BAB I

PENDAHULUAN

1.1 Latar Belakang

Pemakaian teknologi komputer sebagai salah satu aplikasi dari teknologi informasi sudah menjadi suatu kebutuhan, seiring dengan kemajuan teknologi, teknologi *instant messanger* yang dulu hanya digunakan untuk melakukan percakapan dalam satu jaringan terpadu sekarang sudah bisa digunakan untuk saling bertukar *file*. Dengan berkembangnya teknik telekomunikasi dan sistem pengolahan data yang berkaitan erat dengan komunikasi antar pengguna komputer yang satu dengan pengguna komputer yang lain yang berfungsi untuk menyalurkan data, sehingga masalah keamanan menjadi salah satu aspek penting dari teknologi itu sendiri.

Dalam komunikasi data, terdapat sebuah metode pengamanan data yang dikenal dengan nama kriptografi. Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data, serta keaslian pengirim. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum seperti LAN atau *internet* tidak dapat diketahui atau dimanfaatkan oleh orang yang tidak berkepentingan atau yang tidak berhak menerimanya.

Dalam hal teknik pengamanan data, banyak metode kriptografi yang dapat digunakan. Metode-metode kriptografi tersebut mempunyai teknik dan cara

tersendiri. Langkah-langkah pengerjaan setiap metode pun berbeda-beda, baik dari segi panjang maupun kerumitan. Salah satu metode kriptografi yang akan diterapkan pada penulisan tugas akhir ini adalah metode RSA (Rivest-Shamir-Adleman).

Pada penulisan tugas akhir ini akan dilakukan perancangan dan pembangunan perangkat lunak untuk komunikasi data pada jaringan lokal dan penerapan sistem keamanan dengan teknik kriptografi algoritma RSA pada perangkat lunak tersebut, dan lebih menitik beratkan pada keamanan data waktu dikirim dan waktu diterima pada jaringan komputer.

Berdasarkan uraian diatas, penulis bermaksud untuk mengambil tugas akhir (skripsi) dengan judul **"PERANCANGAN DAN PENERAPAN SISTEM KEAMANAN PADA PERANGKAT LUNAK KOMDAT LAN MENGGUNAKAN KRIPTOGRAFI DENGAN ALGORITMA RSA".**

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah yang diuraikan, dapat diidentifikasikan masalahnya, yaitu bagaimana membangun suatu perangkat lunak untuk komunikasi data pada jaringan komputer dan menerapkan teknik enkripsi-dekripsi dengan menggunakan kriptografi algoritma RSA pada perangkat lunak yang dibangun untuk menjaga keamanan data baik waktu dikirim ataupun waktu diterima.

1.3 Maksud dan Tujuan

Maksud penyusunan tugas akhir ini adalah untuk merancang suatu perangkat lunak untuk keamanan data dengan menggunakan kriptografi algoritma RSA.

Tujuan dari penyusunan tugas akhir ini yaitu :

1. Untuk merancang dan membangun sebuah perangkat lunak untuk melakukan komunikasi data pada jaringan komputer lokal.
2. Menerapkan teknik kriptografi algoritma RSA pada perangkat lunak yang dibangun untuk menjaga keamanan data dengan cara melakukan enkripsi pada data yang akan dikrim dan dekripsi pada data yang diterima baik berupa data teks ataupun *file*.

1.4 Batasan Masalah

Karena keterbatasan waktu dan pengetahuan penulis, maka ruang lingkup permasalahan dalam penulisan tugas akhir ini dibatasi pada bidang kajian yang akan dibahas yaitu :

1. Data yang akan dienkripsi hanya menangani teks dan *file* teks.
2. Algoritma Kriptografi yang digunakan adalah RSA (Rivest-Shamir-Adleman).
3. Permasalahan lebih dititik beratkan pada keamanan data saat dikirim dan diterima.

4. Panjang kunci yang digunakan 64 Bit.

5. Perangkat lunak ini dibangun pada perangkat komputer berbasiskan sistem operasi Windows XP Profesional.

6. Perangkat lunak dibangun menggunakan MS Visual Basic 6.0 yang berfungsi sebagai tempat penulisan *script* yang digunakan.

1.5 Metodologi Penelitian

Metodologi Penelitian merupakan tahapan-tahapan yang dilalui oleh peneliti mulai dari perumusan masalah sampai kesimpulan. Dalam penyelesaian Tugas Akhir ini, penulis menggunakan beberapa metode penelitian, antara lain :

1.5.1 Metode Penelitian

Metode Penelitian merupakan cara-cara atau teknik dalam melakukan suatu penelitian. Dalam pembuatan tugas akhir ini, penulis menggunakan metode penelitian *Eksperimental* yang berarti peneliti mengadakan kegiatan percobaan untuk melihat sesuatu hasil.

1.5.2 Metode Pengumpulan Data

Dalam penyusunan tugas akhir ini penulis menggunakan metode dan langkah pengumpulan data sebagai berikut :

a. Studi Literatur.

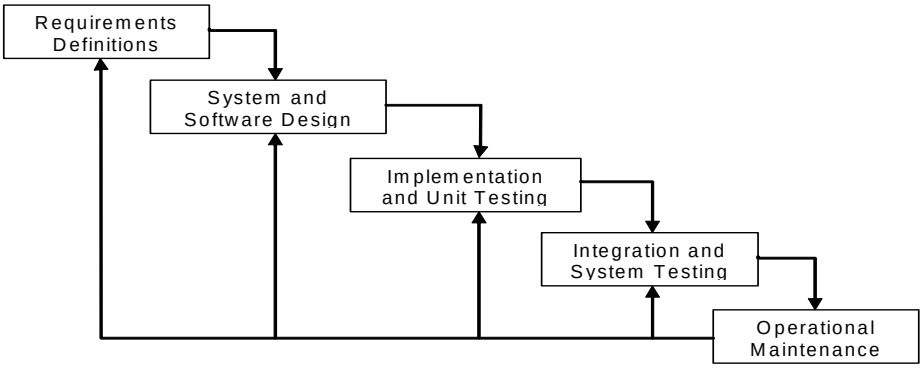
Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan metode kriptografi RSA.

b. Observasi.

Teknik pengumpulan data dengan mengadakan penelitian dan peninjauan langsung terhadap masalah yang diambil.

1.5.3 Metode Pembuatan Perangkat Lunak.

Teknik analisis data dalam pembuatan perangkat lunak menggunakan paradigma perangkat lunak secara *waterfall*, yang meliputi beberapa proses diantaranya :



Gambar 1.1 Diagram Alir Secara *Waterfall*

1. *Requirements Definitions*

   Maksudnya adalah untuk mengidentifikasikan masalah, menentukan penyebabnya, dan garis besar strategi untuk pemecahannya.

2. *System and Software Design*

   Perancangan program aplikasi merupakan upaya untuk membangun desain sistem yang akan dibuat. Perancangan program aplikasi meliputi perancangan desain *input* dan *output* serta merancang menu program yang akan berfungsi untuk memudahkan pengguna untuk menjalankan sistem yang akan dibangun.

3. *Implementation and Unit Testing*

   Hasil langkah ketiga adalah melakukan simulasi yang tengah dirancang pada langkah sebelumnya. Dengan melakukan simulasi dapat diketahui berfungsi atau tidaknya suatu sistem yang dibangun. Hasil dari simulasi ini akan dilakukan pada langkah kelima yaitu dengan melakukan pengujian validasi pada sistem tersebut.

4. *Integration and System Testing*

   Hasil rancangan yang telah dibuat selanjutnya divalidasi, yang meliputi kegiatan konfirmasi dan konsultasi kepada dosen pembimbing. Selain itu tahap validasi ini dilakukan pengujian terhadap hasil rancangan dengan menguji cobakan data. Bila hasil rancangan ini dianggap belum valid, maka rancangan perlu diperbaiki atau dilengkapi.

5. *Operational Maintenance*

   Pada langkah ini, akan dicoba hasil yang telah siap dioperasikan.

1.6 Sistematika Penulisan

Untuk mempermudah penulisan, maka penyusunan skripsi ini dibagi kedalam V (lima) bab, yaitu sebagai berikut :

BAB I. PENDAHULUAN

Bagian ini menguraikan tentang latar belakang masalah, identifikasi masalah, batasan masalah, maksud dan tujuan penelitian, metode pengumpulan data serta sistematika penulisan.

BAB II. LANDASAN TEORI

Bagian ini membahas tentang hal-hal yang berkaitan dengan kriptograpi, enkripsi dan dekripsi.

BAB III. ANALISIS DAN PERENCANAAN

Bagian ini menganalisis masalah dari model penelitian untuk memperlihatkan keterkaitan antar variabel yang diteliti secara model matematis untuk analisisnya.

BAB IV. IMPLEMENTASI DAN PENGUJIAN

Bagian ini merupakan tahapan yang dilakukan dalam penelitian secara garis besar sejak dari tahap persiapan sampai penarikan kesimpulan, metode dan kaidah yang diterapkan dalam penelitian. Termasuk menentukan variabel penelitian, identifikasi data yang diperlukan dan cara pengumpulannya, penentuan contoh penelitian dan teknik pengambilannya, serta metode/teknik analisis yang akan dipergunakan dan perangkat lunak yang akan dibangun jika ada.

BAB V. KESIMPULAN DAN SARAN

Bagian ini berisi kesimpulan dan saran yang sudah diperoleh dari pembahasan bagian sebelumnya.