BAB I
PENDAHULUAN

1.1. Latar Belakang

Saat ini data dan informasi menjadi suatu hal yang tidak dapat dipisahkan lagi dari setiap aspek kehidupan. Data merupakan sebuah bahan baku untuk menghasilkan sebuah informasi. saat ini masyarakat kita disebut sebagai *information-based sociaty* yang artinya bahwa dunia sudah terlibat dalam hal pengumpulan, pertukaran, pembuatan dan pengaksesan informasi.

Sebagian besar kalangan terbiasa dengan aplikasi *Microsoft Office* yang sangat memudahkan siapa saja dalam melakukan pengolahan data. Pengolah kata *Microsoft Word* begitu mudah digunakan sehingga siapapun yang menggunkaannya akan merasa nyaman dengan pengolahan kata ini. Pengolahan kata disimpan sebagai *file Microsoft Word*.

Kemajuan sisi teknologi komputer dan telekomunikasi bagaikan pisau bermata dua. Disatu sisi kita dimudahkan dengan adanya teknologi itu, namun disisi lain aspek kejahatan dengan menggunakan teknologi ini juga semakin meningkat. Sebagai contoh banyak informasi atau data milik perusahaan yang hanya boleh diketahui oleh orang-orang tertentu dalam perusahaan untuk itu keamanan data yang digunakan harus terjamin dalam batasan tertentu.

Adanya potensi tindakan peretasan jaringan maupun pengambilan user account dapat mengakibatkan terjadinya kerawanan kerahasiaan suatu data atau dokumen sehingga diperlukan suatu aplikasi yang dapat mengamankan data, khususnya untuk *shared document* pada jaringan komputer lokal agar dokumen atau data tersebut hanya dapat dibaca oleh orang yang berhak.

Algoritma RSA merupakan salah satu teknik mengamankan data dengan cara mencocokkan kunci publik yang dimiliki pengirim dokumen dan penerima dokumen, yang selanjutnya dilakukan proses penguraian dengan sebuah kunci privat (pribadi). Teknik ini sangat membantu proses pengamanan data, karena hanya orang yang mempunyai kunci privat saja yang dapat menguraikan isi file tersebut. Sama halnya dengan algoritma ElGamal yang merupakan salah satu

algoritma kriptografi kunci publik yang pada umumnya digunakan untuk digital signature yang kemudian bisa digunakan untuk melakukan enkripsi dan dekripsi.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka perumusan masalah dalam aplikasi pengamanan data dokumen word ini adalah

"Bagaimana membuat suatu aplikasi yang dapat mengenkripsi dan mendekripsi sebuah dokumen untuk menjaga keamanan dan kerahasiaan data?"

1.3. Tujuan Penelitian

Tujuan penelitian ini untuk meningkatkan keamanan dan kerahasiaan dokumen agar tidak dapat dibaca atau diketahui isinya oleh orang yang tidak berhak atau orang yang tidak diinginkan.

1.4. Batasan Masalah

Agar masalah tidak menyimpang dari tujuan awal yang telah direncanakan maka diperlukan suatu batasan masalah.

1. Metode enkripsi yang digunakan adalah algoritma RSA yang dilanjutkan dengan algoritma ElGamal. Dan metode yang digunakan untuk mendekripsi adalah algoritma ElGamal yang kemudian dilanjutkan dengan algoritma RSA.
2. Dokumen yang digunakan adalah dokumen microsoft word dengan format docx atau doc (microsoft word 97-2003)
3. Bekerja pada sistem operasi windows
4. Aplikasi dibangun menggunakan Visual Basic 6
5. Tidak membahas mengenai jaringan atau proses pengiriman data.

1.5. Metodelogi Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut :

1) Studi literatur

   Studi literatur yang dilakukan dengan cara membaca dan mempelajari beberapa sumber tertulis (makalah, jurnal, dan paper) yang berkaitan dengan proses enkripsi dan dekripsi.

2) Analisis sistem

   Analisis sistem dilakukan berdasarkan hasil observasi yang dilakukan peneliti.

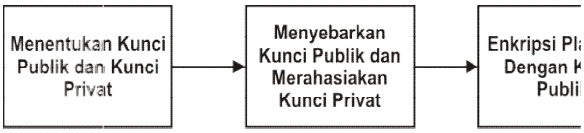
3) Perancangan sistem

   a. Input

      Memasukkan data yang menjadi penelitian.

   b. Proses

      Algoritma kriptografi asimetris *RSA* dan *ElGamal* akan membantu penyelesaian penelitian dengan menganalisis data yang diinputkan dan melakukan beberapa perhitungan untuk menentukan hasil analisis yang dijadikan penelitian. Gambar 1.1 menunjukkan proses-proses yang dilakukan dengan algoritma *RSA* dan *ElGamal*



Gambar 1.1 Diagram Blok Proses-Proses RSA dan ElGamal

   c. Output

      Peneliti akan memperoleh data yang terenkripsi maupun yang telah terdekripsi hasil dari algoritma *RSA* dan *ElGamal* untuk meningkatkan tingkat keamanan data.

d. Implementasi

Yaitu penerapan hasil perancangan sistem yang akan dibuat dalam bentuk aplikasi program yang selanjutnya akan dapat digunakan oleh pengguna.

4) Implementasi dan pengujian

Pengujian dimaksudkan untuk mengetahui sejauh mana kinerja sistem dalam mengelolah data sehingga mampu menghasilkan aplikasi yang sesuai dengan yang diharapkan.

5) Penyusunan laporan

Pembuatan laporan skripsi lengkap dengan analisis yang didapat

1.6. Sistematika Penulisan

Tugas akhir ini terdiri dari 5 (lima) bab, dimana masing-masing bab terdiri dari sub-sub bab yang menjelaskan isi dari bab-bab tersebut. Adapun sistematika penulisan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini menguraikan hal-hal yang berkaitan dengan masalah-masalah yang dihadapi, antara lain latar belakang, perumusan masalah, batasan masalah yang menjelaskan batasan dari aplikasi yang dibuat, tujuan yang diharapkan dari aplikasi dan konstribusi yang diperoleh dengan adanya aplikasi tersebut.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori-teori penunjang yang diharapkan dapat menjelaskan secara singkat mengenai teori yang berkaitan dengan permasalahan yang sedang dihadapi.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi tentang analisis, perancangan sistem dan perangkat yang digunakan

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Berisi tentang implementasi hasil pengujian program serta analisis terhadap kinerja program.

BAB V PENUTUP

Berisi tentang kesimpulan dari analisis pengujian dan beberapa saran yang bermanfaat dalam pengembangan program di waktu mendatang.

DAFTAR PUSTAKA.