PERANCANGAN DAN IMPLEMENTASI KRIPTOGRAFI ALGORITMA RIVEST CODE 6 PADA FILE DOKUMEN

TUGAS AKHIR

Diajukan Sebagai Persyaratan
Untuk Memperoleh Gelar Ahli Madya dari
Politeknik Universitas Andalas

Oleh

DEBI ABDILLAH
BP. 06 075 005

PROGRAM STUDI TELEKOMUNIKASI MULTIMEDIA
JURUSAN TEKNIK ELEKTRO
POLITEKNIK UNIVERSITAS ANDALAS PADANG
2010

ABSTRAK

Perancangan dan Implementasi Kriptografi Algoritma Rivest Code 6 Pada File Dokumen

Oleh
Debi Abdillah
06 075 005

Keamanan dan kerahasiaan sebuah data dalam komunikasi dan pertukaran informasi sangatlah penting. Seringkali data yang penting, dalam komunikasi dan pertukaran informasi kadang tidak sampai kepada penerima atau tidak hanya diterima oleh penerima tetapi juga oleh pihak lain yang melakukan pembajakan atau penyadapan. Hal ini membuat data tersebut menjadi tidak berguna lagi dan lebih parahnya lagi kadang data atau informasi tersebut oleh pihak pembajak digunakan untuk menjatuhkan pihak lain. Oleh karena itu kriptografi sangat dibutuhkan dalam menjaga kerahasiaan data.

Algoritma kriptografi terdiri dari algoritma enkripsi dan algoritma dekripsi. Enkripsi berguna untuk melindungi data agar tidak terlihat oleh pihak yang tidak berhak. Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan algoritma Rivest Code 6 (RC6). Model ini merupakan salah satu algoritma kunci simetris yang berbentuk block chipe.

Pada tugas akhir ini format file yang bisa diekripsi adalah file dengan format pdf, ppt, dan xlm.

Kata kunci: Kriptografi, RC6(Rivest Code 6), Block cipher, simetris, private key

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi internet dalam beberapa tahun terakhir ini, telah membawa perubahan besar bagi distribusi data, kemudahan distribusi data atau pesan melalui dunia internet disisi lain menimbulkan dampak negatif, yaitu pihak yang tidak bertanggung jawab akan mengacak, menghapus, serta mengambil data pihak lain dan menjadikan sebagai hak ciptanya. Selama ini pesan atau data yang sifatnya tidak bisa diketahui pihak lain yang dikirimkan kesebuah *email*, sebagian beranggapan bahwa pesan atau data tersebut tidak ada yang bisa mengetahuinya, tapi sebenarnya ada pihak *server* yang membaca bahkan mengetahui isi pesan tersebut, karna setiap pesan yang dikirim atau yang masuk akan disimpan didalam sebuah *server* khusus untuk penyimpanan, untuk menghindari hal tersebut maka diperlukannya kriptografi.

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut oleh pihak yang berkepentingan, apakah pesan, data, atau informasi masih autentifikasi atau tidak. Pesan, data, atau informasi yang sifatnya rahasia akan tidak berguna lagi apabila informasi itu di akses oleh pihak-pihak yang tidak berhak atau berkepentingan.

Menurut Menezes et al, Doraiswamy et al. dan Kurniawan, kriptografi adalah seni dan ilmu pengetahuan untuk menjaga keamanan informasi. Orangnya disebut sebagai cryptographer. Kebalikan dari kriptografi adalah cryptanalysis,

yaitu seni dan ilmu untuk memecahkan chipertext menjadi plaintext tanpa melalui cara yang seharusnya. Orangnya disebut sebagai cryptanalyst. Ada beberapa model dan metode enkripsi, diantaranya adalah enkripsi dengan algoritma Rivest Code 2 (RC 2), RC 4, RC 5, RC 6, IDEA, BLOWFISH,TWOFISH, AES,DES dan lain sebagainya.

Salah satu algoritma kriptografi adalah algoritma Rivest code 6 (RC 6) yang memilki keamanan yang cukup tinggi, padat, sederhana serta menawarkan perfomansi yang sangat bagus dan fleksibel untuk Pengamanan suatu data atau informasi, ada dua fitur utama dalam RC 6 dibandingkan dengan RC 5 yaitu perkalian interger dan penggunaan empat buah register yang berukuran w/4 bit. Selain bertujuan untuk meningkatkan keamanan, kriptografi juga berfungsi untuk melindungi pesan, data, atau informasi agar tidak dapat diakses oleh pihak-pihak yang tidak berhak, serta mencegahnya untuk menyisipkan dan menghapus pesan, data, atau informasi tersebut.

Memperhatikan permasalahan diatas maka perlu dibuat sebuah *software* untuk menjaga kerahasiaan data, yaitu dengan teknik kriptografi dengan menggunakan algoritma *rivest code 6*. Dimana algoritma *rivest code 6* selain aman algoritma ini jauh lebih cepat proses kerjanya dibadingkan dengan algoritma *rivest code* sebelumnya.

1.2. Perumusan Masalah

Perumusan masalah yang dapat dirumuskan dari permasalahan di atas adalah sebagai berikut ini :

1. Bagaimana mekanisme kerja enkripsi dan dekripsi data dengan menggunakan algoritma RC 6

2. Bagaimana mengimplementasi algoritma RC 6 di dalam melakukan enkripsi dan dekripsi file.

1.3. Batasan Masalah

Untuk mengatasi permasalahan yang ada di atas, maka cakupan masalah akan dibatasi, yaitu sebagai berikut:

1. Dalam tugas akhir ini akan membahas tentang kriptografi dan algoritma *rivest code* 6
2. Aplikasi memakai algoritma RC 6 dengan proses enkripsi dan deskripsi data
3. Implementasi dari fungsi RC 6 dalam perubahan pesan atau data.

1.4. Tujuan

Tujuan yang ingin dicapai pada pelaksanaan tugas akhir ini untuk memahami tentang teknik kriptografi pada file dokumen seperti *mikrosoft word*, *mikrosoft exel* dan lain sebagainya, dengan menggunakan algoritma *Rivest Code 6* (RC 6) secara langsung serta dapat mengimplementasikan dengan mengekripsi dan dekripsikan data atau file dokumen tersebut.

1.5. Metode Penelitian

Metode yang digunakan dalam pembuatan tugas akhir ini adalah :

1. Studi Literatur

   Dilakukan dengan cara mengumpulkan data dan informasi serta mempelajari referensi penunjang baik yang diperoleh dari buku, media cetak, majalah, maupun pencarian bahan melalui *browsing* di internet yang berhubungan dengan pembuatan kriptografi algoritma RC 6 pada tipe file dokumen menggunakan *software visual C++ 6.0.*

BAB V

PENUTUP

5.1. Kesimpulan

Kesimpulan yang dapat diambil setelah mengimplementasikan kriptografi pada file dokumen dengan menggunakan algoritma RC6 (*rivest code 6)* ini adalah:

1. Proses kerja algoritma *rivest code 6* lebih cepat dibandingkan dengan algoritma rivest code sebelumnya karna RC 6 bekerja dengan empat buah register.
2. Proses enkripsi tidak akan mempengaruhi terhadap ukuran file karena tidak adanya proses padding.
3. Perbedaan terhadap panjang kunci akan sangat mempengaruhi terhadap hasil *chipertext* yang akan dihasilkan.

5.2. Saran

1. Untuk pengembangan tugas akhir ini kedepannya agar bisa ditambahkan sebuah informasi lamanya waktu proses terhadap enkripsi dan pengaruh dari banyaknya program yang masih jalan terhadap waktu yang diperlukan untuk dekripsi atau enkripsinya.
2. Perlu dikembangkan juga atau mengimplementasikan kriptografi algoritma RC 6 ini pada pengamanan *website* dan pengiriman sms pada telepon seluler

DAFTAR PUSTAKA

Abdurohman, Maman. *Analisis Performansi Algoritma Kriptografi RC6.* Fakultas Teknologi Informasi, T. Elektro, ITB. Bandung, 2002.

Andrizal. *Algoritma Enkripsi Rivest Code 5 (RC-5).* Teknik Elektro. ITB. Bandung.

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi.* Yogyakarta: Andi Offset.

Kurniawan, Agus. 2002. *Pemograman jaringan Internet dengan visual C++,* Jakarta: PT Elex Media Komputindo

Panggabean, Igor Bonny Tua. *Perbandingan Algoritma RC6 dengan Rijndael pada AES.* Teknik Informatika. ITB. Bandung

Permana, Rangga Wisnu Adi. *Implementasi Algoritma RC6 Untuk Enkripsi SMS Pada Telepon Selular.* Teknik Informatika. ITB.Bandung

Prayudi , Yudi dan Idham Halik. *StudiI dan Analisis Algoritma Rivest Code 6 (RC6) Dalam, Enkripsi/Dekripsi Data.* Fakultas Teknologi Industri, Teknik Informatika, Universitas Islam Indonesia. Yogyakarta. 2005

Raharjo, budi. 2004. *Mengungkap Rahasia Pemograman dalam C++,* Yogyakarta: Informatika Bandung.

Sadeli, Muhammad. *E-Trik Visual C++ 6.0 Dasar Pemrograman.* Jakarta. Maxikom.