BAB I

PENDAHULUAN

I.1. Latar Belakang

Ilmu yang mempelajari tentang cara-cara pengamanan data dikenal dengan istilah Kriptografi, sedangkan langkah-langkah dalam kriptografi disebut algoritma kriptografi. Kriptografi merupakan suatu seni dimana sebuah data diamankan melalui proses penyandian. Pada permulaannya kriptografi digunakan untuk mengamankan sebuah data berupa teks. Bermacam-macam algoritma yang digunakan dalam mengamankan sebuah data.

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 notepad atau wordpad. Data sebenarnya sifatnya rahasia karena seseorang yang menggunakan aplikasi wordpad 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 disalahgunakan bagi orang yang tidak bertanggung jawab.

Dalam proses penyandian, penyandian yang digunakan adalah RSA *Coding* dan MD5, dimana RSA dan MD5 merupakan proses penyandian kunci asimetris, sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitan. Kunci umum dan kunci pribadi yang digunakan adalah suatu bilangan prima , dan disarankan bilangan prima yang besar. Hal ini digunakan untuk

pencegahan usaha pemecahan *chipper text*, karena semakin besar bilangan prima yang digunakan sebagai kunci maka semakin sulit mencari bilangan besar sebagai faktornya.

Berdasarkan uraian diatas penulis mengangkat judul ”**Studi Perbandingan Algoritma RSA dan MD5 Untuk Keamanan Data Teks**”.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah pada penulisan skripsi ini adalah :

1. Dalam segi mengamankan data metode RSA sulit dalam memfaktorkan bilangan yang besar menjadi faktor-faktor prima sedangkan metode MD5 kesulitannya dalam hal menemukan bilangan terbatas pada keluaran dan bilangan tak terbatas pada masukannya.
2. Saat ini belum begitu banyak aplikasi studi perbandingan keamanan data algoritma RSA dan MD5.

I.2.2. Rumusan Masalah

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

1. Bagaimana membangun sistem keamanan data menggunakan metode RSA dan MD5 ?
2. Bagaimana memahami perbandingan keamanan data antara metode RSA denga MD5 ?

I.2.3. Batasan Masalah

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

1. Sistem yang dirancang dalam penanganan keamanan data teks menggunakan metode RSA dan MD5.
2. Bahasa pemrograman dalam perancangan aplikasi keamanan data menggunakan program visual studio 2010.
3. Dalam perancangan aplikasi keamanan data dilakukan dengan menggunakan diagram UML

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan dari penelitian ini adalah :

1. Memperoleh aplikasi kemananan *file* data dengan memanfaatkan metode RSA dan MD5.
2. Mengetahui kelebihan dan kekurangan aplikasi pengamanan data menggunakan metode RSA dan MD5.
3. Mengetahui proses keamanan *file* data menggunakan metode RSA dan MD5.

I.3.2. Manfaat Penelitian

Manfaat dari penelitian ini adalah

1. Menambah pengetahuan dalam melakukan pengamanan data teks menggunakan metode RSA dan MD5.

2. Perbandingan RSA dan MD5 sebagai bahan referensi bagi peneliti lain yang ingin mengembangkannya dalam proses pengamanan data teks.
3. Perangkat lunak perbandingan RSA dan MD5 untuk mempermudah dalam mengamankan data yang berjenis teks.

I.4. Metodologi Penelitan

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 RSA dan MD5. Informasi tersebut dapat diperoleh dari literatur, buku-buku dan *internet*.

2. Diskusi

Berupa konsultasi dengan dosen pembimbing dan rekan-rekan mahasiswa mengenai masalah yang timbul dalam penulisan.

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 studi perbandingan antara RSA dan MD5.
2. Sistem yang dirancang dapat menghasilkan data yang lebih aman.

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, 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 di masa yang akan datang.