BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kriptografi merupakan salah satu komponen yang tidak dapat diabaikan dalam membangun keamanan komputer. Kriptografi merupakan suatu ilmu dan seni (*science and art*) dalam penyandian data, yang bertujuan untuk menjaga kerahasiaan dan keamanan data dari serangan ataupun diketahui oleh pihak yang tidak berhak. Dikatakan ilmu (*science*) karena menggunakan matematika aljabar, terutama teori bilangan sebagai dasarnya. Dikatakan seni (*art*) karena dalam aplikasinya memiliki pola-pola tertentu dalam proses penyandian yang unik.

Penelitian mengenai kriptografi pun telah banyak dilakukan oleh para kriptoanalis. Antara lain Inu Laksito Wibowo (2001), Gok Asido Haro (2006), Retno Aji Wulandari (2009), Roby Irawan (2009), Eka Saefan Rukzam (2009), dan Nefianti (2009). Dari penelitian yang telah mereka lakukan menghasilkan program aplikasi untuk melakukan enkripsi data, baik berupa teks maupun gambar dengan berbagai metode dan algoritma yang berbeda-beda dan platform yang berbeda pula dalam pengimplementasiannya. Namun dari semua penelitian tersebut belum ada yang melakukan proses enkripsi dan dekripsi data sekaligus melakukan proses *digital signature* (tanda tangan digital), yang digunakan untuk mengetahui apakah ini benar-benar data yang berasal dari sistem yang dimaksud, maka perlu melakukan suatu verifikasi. Kemudian data yang terenkripsi dan data *signature* selanjutnya dikirim.

Penulis melakukan penelitian ini dengan harapan mampu menghasilkan sebuah model kriptosistem untuk mengenkripsi dan mendekripsi data yang sangat penting dan rahasia sekaligus melakukan *digital signature*, sehingga dapat digunakan secara luas di berbagai bidang. Oleh sebab itu penulis mengambil judul penelitian yaitu " Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature Dengan .NET ".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka yang menjadi pokok permasalahan dalam penulisan laporan skripsi ini adalah :

1. Bagaimana mengimplementasikan algoritma RSA untuk pengamanan data sehingga data tersebut dapat dijaga keaslian dan kerahasiaanya?
2. Bagaimana melakukan proses enkripsi dan dekripsi data sekaligus melakukan proses *digital signature* (tanda tangan digital) untuk keabsahan data?
3. Bagaimana cara melakukan pengujian terhadap penerapan-penerapan tersebut?

1.3 Batasan Masalah

Berdasarkan rumusan masalah di atas, adapun batasan masalah dalam penulisan laporan skripsi ini adalah :

1. Model kriptosistem ini dirancang dan dibuat sebagai program keamanan data berbasis *desktop*.

2. Lingkup permasalahan hanya dibatasi pada penggunaan algoritma RSA untuk pengolahan data berbasis file teks (*.txt), dan file non-teks yaitu file dokumen (*.doc, dan *.pdf), file gambar (*.bmp, *.gif, dan *.jpg), serta file audio (*.mp3) pada proses enkripsi dan dekripsi.
3. Model kriptosistem ini mengimplementasikan *digital signature* dengan .NET dimana proses *signature* serta verifikasi data hanya diterapkan pada enkripsi dan dekripsi file teks (*.txt).
4. Model kriptosistem ini dibangun pada sistem operasi Windows Vista Home Basic®, dan bahasa pemrograman yang digunakan adalah program Microsoft Visual Studio 2008® serta komponen .NET Framework.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penulisan skripsi ini adalah:

1. Mengimplementasikan algoritma RSA ke dalam suatu perangkat lunak untuk mengamankan data berbasis file teks (*.txt), dan file non-teks yaitu file dokumen (*.doc, dan *.pdf), file gambar (*.bmp, *.gif, dan *.jpg), serta file audio (*.mp3).
2. Sebagai tinjauan enkripsi dan dekripsi yang sudah ada dengan algoritma enkripsi yang dibuat akan menjadi acuan dalam pembentukan ide logika dan algoritma yang mungkin dikembangkan dikemudian hari.
3. Menghasilkan model kriptosistem guna meningkatkan keamanan data yang sangat penting dan rahasia agar tidak dapat diakses oleh orang yang tidak berhak.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dalam penulisan skripsi ini antara lain :

1. Model kriptosistem ini dapat diterapkan secara tepat oleh pihak-pihak maupun instansi yang menginginkan kerahasian dan informasi yang dimiliki tetap terjaga dari pihak-pihak yang tidak berhak.
2. Untuk kedepannya, model kriptosistem ini dapat dikembangkan menjadi aplikasi yang dapat mengenkripsi semua ekstensi file baik file teks, gambar, audio dan video maupun suatu direktori atau *drive* tertentu sesuai kebutuhan pengguna dan penambahan beberapa *tool* untuk meningkatkan performa aplikasi itu sendiri.

1.6 Metodologi Penelitian

Metode yang digunakan dalam penulisan skripsi ini yaitu :

1. Melakukan studi pustaka untuk mengetahui kelebihan dan kelemahan dari penelitian yang telah dilakukan, metode-metode berupa algoritma yang digunakan dan *software* yang diperlukan dalam penelitian.
2. Persiapan dalam penelitian, baik alat maupun hal penunjang lainnya.
3. Perancangan antarmuka model kriptosistem.
4. Implementasi algoritma ke dalam program.
5. Melakukan serangkaian uji coba dan simulasi model program yang dibangun untuk mengetahui letak kesalahan program.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini menguraikan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menguraikan hasil peninjauan pustaka mengenai penelitian-penelitian yang telah dilakukan sebelumnya dan dasar teori yang menunjang penyelesaian masalah dalam penyusunan laporan skripsi ini.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas tentang alat-alat penelitian yang digunakan baik dari segi hardware maupun software dan cara penelitian yang dilakukan.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi tentang implementasi penelitian serta hasil yang diperoleh, dan terakhir pengujian model yang dibangun.

BAB V PENUTUP

Bab ini terdiri atas kesimpulan dari keseluruhan bab mengenai penelitian yang telah dilakukan yang dapat menjawab pertanyaan pada rumusan masalah serta saran oleh penulis guna mengembangkan aplikasi ini agar lebih baik lagi.