BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan tekonolgi informasi saat ini, semakin mempermudah manusia untuk mengetahui semua hal dalam waktu singkat. Namun tidak semua informasi boleh diketahui oleh publik. Hampir semua program aplikasi seperti MS Word, WordPerfect, Excel, PKZip menyediakan fasilitas proteksi data dengan pem-password-an, tetapi sebenarnya fasilitas ini mudah untuk dibongkar.

Bahkan program khusus yang memproteksi data dengan metode *DES* yang lebih cepat, sebenarnya sangat tidak aman. Metode *DES* yang digunakan mempunyai kesalahan dalam implementasinya yang sangat mengurangi keefektifan dari metode tersebut. Walaupun dapat menerima password sampai 40 karakter, karakter ini kemudian diubah menjadi huruf besar semua dan kemudian di-reduce menjadi 8 karakter.

Hal ini menyebabkan pengurangan yang sangat besar terhadap kemungkinan jumlah kunci enkripsi, sehingga tidak hanya terbatasnya jumlah password yang mungkin, tetapi juga ada sejumlah besar kunci yang equivalen yang dapat digunakan untuk mendekrip file.

Beberapa program akan secara otomatis membongkar proteksi program aplikasi seperti MS Word, Excel, Word Perfect, PKZip 2.x, Quattro Pro dengan sangat mudah, bahkan ada program yang menambahkan 'delay loop' sehingga seolah-olah program tersebut sedang bekerja keras membongkar password. Salah

satu perusahaan tersebut adalah Access Data, mereka membuat software yang dapat membongkar WordPerfect (versi 4.2-6.1, enkripsi 'regular' atau 'enhanced', Microsoft Word (versi 2.0-6.1), Microsoft Excel (semua versi termasuk versi Macintosh), Lotus 1-2-3 (semua versi), Quattro Pro, Paradox, Pkzip, Norton's Diskreet (baik metoda DES maupun 'proprietary'), Novell NetWare (versions 3.x-4.x), dll. Access Data menyediakan program demo yang dapat memecahkan password sampai 10 karakter.

Alasan utama kurang baiknya proteksi dari program-program diatas adalah untuk mendapatkan izin ekspor dari pemerintah Amerika Serikat dengan mudah, karena di sana untuk mengekspor program enkripsi yang kuat memerlukan izin yang ketat dari pemerintah.

Untuk proteksi data yang cukup penting tidak ada jalan lain selain menggunakan program khusus proteksi/enkripsi data. Saat ini telah banyak beredar program khusus proteksi data baik freeware, shareware, maupun komersial. Namun dari segi kecepatan masih perlu dipertanyakan, karena metode-metode enkripsi yang ada biasanya menghasilkan *delay* pada proses enkripsi. Kesalahan fatal lain adalah menyertakan password pada data hasil enkripsi sehingga dengan mudah dapat dicari passwordnya.

Penulis melakukan penelitian ini dengan harapan mampu menghasilkan sebuah software enkripsi data yang dapat memenuhi standar enkripsi dan dapat digunakan secara luas oleh berbagai bidang. Penelitian ini akan mengimplementasikan algoritma *Twofish* yang merupakan salah satu algoritma

kandidat *NIST* (*National Institute of Standard and Technology*) sebagai algoritma pengganti *DES*.

1.2 Rumusan Masalah

Berdasarkan pemaparan diatas maka dapat diidentifikasikan beberapa permasalahan yang dihadapi dalam penelitian ini adalah sebagai berikut :

1. Dari pengamatan penulis kekuatan dari metoda-metoda enkripsi adalah pada kunci (dari password yang kita masukkan) sehingga walaupun algoritma metoda tersebut telah tersebar luas, orang tidak akan dapat membongkar data tanpa kunci yang tepat. Walaupun tentunya untuk menemukan metoda tersebut diperlukan teori matematika yang cukup rumit. Tetapi intinya ialah bagaimana penulis mengimplementasikan metoda-metoda yang telah diakui keampuhannya tersebut didalam aplikasi sehingga dapat meningkatkan keamanan dari aplikasi yang dibuat.
2. Bagaimana membuat program enkripsi yang cepat. Mengingat jalur informasi yang semakin cepat, membutuhkan tingkat keamanan data dan informasi yang tinggi yang tidak memakan banyak waktu.
3. Bagaimana membuat program enkripsi yang mudah dikoreksi dalam perancangannya, sesuai dengan karakter algoritma enkripsinya.

1.3 Batasan Masalah

Dari rumusan masalah di atas, maka penulis menentukan batasan masalah. Hal ini sebagai solusi permasalahan, serta untuk membatasi lingkup pembahasan masalah yang telah ditentukan. Yaitu sebagai berikut:

1. Model kriptosistem dirancang dan dibuat sebagai program keamanan data berbasis desktop dengan data terbatas.
2. Model kriptosistem diimplementasikan ke dalam bahasa pemrograman Java dengan spesifikasi *J2SE (java to standart edition)*. Dan dijalankan dalam sistem operasi Windows.
3. Model kriptosistem hanya sebatas pengimplementasian algoritma Twofish dan tidak membahas tentang distribusi kunci.
4. Pada implementasi Algoritma Twofish yang optimal, Twofish dapat mencapai kecepatan 17,8 *clock cycle* per byte. Dengan catatan syarat-syarat optimasi terpenuhi :
    a. Kunci dalam proses enkripsi dan dekripsi menggunakan kunci yang sama (kunci simetrik) dengan panjang karakter kunci minimal 8 karakter dan maksimal 56 karakter.
    b. Lebih aman jika diterapkan tanpa adanya pengurangan jumlah iterasi (dengan asumsi *user* tidak menggunakan *weak key*).
    c. Diterapkan untuk aplikasi yang tidak sering berganti kunci.

1.4 Tujuan Penelitian

Tujuan dari penerapan algoritma Towfish ini adalah untuk membuat sebuah model kriptosistem yang mampu meningkatkan keamanan data. Selain itu, penelitian ini juga bertujuan untuk menganalisis kinerja algoritma Towfish dengan simulasi data terbatas.

1.5 Manfaat Penelitian

Manfaat yang diharapkan adalah alternatif enkripsi data menggunakan algoritma Towfish ini mampu diterapkan secara tepat oleh pihak-pihak maupun instansi yang menginginkan kerahasiaan dari informasi yang dimiliki tetap terjaga. Sehingga didapatkan kinerja program yang berkualitas untuk mendapatkan sebuah model kriptosistem yang baik dan dapat dikembangkan lebih lanjut menjadi sebuah algoritma yang sulit untuk dibongkar oleh seorang *cryptanalysis*.

1.6 Metode Penelitian

Metode penelitian merupakan cara atau teknik yang dilakukan peneliti untuk menyusun suatu karya tulis dan mengumpulkan data-data yang dibutuhkan. Dalam kasus ini penulis menggunakan beberapa metode pengumpulan data, yaitu:

1. Metode Observasi

   Metode ini merupakan cara untuk melakukan pengamatan secara langsung terhadap objek penelitian. Menggali dan merumuskan masalah yang ada selama ini dan menentukan solusi permasalahan.

2. Metode Wawancara

   Metode ini merupakan metode pengumpulan data dengan cara wawancara terhadap pihak-pihak yang bersangkutan dan orang-orang yang berkompeten di bidang IT khususnya bidang keamanan data sebagai nara sumber.

3. Metode Kepustakaan

   Metode kepustakaan merupakan studi literatur untuk mengumpulkan data atau informasi yang berhubungan dengan objek penelitian yang dilakukan. Penulis melakukan studi literatur dari berbagai tulisan ilmiah dan melakukan download data dari berbagai macam sumber di internet.

4. Metode Eksperimental

   Metode eksperimental dilakukan dengan cara mengimplementasikan perancangan yang telah dibuat ke dalam komputer. Objek dalam hal ini penulis menyajikan simulasi enkripsi dan dekripsi data serta hasil dan analisanya.

1.7 Sistematika Penulisan

Sistematika penulisan laporan disusun menggunakan dasar-dasar penulisan ilmiah. Metode ini dilakukan agar penyusunan laporan menjadi lebih teratur dan mudah dipahami. Sistematika laporan dibagi dalam lima bab, yaitu sebagai berikut:

Bab I : Pendahuluan

Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan metode pengumpulan data.

Bab II : Dasar Teori

Bab ini berisi tentang dasar-dasar teori yang digunakan dalam penelitian.

Bab III : Perancangan dan Implementasi Sistem

Bab ini berisi mengenai semua hal yang harus dipersiapkan dalam penelitian, baik dari sisi hardware maupun software. Serta perancangan antar muka sistem.

Bab IV : Uji Coba Sistem

Bab ini berisi mengenai uji coba kesesuaian sistem dengan rancangan sebelummnya.

Bab V : Penutup

Bab ini merupakan bab penutup yang menyajikan kesimpulan penelitian serta saran.