapat dirumuskan suatu permasalahan, yaitu menganalisa kinerja Algoritma *Rijndael* dan *RC4* dengan inputan teks dan *file* teks.

1.3. Tujuan dan Manfaat

Tujuan dilaksanakan Tugas Akhir ini adalah :

1. Menghasilkan program aplikasi kriptografi yang dapat mengamankan data dari sebuah teks dan *file* teks dengan algoritma *Rijndael* dan *RC4.*

2. Menganalisa kinerja algoritma *Rijndael* dan *RC4* dengan inputan teks yang terdapat dalam *keyboard* dan *file* teks yang berekstensi .txt

Manfaat dari penelitian Tugas Akhir ini diantaranya :

Sebagai usaha untuk mengamankan sebuah data dari sebuah file teks dimana hanya orang tertentu saja yang berhak mengetahui.

1.4. Ruang Lingkup

Dalam pengerjaan tugas akhir ini akan dilakukan beberapa pembatasan ruang lingkup agar nantinya pengerjaan tugas akhir ini tidak keluar dari target yang diharapkan, diantaranya adalah sebagai berikut.

1. *Input* data merupakan teks yang terdapat dalam *keyboard* dan *file* teks yang ekstensi .txt.
2. *Output* berupa teks dan file teks yang sudah disandikan.
3. Menganalisa kinerja dua algoritma yaitu algoritma *Rijndael* dan *RC4* dengan menggunakan panjang kunci yang sama yaitu 128 bit.
4. Dalam membandingkan algoritma *Rijndael* dan *RC4* variabel yang digunakan yaitu kecepatan enkripsi dan dekripsi dan ukuran *ciphertext*.
5. Metode Perancangan Sistem yang digunakan adalah metode perancangan *Rational Univiet Process* (RUP), dimana model ini melakukan sebuah pendekatan kepada perkembangan perangkat lunak yang berbasis objek.
6. Pembangunan aplikasi ini menggunakan bahasa pemrograman *java* yang dibantu dengan *software NetBeans*.
7. Teks yang di enkripsi berupa *alphabet* dan simbol-simbol lainnya sesuai dalam *keyboard* dan *file* teks yang berekstensi .txt.

1.5. Sistematika Penullisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Bab ini menjelaskan tentang hal-hal yang melatar belakangi dari pembuatan tugas akhir ini, rumusan permasalahan yang dikerjakan, tujuan

dan manfaat yang diharapkan, ruang lingkup yang membatasi, dan sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Bab tinjauan pustaka menjelaskan tentang istilah-istilah dan metode-metode yang digunakan di dalam penulisan tugas akhir ini.

BAB III DEFINISI KEBUTUHAN, ANALISIS, DAN PERANCANGAN

Bab definisi kebutuhan, analisis dan perancangan sistem ini menjelaskan tentang definisi kebutuhan, analisa dan perancangan sistem yang akan dibuat dan dikembangkan oleh penulis.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini menjelaskan tentang implementasi sistem yang dibangun berdasarkan perancangan yang sudah dijelaskan pada bab sebelumnya, beserta hasil pengujian dari sistem yang dibuat.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dari pengerjaan tugas akhir ini, beserta dengan saran yang dapat diajukan guna pengembangan sistem ini ke depannya.