

BAB I

PENDAHULUAN

I.1. Latar Belakang Masalah

Metode kriptografi digunakan untuk mengamankan data yang bersifat rahasia agar tidak diketahui oleh orang lain. Metode kriptografi yang dapat digunakan untuk mengamankan data ada bermacam-macam. Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Namun, masalah utamanya adalah bagaimana mengetahui dan memahami cara kerja atau algoritma dari metoda kriptografi tersebut. Penulis memilih metode kriptografi RC5 karena menurut Rivest metode RC5 ini merupakan algoritma *state table* yang terbaik dan teraman yang disediakan untuk *secure socket layer*.

Data dokumen merupakan data yang dapat digolongkan sebagai data pribadi. Salah satu cara mengamankan data dokumen itu memberikan pengamanan *file* tersebut. *File* dokumen yang berjenis teks di aplikasikan dengan perangkat lunak *Microsoft word* atau notepad. Data ini isinya sebenarnya sifatnya rahasia karena seseorang yang menggunakan aplikasi untuk surat menyurat, isi dari surat menyurat ini sifatnya sangat rahasia sekali jika tidak dilakukan pengamanan maka isi surat tersebut bisa dirusak orang bukan itu saja tetapi isi dari surat itu dapat dibaca seseorang dan itu bisa disalah gunakan bagi orang yang tidak bertanggung jawab.

Berdasarkan uraian diatas penulis mengangkat judul ”**Perancangan Aplikasi Sistem Keamanan Data Menggunakan Metode RC5**”.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah pada penulisan skripsi ini adalah :

1. Mengamankan data dengan memberikan sandi menggunakan metode RC5.
2. Untuk menghindari pembacaan isi *file* data yang asli.

I.2.2 Rumusan Masalah

Berdasarkan identifikasi masalah diatas adapun yang menjadi rumusan masalah pada penulisan skripsi ini adalah :

1. Bagaimana merancang pembuatan sistem keamanan data kriptografi menggunakan metode RC5 ?
2. Bagaimana membangun aplikasi keamanan menggunakan metode RC5 ?

I.2.3. Batasan Masalah

Agar pembahasan tidak menyimpang dari tujuannya maka dilakukan pembatasan masalah sebagai berikut:

1. Aplikasi dalam penanganan keamanan data menggunakan metode RC5.
2. Sistem keamanan data yang dibangun berformat txt.
3. Perancangan aplikasi menggunakan pemrograman visual studio 2010.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan dari penelitian ini adalah :

1. Membangun aplikasi kemananan data dengan menggunakan metode RC5.
2. Mengetahui proses keamanan *file* data menggunakan metode RC5

3. Mengetahui kelebihan dan kekurangan metode RC5.

I.3.2. Manfaat

Manfaat dari penelitian ini adalah

1. Aplikasi RC5 dapat digunakan sebagai fasilitas pendukung dalam proses sistem keamanan data.
2. Dengan aplikasi RC5 ini maka isi dari data tersebut tidak dapat dibaca lagi tanpa seijin pemiliknya.
3. Sebagai bahan referensi bagi peneliti lain yang ingin merancang pengembangan aplikasi tentang RC5.

I.4. Metodologi Penelitian

Berisi langkah-langkah diperlukan untuk mencapai tujuan perancangan yang dilakukan. Adapun metodologi dalam pengumpulan data adalah:

1. Studi Pustaka dan Literatur

Pada tahap ini dilakukan pengumpulan informasi yang diperlukan untuk sistem kriptografi RC5. Informasi tersebut dapat diperoleh dari literatur, buku-buku dan *internet*.

2. Metode Perancangan

Pada tahap ini melakukan perancangan yang meliputi :

- a. Perancangan Layar

Merancang tampilan *user interface* aplikasi RC5.

- b. Perancangan Sistem

Merancang sistem yang akan berjalan pada aplikasi RC5

c. Implementasi

Mengimplementasikan rancangan-rancangan yang telah dibuat.

I.4.1. Bagaimana sistem yang lama dengan sistem yang akan dirancang

Berdasarkan analisa yang penulis lakukan, ada beberapa kekurangan dalam sistem yang lama antara lain sebagai berikut :

1. Apabila data dokumen itu dibuka maka isi dari data asli langsung ditampilkan.
2. Penyajian tanpa menggunakan *enkripsi* tidak terjamin keaslian datanya lagi.

I.4.2. Sistem yang akan dirancang

1. Sistem yang dirancang adalah sistem keamanan *file* data dengan metode RC5.
2. Sistem yang dirancang dapat menghasilkan data tersebut terenkripsi.

I.4.3. Pengujian / Uji Coba sistem yang sudah dibuat

Pada tahapan ini penulis akan menguji dan menilai hasil implementasi serta menguraikan kebutuhan minimum dari perangkat lunak yang dibangun baik *software* maupun *hardware*.

I.5. Sistematika Penulisan

BAB I : PENDAHULUAN

Dalam bab I membahas tentang latar belakang, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Berisikan kajian teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Berisikan tentang analisa sistem yang sedang berjalan dan usulan sistem yang akan dirancang pada penulisan skripsi ini. Selain itu, juga berisikan tentang rancangan sistem yang akan dibangun.

BAB IV : HASIL DAN UJI COBA

Berisi tentang tampilan hasil sistem yang dirancang, pembahasan hasil dan uji coba sistem yang dibuat serta memaparkan kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Bab ini merupakan rangkuman hasil penelitian berupa kesimpulan dan saran yang mungkin berguna bagi perusahaan di masa yang akan datang.