BAB III

ANALISIS KEBUTUHAN PERANGKAT LUNAK

3.1 Kebutuhan Analisis

Analisis sistem (system analysis) dapat didefinisikan sebagai penguraian dari suatu sistem informasi yang utuh kedalam komponennya untuk mengidentifikasi dan mengevaluasi permaslahan – permasalahan, kesempatan-kesempatan, hambatan-hambatan yang terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya[JOG99].

Tahap analisis merupakan tahap yang paling penting, karena kesalahan didalam tahap ini akan menyebabkan juga kesalahan pada tahap selanjutnya. Oleh karena itu dibutuhkan suatu metode yang dapat digunakan sebagai pedoman dalam pengembangan suatu sistem. Adapun analisis yang diapakai adalah

a. Kebutuhan masukan (input)
b. Kebutuhan keluaran (output)
c. Kebutuhan perangkat lunak
d. Kebutuhan perangkat keras

3.2 Metode Analisis

Metode yang dipakai untuk menganalisis kebutuhan untuk mendukung rancang bangun implementasi kriptografi algoritma RSA adalah dengan metode analisis terstruktur (*Stuctured Approach*), yang menggambarkan secara menyeluruh target dan kebutuhan sistem yang diperlukan, sehingga hasil dari

analisis akan menghasilkan analisis dari kebutuhan sistem yang terstruktur dan dapat didefinisikan dengan baik dan jelas.

3.3 Langkah-langkah Analsis Sistem

Didalam tahap analisis sistem terdapat langkah-langkah dasar yang harus dilakukan dalam menganalisis sistem, yaitu:

a. *Identfy*, yaitu mengidetifikasi masalah. Mengidentifikasi masalah merupakan langkah pertama yang dilakukan dalam tahap analsis sistem. Masalah dapat didefinisikan sebagai suatu pernyataan yang diinginkan untuk dipecahkan
b. *Understand*, yaitu memahami kerja dari sistem yang ada. Langkah ini dapat dialkukan dengan mempelajari secara terperinci bagaimana sistem yang ada beroperasi.
c. *Analyze*, yaitu menganalisa sistem. Langkah ini dilakukan berdasarkan data yang diperoleh.
d. *Report*, yaitu membuat laporan. Setelah analisis sistem ini selesai dilakukan, tugas berikutnya dari analisis sistem dan timnya adalah membuat laporan hasil analis.

3.4 Hasil Analisis

Setelah dilakukan analisis, dapat diketahui apa yang menjadi masukan, keluaran, kinerja yang diharapkan, fungsi-fungsi yang diperlukan serta antarmuka untuk memudahkan user dalam menggunakan sistem yang dibuat.

3.4.1 Analsis Masukan

Input yang dibutuhkan untuk mengimplementasikan enkripsi ini adalah dokumen elektronik (semua file yang tersimpan di disk) dan file teks yang nantinya akan dienkripsi menjadi file berekstensi *.enc dan file teks yang tidak terbaca/disamarkan (tidak sesuai dengan aslinya).

3.4.2 Analisis Keluaran

Output atau keluaran yang diharapkan dari enkripsi ini adalah data atau file yang berubah dari data asalnya sehingga sudah tidak dapat dipahami lagi. Untuk dapat memahami lagi data yang ada dibutuhkan proses dekripsi yang akan menghasilkan keluaran data sama persis dengan data sebelum dienkripsi. Adapaun data hasil enkripsi nantinya akan berektensi *.enc

3.4.3 Analisis Antarmuka

Antarmuka (*interface*) dirancang agar pengguna dapat berinteraksi secara baik dengan dengan sistem yang dibangun, sehingga tercipta komunikasi yang mudah dipahami. Komunikasi tersebut dapat terdiri dari proses memasukan data, dan menampilkan kepada pengguna. Untuk tercapainya antarmuka yang diinginkan, ada beberapa hal yang perlu menjadi pedoman, yaitu:

1. Aplikasi harus menyediakan perintah-perintah apa yang harus dikerjakan oleh pengguna.
2. Layar dialog harus dibikin sedemikian rupa sehingga informasi, perintah, dan bantuan-bantuan selalu ditampilkan pada area yang sudah pasti. Dengan demikian pengguna akan dapat dengan mudah mencari informasi yang

diinginkan. Untuk itu layar dialog dibagi menjadi jendela-jendela yang sesuai dengan kegunaannya masing-masing.

3. Menggunakan kata-kata yang mudah dimengerti untuk dialog.
4. Hindari mnggunakan singkatan-singkatan kata.
5. Hindari menggunakan simbol-simbol yang tidak dimengerti.
6. Menggunakan kata-kata yang tetap untuk maksud dan fungsi yang sama.

Pada dasarnya rancangan antarmuka yang dibuat bagi pengguna sedapat mungkin mengakibatkan pengguna tahu apa yang harus dilakukan dengan melihat antarmuka aplikasi tersebut.

3.4.4 Analisis Fungsi

1. Pembangkitan kunci

   Merupakan proses pemilihan bilangan prima secara acak kemudian melalui perhitungan akan dihasilkan dua buah kunci yaitu kunci publik dan kunci privat.

2. Enkripsi

   Merupakan proses penguraian dari data yang dapat dipahami *(plain text)* menjadi data yang tidak dapat diapahami *(chipper text)*.

3. Dekripsi

   Merupakan proses mengebalikan data hasil enkripsi yang tidak dapat dipahami (*chipper text*) menjadi data yang dapat dipahami (*plain text*).

3.4.5 Kebutuhan Perangkat Lunak

Untuk membuat sistem aplikasi ini diperlukan Software untuk membuat aplikasi program RSA adalah sebagai berikut:

- Sistem operasi Windows Xp.
- Visual Borland Delphi 7
- Microsoft FrontPage
- Adobe Photoshop 7