BAB I

PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu sistem, pesan, data atau informasi. Masalah keamanan seringkali kurang mendapat perhatian dari para perancang dan pengelola sitem informasi. Seringkali masalah keamanan berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih authentifikasi. Pesan, data, atau informasi akan tidak menjadi rahasia lagi apabila di tengah jalan informasi itu di akses oleh orang yang tidak berhak atau berkepentingan.

Kriptografi merupakan seni dan ilmu untuk menjaga keamanan data. Dalam menjaga keamanan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali (Rahardjo Budi 2004).

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan dari kunci yang dipakainya. Algoritma Simetri, menggunakan satu kunci untuk enkripsi dan deskripsinya. Algoritma Asimetri, mengunakan kunci yang berbeda untuk enkripsi dan dekripsinya. Algortima terakhir adalah *Hash Function*. Algoritma Asimetri mempunyai beberapa beberapa macam algoritma antara lain RSA, DSA, Diffie-Helman (Ariyus Dony, 2006).

RSA adalah salah satu model dan metode enkripsi. Keamaan enkripsi dari RSA cukup baik, hal ini terjadi karena sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima (Munir Rinaldi, 2006). RSA banyak diaplikasikan untuk mengenkripsi teks. Teks merupakan data yang penting dan paling sering digunakan, apalagi jika teks tersebut berisi rahasia penting suatu perusahaan maupun rahasia pribadi seseorang. Data teks sering menjadi sasaran kejahatan. Sebagai contoh, teks yang berisi privasi seseorang diambil kemudian di-publishkan ke internet oleh orang yang tidak berhak. Maka untuk melindungi teks tersebut dari orang-orang yang tidak berhak, akan dibuat sebuah aplikasi kriptografi file teks menggunakan algoritma RSA.

1.2 Perumusan masalah

Perumusan masalahnya yaitu “Bagaimana membuat suatu aplikasi enkripsi data pada file teks menggunakan algoritma RSA?“

1.3 Pembatasan Masalah

Pembatasan masalah penelitian ini adalah aplikasi kriptografi pada file teks berformat .txt (notepad) dengan algoritma RSA dan panjang karakter maksimal 1000 karakter.

1.4 Tujuan

Penelitian ini bertujuan untuk membuat suatu aplikasi enkripsi data pada file teks menggunakan algoritma RSA.

1.5 Manfaat Penelitian

Penulisan tugas akhir ini dapat memberikan manfaat bagi para pengguna email, dan bagi para pengguna yang mempunyai banyak dokumen rahasia, sebagai berikut:

1. Dapat melindungi isi pesan, data, atau isi informasi agar tidak dapat diakses oleh orang-orang yang tidak berhak.
2. Dapat mencegah orang-orang yang tidak berhak, menyisipkan atau menghapus isi pesan, data atau isi informasi.

1.6 Metoda Penelitian

Metode yang digunakan dalam melakukan penelitian ini adalah :

1.6.1 Metoda pengumpulan data

Metode pengumpulan data yang digunakan dalam penelitian ini menggunakan metode *Library Research* (Penelitian Kepustakaan) yaitu mengumpulkan data-data dengan cara membaca buku dan jurnal ilmiah yang berhubungan dengan penulisan penelitian ini.

1.6.2 Metoda pengembangan perangkat lunak

Dalam penelitian ini metode pengembangan perangkat lunak yang digunakan adalah Model *Waterfall*. Model *Waterfall* adalah Model pertama yang diterbitkan untuk proses pengembangan perangkat lunak diambil dari proses rekayasa lain (Royce, 1970). Berkat penurunan dari satu fase ke fase yang lainnya, model ini dikenal sebagai ‘model air terjun’ atau siklus hidup perangkat lunak.

Tahap-tahap utama dari model ini memetakan kegiatan-kegiatan pengembangan dasar yaitu :

1. Analisis dan definisi persyaratan. Pelayanan, batasan dan tujuan sistem ditentukan melalui konsultasi dengan user sistem. Persyaratan ini kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi sistem.
2. Perancangan sistem dan perangkat lunak. Proses perancangan sistem membagi persyaratan dalam sistem perangkat keras atau perangkat lunak. Kegiatan ini menentukan arsitektur secara keseluruhan. Perancangan perangkat lunak melibatkan identifikasi dan deskripsi abstraksi sistem perangkat lunak yang mendasar dan hubungan-hubungannya.
3. Implementasi dan pengujian unit. Pada tahap ini, perancangan perangkat lunak direalisasikan sebagai serangkaian program atau unit program. Pengujian unit melibatkan verifikasi bahwa setiap unit telah memenuhi spesifikasinya.
4. Integrasi dan pengujian sistem. Unit program atau program individual diintegrasikan dan diuji sebagai sistem yang lengkap untuk menjamin bahwa persyaratan sistem telah tepenuhi. Setelah pengujian sistem, perangkat lunak dikirim kepada pelanggan.
5. Operasi dan pemeliharaan. Biasanya, ini merupakan fase siklus hidup yang paling lama. Sistem diinstall dan dipakai. Pemeliharaan mencakup koreksi dari berbagai error yang tidak ditemukan pada tahap-tahap terdahulu, perbaiakan atas implementasi unit sistem dan pengembangan pelayanan sistem, sementara persyaratan-persyaratan baru ditambahkan. Pada Tahap ini tidak termasuk dalam penelitian tugas akhir.

1.7 Sistematika Penulisan

Untuk memberikan gambaran secara garis besar, berbagai isi dari laporan penulisan, berikut akan diuraikan secara singkat sistematika penulisannya sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini akan menjelaskan tentang latar belakang penulisan, perumusan masalah, batasan masalah, tujuan, manfaat, metoda penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini berisi tentang teori– teori dasar kriptografi, teori-teori yang digunakan sebagai landasan dan acuan dalam penulisan skripsi, baik itu teori dasar atau umum dan teori khusus yang berhubungan dengan topik yang dibahas.

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini akan dibahas antara lain: Analisis Sistem yang akan dibuat, Struktur Datanya, Desain Input dan Output, Desain Menu dan model yang akan digunakan.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bab implementasi dan pengujian, akan dibahas adalah proses pembuatan program serta program inti atau prosedur inti itu sendiri beserta tampilan, dan pengujian program baik berupa pengujian alur algoritma atau pengujian secara fungsionalitas.

BAB V PENUTUP

Bab ini merupakan bab terakhir dimana penulis mencoba untuk menarik kesimpulan dan memberikan saran yang diperoleh selama pelaksanaan penelitian.