ENKRIPSI FILE TEXT MENGGUNAKAN ALGORITMA VIGENERE DAN AFFINE CIPHER

SKRIPSI

Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
Pada Jurusan Ilmu Komputer / Informatika

Disusun oleh:

ANDRI RAMADHAN

J2F008090

JURUSAN ILMU KOMPUTER / INFORMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

2015

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Judul : Enkripsi *File Text* Menggunakan Algoritma *Vigenere* Dan *Affine Cipher*

Nama : Andri Ramadhan

NIM : J2F 008 090

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 : Enkripsi *File Text* Menggunakan Algoritma *Vigenere* Dan *Affine Cipher*

Nama : Andri Ramadhan

NIM : J2F 008 090

Telah diujikan pada sidang tugas akhir pada tanggal 27 Agustus 2015 dan dinyatakan lulus pada tanggal 31 Agustus 2015

Semarang, 31 Agustus 2015

Mengetahui,

Ketua Jurusan Ilmu Komputer/
Informatika
FSM UNDIP,

Nurdin Bahtiar, S.Si, MT
NIP. 19790720 200312 1 002

Panitia Penguji Tugas Akhir
Ketua,

Ragil Saputra, S.Si, M.Cs
NIP. 1980 10 21 2005 01 1 003

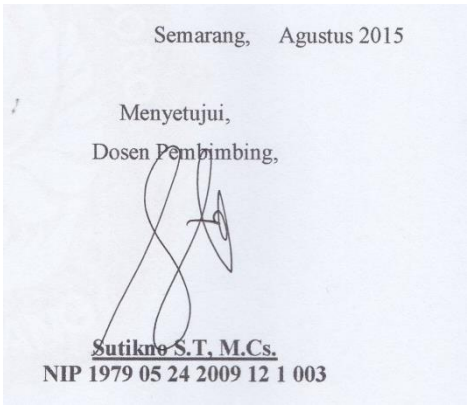
HALAMAN PENGESAHAN

Judul : Enkripsi *File Text* Menggunakan Algoritma *Vigenere* Dan *Affine Cipher*

Nama : Andri Ramadhan

NIM : J2F 008 090

Telah diujikan pada sidang tugas akhir pada tanggal 27 Agustus 2015 dan dinyatakan lulus pada tanggal 31 Agustus 2015



ABSTRAK

Pengiriman pesan rahasia sekarang ini rentan terhadap pencurian data pesan karena tingkat keamanan yang rendah dan datanya mudah dipecahkan. Pada penelitian ini dibangun suatu program atau aplikasi yang dapat berfungsi sebagai sistem keamanan pesan. Aplikasi ini bekerja dengan mengenkripsi dan mendekripsi pesan berupa *file text* dengan dua metode kriptografi, yaitu *vigenere cipher* dan *affine cipher*. Model proses pengembangan perangkat lunak menggunakan *waterfall*. Bahasa pemrograman yang dipakai pada aplikasi ini adalah MATLAB. Aplikasi ini bekerja dengan memasukan *file text* lalu dengan memasukan kunci *vigenere* untuk dienkripsi oleh metode *vigenere cipher* menghasilkan *ciphertext vigenere* lalu dienkripsi lagi oleh *affine cipher* menghasilkan *ciphertext affine* yang disimpan pada *file ciphertext*. Hasil dari enkripsi tersebut didekripsi menggunakan metode *affine cipher* yang menghasilkan *ciphertext vigenere* lalu didekripsi oleh *vigenere cipher* beserta kunci yang sama pada saat enkripsi yang menghasilkan *file text* semula.

Kata kunci : keamanan, *file text*, kriptografi, *vigenere cipher*, *affine cipher*, *ciphertext*, model proses *waterfall*

ABSTRACT

Now, delivering a secret message was vulnerable from message data theft because of the low level of security and data was easily solved. In this part, we were constructed a program or application that could be functioned as a security system message. This application worked when text file were encrypted in the form with two methods of cryptography. Model rocess of software development used waterfall model. The programming language used MATLAB. This application worked by inserting a text file and then entered a key vigenere which encrypted with vigenere cipher method and produced ciphertext vigenere then encrypted again by affine ciphers generate affine ciphertext stored in the ciphertext file. Results of the encryption was decrypted using affine cipher method that produced ciphertext vigenere then decrypted by the vigenere cipher along the same key during the encryption and produced the original text file.

Key : security, text file, cryptography, vigenere cipher, affine cipher, ciphertext, waterfall model

KATA PENGANTAR

Puji syukur pada kehadirat Allah SWT karena berkat Rahmat dan Hidayah-Nya penulis dapat menyelesaikan laporan tugas akhir yang berjudul **"**Enkripsi File Text Menggunakan Algoritma *Vigenere* dan *Affine Cipher***"** dengan baik dan lancar. Laporan tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu (S1) pada Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Pelaksanaan penyusunan laporan tugas akhir ini, banyak mendapat bimbingan, arahan, dan bantuan dari berbagai pihak. Oleh karena itu dengan segala kerendahan hati, penulis ingin mengucapkan terima kasih dengan tulus kepada :

1. Prof. Dr. Widowati, Msi, selaku Dekan FSM UNDIP.
2. Nurdin Bahtiar, S.Si, M.T selaku Ketua Jurusan Ilmu Komputer / Informatika.
3. Indra Waspada, ST, M.TI, selaku Koordinator Tugas Akhir.
4. Sutikno, S.T, M.Cs., selaku dosen pembimbing. .
5. Semua pihak yang telah membantu hingga selesainya tugas akhir ini, yang tidak dapat disebutkan satu persatu. Semoga Allah SWT membalas segala kebaikan yang telah diberikan.

Laporan tugas akhir ini masih banyak terdapat kekurangan baik dari penyampaian materi maupun isi dari materi itu sendiri. Hal ini dikarenakan keterbatasan kemampuan dan pengetahuan dari penulis. Oleh karena itu, kritik dan saran yang bersifat membangun sangat diharapkan.

Semoga laporan tugas akhir ini dapat bermanfaat bagi penulis dan juga pembaca pada umumnya.

Semarang,Agustus 2015

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini memaparkan latar belakang, rumusan masalah, tujuan dan manfaat, dan ruang lingkup penelitian tugas akhir dengan judul "Enkripsi *File Text* Menggunakan Algoritma *Vigenere* dan *Affine Cipher*"

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi pada saat ini telah mengubah cara masyarakat dalam berkomunikasi. Pada era tahun 1910-an, komunikasi jarak jauh masih dilakukan dengan cara konvensional, yaitu dengan cara saling mengirim surat dan beberapa menggunakan telegram. Saat ini penggunaan penyampaian pesan digital dengan perkembangan internet telah banyak digunakan mulai *email*, *chatting*, sms dan sebagainya. Pengguna dari fasilitas ini mencapai angka jutaan, ini bisa dilihat dari jumlah pengguna situs *yahoo*, *gmail*, *twitter* atau *facebook* dan sebagainya. Seiring dengan berkembangnya teknologi saat ini, maka semakin memudahkan para pelaku kejahatan komputer (*cyber crime*), dimana aktivitas mereka sangat mengganggu privasi seseorang dengan menyalahgunakan teknologi komputer yang berkembang pesat. Terbukti tindak kejahatan *cyber crime* di Indonesia saat ini cukup mengkhawatirkan, sehingga menambah tingkat keterpurukan Indonesia di mata dunia Internasional (Hasibuan, 2014).

Berbagai macam teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan data atau pesan agar terhindar dari orang yang tidak berhak. Salah satu cara untuk mengatasi permasalahan tersebut adalah menyandikan pesan rahasia, teknik ini disebut kriptografi. Teknik kriptografi yang sering digunakan pada penelitian sebelumnya adalah *Vigenere Cipher*, namun dengan satu metode kriptografi itu masih bisa dipecahkan oleh *cryptanalis*. Dalam penelitian ini, penulis menambahkan dua metode kriptografi yaitu menggunakan *Affine Cipher* dan *Vigenere Cipher*.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana menerapkan *Vigenere Cipher* dan

Affine Cipher untuk mengenkripsi *file text* dan mendekripsi kembali guna untuk mengamankan data.

1.3 Tujuan dan Manfaat

Tujuan yang ingin dicapai dari pembuatan tugas akhir ini adalah menghasilkan suatu perangkat lunak yang dapat memberikan keamanan sebuah *file text* yang bersifat penting, memberikan kemudahan dalam mengamankan data.

Adapun manfaat yang diharapkan dari penelitian tugas akhir ini adalah meminimalisir gangguan saat pengiriman pesan yang dapat dilakukan oleh penyadap serta mengurangi kekhawatiran pengirim akan tersampaikannya pesan rahasia tersebut ke pihak penerima dengan keamanan yang tetap terjaga.

1.4 Ruang Lingkup Penelitian

Ruang lingkup yang didefinisikan dalam pelaksanaan tugas akhir ini adalah :

1. Pesan yang akan dienkripsi hanya berupa *file text* (**.txt*)
2. Metode kriptografi menggunakan *viginere cipher* dan *Affine Cipher*,
3. Bahasa pemrograman memakai Matlab,
4. Hasil Enkripsi dan Dekripsi pesan ditentukan oleh tabel vigenere yang berjumlah 27 alfabet yaitu huruf A-Z dan spasi(*space*) dengan ketentuan menggunakan *uppercase* pada aplikasi ini
5. Proses pengujiannya menggunakan metode *blackbox*. Pengujian pelatihan data dari *file text* menggunakan parameter kode ASCII yaitu merubah huruf menjadi angka untuk perhitungannya.

1.5 Sistematika Penulisan

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

BAB 1 PENDAHULUAN

Berisi uraian latar belakang masalah, perumusan masalah, tujuan dan manfaat, ruang lingkup penelitian, serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Berisi penjelasan singkat tentang konsep-konsep yang mendukung pengembangan aplikasi, meliputi metode *waterfall*, kriptografi, vigenere cipher, affine cipher, data flow diagram (DFD), flowchart dan Matlab.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Membahas proses pengembangan sistem pada tahap definisi kebutuhan, analisis dan perancangan, dengan hasilnya berupa desain dan rancangan aplikasi yang akan dikembangkan.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Membahas hasil pengembangan aplikasi pada tahap implementasi dan menerangkan rincian pengujian aplikasi.

BAB 5 PENUTUP

Berisi kesimpulan yang diambil berkaitan dengan aplikasi yang dibangun dan saran untuk pengembangan lebih lanjut.