SISTEM KEAMANAN FILE MENGGUNAKAN METODE ENKRIPSI BLOWFSIH

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk mendapatkan gelar Ahli Madya pada

Jurusan Teknologi Informasi Program Studi Teknik Komputer

Oleh :

RIOSTEVANO

BP. 06 093 001

PROGRAM STUDI TEKNIK KOMPUTER

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK UNIVERSITAS ANDALAS

PADANG

2009

ABSTRAK

Kemajuan teknologi informasi saat ini sudah sangat berkembang. Oleh karena itu, banyak terjadi permasalahan-permasalahan yang tidak diinginkan pada jaringan komputer. Permasalahan tersebut tidak hanya merugikan sebelah pihak melainkan kedua belah pihak. Maka dari itu, keamanan dan kerahasiaan file menjadi hal yang sangat penting. Untuk melindungi file tersebut dari pihak-pihak yang mencurigakan diperlukan teknik kriptografi dengan metode enkripsi.

Salah satu metode enkripsi yang dikenal adalah Blowfish. Blowfish merupakan salah satu jenis algoritma enkripsi yang termasuk golongan *Symmetric Cryptosystem* yaitu metode enkripsi yang menggunakan kunci yang sama pada proses enkripsi dan dekripsi.

Dalam tugas akhir ini berisi pembahasan mengenai proses enkripsi file pada algoritma kunci simetri dengan *cipher* blok yaitu algoritma Blowfish. Proses enkripsi dilakukan melalui perhitungan dan implementasi. Proses perhitungan berdasarkan jaringan feistel menggunakan salah satu operasi dari gerbang logika dan enkripsi file di-implementasikan pada salah satu aplikasi yang dikhususkan untuk algoritma ini.

Kata kunci : Algoritma Blowfish

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era globalisasi ini, dimana segala sesuatunya itu berjalan dengan cepat, kemajuan teknologi semakin memudahkan manusia untuk berkomunikasi dan saling bertukar informasi.

Keamanan dan kerahasiaan sebuah file atau informasi dalam komunikasi dan pertukaran informasi menjadi hal yang sangat penting. Itu dikarenakan seringkalinya file atau informasi yang penting kadang tidak sampai ke tangan si penerima atau bisa juga file tersebut sampai ke tangan si penerima tapi file yang di terima tersebut di sadap terlebih dahulu tanpa sepengetahuan dari si pengirim maupun oleh si penerima itu sendiri.

Hal inilah yang seringkali ditakutkan oleh pihak-pihak yang saling ingin bertukar informasi. Mereka takut apakah file yang mereka kirim tersebut bisa sampai ke si penerima atau tidak. Oleh sebab itu, pentingnya file yang di berikan tersebut agar bisa sampai ke penerima dalam bentuk yang autentik diperlukannya sebuah metode untuk merahasiakan file yang dikirim tersebut. Maka pihak-pihak yang bersangkutan kebanyakan saling bertukar informasi itu menggunakan beberapa macam metode untuk menjaga kerahasiaan pesan mereka, diantaranya dengan menggunakan sebuah metode penyandian pesan yang bernama Kriptographi (*Cryptographi*) untuk merahasiakan pesan yang mereka kirimkan.

Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi saat ini. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan informasi. Dalam waktu singkat, amat banyak bermunculan algoritma-algoritma baru yang dianggap lebih unggul daripada pendahulunya.

Namun, tetap saja *cipher* yang digunakan tidak lepas dari penemuan lama. Algoritma kunci simetri termasuk algoritma yang masih sering digunakan dalam pembuatan algoritma kriptografi. Pada saat ini, algoritma enkripsi kunci simetri yang banyak digunakan adalah algoritma blok, yang beroperasi pada suatu potongan pesan (blok) yang berukuran sama (biasanya 64 bit) pada suatu saat.

Semenjak pertama kali ditemukan, telah banyak penemuan-penemuan baru dalam penerapan cipher blok. Salah satunya adalah algoritma Blowfish. Sejak saat itu, telah dilakukan berbagai macam analisis, dan perlahan-lahan mulai mendapat penerimaan sebagai algoritma enkripsi yang kuat. Sampai saat ini dianggap masih belum ada attack yang dapat memecahkan Blowfish. Blowfish adalah algoritma yang tidak dipatenkan dan *license- free*, dan tersedia secara gratis untuk berbagai macam kegunaan.

Berdasarkan permasalahan diatas, maka dilakukan pengkajian dan pembahasan yang dituangkan dalam bentuk tugas akhir dengan judul :

"SISTEM KEAMANAN FILE MENGGUNAKAN METODE ENKRIPSI BLOWFISH".

1.2 Rumusan masalah

Dalam tugas akhir ini yang akan dibahas adalah :

1. Bagaimana memahami cara kerja dan struktur algoritma dari blowfish dalam enkripsi-dekripsi file pada beberapa format file yaitu (.txt), (.doc), (.jpg), dan (.mp3).
2. Bagaimana cara enkripsi file menggunakan blowfish advance cs.

1.3 Tujuan

Tujuan yang ingin dicapai dalam penulisan tugas akhir ini adalah

1. Agar dapat memahami cara kerja dan struktur algoritma dari Blowfish dalam enkripsi-dekripsi file pada beberapa format file yaitu (.txt), (.doc), (.jpg), dan (.mp3).
2. Mengetahui cara enkripsi file menggunakan Aplikasi Blowfish Advance CS.

1.4 Batasan masalah

Adapun batasan masalah yang akan dikaji dalam penulisan tugas akhir ini antara lain :

1. Prinsip kerja dari algoritma blowfish..
2. Implementasi enkripsi-dekripsi file menggunakan Blowfish Advance CS

BAB V

PENUTUP

5.1 Kesimpulan

Dari proses perhitungan algoritma blowfish dan implementasi pada aplikasi yang digunakan dapat disimpulkan bahwa :

1. Operasi utama yang digunakan pada algoritma Blowfish adalah penambahan dan XOR.
2. Pada proses enkripsi terdapat 16 kali putaran, setiap putaran selalu melewati fungsi F.
3. Proses enkripsi sama persis dengan dekripsi hanya dengan membalikkan urutannya saja.
4. Pada dasarnya enkripsi file dengan menggunakan aplikasi sama dengan enkripsi file dengan menggunakan metode perhitungan yang berdasarkan jaringan feistel.
5. Tipe file yang selalu beraturan dari hasil enkripsinya adalah file (.doc).
6. Waktu rata-rata yang diperlukan untuk enkripsi-dekripsi file adalah 0,6 detik.
7. Semakin besar *memory* yang digunakan semakin cepat proses enkripsi-dekripsi berlangsung.

DAFTAR PUSTAKA

Atisatya. 2008. *GERBANG LOGIKA DASAR*. (http://www.wordpress.com)

Fink Donal G. *Electronics Engineers Handbook*. Mac Graw Hill.inc. USA: 1982.

Hazzrock. 2009. *Enkripsi Blowfish*. (http://www.scribd.com).

Prasetyo. 2008. *Gerbang logika digital*. (http://ilmukomputer.org)

Rinaldi. 2008. Blowfish. *Metoda Enkripsi Blowfish*. (http://www.informatika.org)

Triandriyanto, pardede. 2008. *STUDI DAN PERBANDINGAN ALGORITMA IDEA DAN ALGORITMA BLOWFISH*, Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2008), Universitas Gunadarma, Depok, 20-21 Agustus.

W4huv3. 2009. Enkripsi Blowfish. *Sekilas tentang enkripsi Blowfish*. (http://www.blogspot.com)

Yudi. Sistem bilangan. *Sistem Digital*. (http://googlepages.com)