BAB I

PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi saat ini dibuktikan dengan banyaknya inovasi yang telah dibuat dari yang rumit hingga sederhana menjadi salah satu penunjang kemajuan manusia, tidak terkecuali dengan kemajuan teknologi informasi dan komputer. Pada kurun waktu ini, komputer menjadi alat bantu paling utama untuk membantu manusia dalam pengerjaan sesuatu agar menjadi lebih cepat dan efisien. Pertukaran dokumen berbasis komputer seperti pesan *e-mail* atau dokumen dalam pesan *e-mail* di internet sudah luas digunakan sebagai transaksi komersiil. Dokumen sering berisi informasi penting seperti kontrak resmi, transaksi keuangan, *record* penjualan dan lain-lain. Keamanan dari suatu data merupakan hal yang perlu diperhatikan dalam menjaga kerahasiaan data terutama bagi dokumen yang isinya hanya boleh diketahui oleh pihak yang berhak saja. Pengiriman data atau dokumen tanpa dilakukan pengamanan akan beresiko terhadap penyadapan, kerahasiaan dan keotentikan data. Oleh karena itu diperlukan suatu sistem pengamanan data yang bertujuan untuk meningkatkan keamanan data, melindungi suatu data atau pesan agar tidak dibaca oleh pihak yang tidak berwenang, dan mencegah pihak yang tidak berwenang untuk menyisipkan, menghapus, ataupun merubah data.

Salah satu ilmu pengamanan data yang terkenal adalah kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna (Munir, 2006). Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau *plaintext* menjadi *ciphertext* (teks tersandi). Sedangkan dekripsi adalah proses penyandian kembali *ciphertext* menjadi *plaintext* (Munir, 2006). Untuk membangun sistem penyimpanan dokumen yang hasil simpanannya tidak dapat dibaca oleh orang, dalam penelitian ini telah dikembangkan model sistem pengamanan dengan proses enkripsi dan dekripsi dengan metode simetrik kriptosistem dan asimetrik kriptosistem. Gabungan algoritma simetrik kriptosistem dan asimetrik kriptosistem disebut sebagai *hybrid cryptosystem* (Fauziah, 2008).

Penggunaan *hybrid cryptosystem* dalam penelitian ini merupakan gabungan algoritma RC4, RSA dan MD5 yang digunakan dalam tiga tahapan pengamanan data pada dokumen. Adapun tahapan pengamanan data meliputi : proses *setup key*, proses enkripsi data, dan proses dekripsi data. Maka dari itu, pada penelitian ini penulis akan menggabungkan tiga algoritma sekaligus yaitu algoritma RC4 digunakan sebagai pengamanan data, RSA digunakan dengan alasan tingkat keamanannya sangat tinggi sebagai pengamanan kunci dan MD5 digunakan sebagai pengujian integritas sebuah berkas. .

Berdasarkan latar belakang diatas, maka penulis mencoba mengembangkan aplikasi desktop yang digunakan untuk pengamanan dokumen. Dengan adanya aplikasi ini, diharapkan dapat membantu dalam pengamanan

sebuah dokumen dengan cara enkripsi dan enkripsi. Untuk itu penulis membuat penelitian skripsi dengan judul "*Hybrid Cryptosystem* Untuk Pengamanan E-dokumen Menggunakan Algoritma RC4, RSA dan MD5".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan di atas, maka untuk mempermudah dalam penulisan karya tulis ini penulis merumuskan permasalahan sebagai berikut :

1. Bagaimana mengamankan sebuah dokumen yang bersifat rahasia dengan cara enkripsi dan dekripsi menggunakan *hybrid cryptosystem*?
2. Bagaimana Membangun aplikasi *hybrid cryptosystem* untuk pengamanan e-dokumen ?
3. Bagaimana mengetahui kinerja aplikasi pengamanan e-dokumen dengan menggunakan *hybrid cryptosystem* ?

1.3 Batasan Masalah

Pembatasan masalah digunakan untuk menspesifikasi arah tujuan penulis. Sehingga, penulis lebih jelas untuk meneliti dan menentukan metode atau cara yang tepat dan cepat untuk tercapainya tujuan penelitian yang dilakukan.

Berdasarkan pada penjelasan diatas, maka dalam hal ini untuk membatasi agar ranah penelitian tidak terlalu luas akan diberikan batasan sebagai berikut :

1. *Hybrid cryptosystem* yang digunakan adalah menggunakan algoritma RC4, RSA, dan MD5.
2. Panjang kunci RC4 maksimal 20 karakter.
3. Kunci publik dan kunci privat pada algoritma RSA berupa angka.
4. Nilai p, q dan e pada RSA bilangan prima.
5. Panjang kunci MD5 yang bisa dienkripsi dalam 16 *bytes* (32 karakter).
6. *Message* atau pesan yang dapat dienkripsi berupa teks dalam ekstensi docx.
7. Ukuran file yang dapat dienkripsi maksimal 5 MB.
8. Tidak membahas aspek keamanan pada jalur komunikasi yaitu pada proses transmisi e-dokumen lewat internet via *email*, keamanan yang bersifat fisik dan keamanan yang berhubungan dengan *personal*.
9. *Software* yang digunakan peneliti dalam membuat aplikasi ini yaitu NetBean 7.2 dan *java* sebagai bahasa pemrogramannya.

1.4 Tujuan Penelitian

Tujuan yang dicapai dalam penelitian ini adalah sebagai berikut :

1. Menghasilkan sebuah aplikasi yang digunakan untuk mengamankan sebuah e-dokumen sehingga menjadi solusi dalam pengamanan dokumen secara cepat dan aman.
2. Mengamankan sebuah dokumen agar tidak dibaca oleh pihak yang tidak berwenang.

3. Merancang dan membuat aplikasi kriptografi untuk mempermudah proses enkripsi dokumen dengan menggunakan algoritma yang unik.
4. Memperdalam ilmu mengenai keamanan dalam sebuah informasi.
5. Perancangan aplikasi ini juga sebagai alat pembelajaran untuk mengimplementasikan ilmu yang dipelajari selama studi di STMIK AMIKOM Yogyakarta.

1.5 Manfaat Penelitian

Manfaat yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Bagi Penulis

   Menerapkan dan mengembangkan ilmu serta teori-teori yang telah didapatkan selama studi sebagai persiapan pengaplikasian pada dunia kerja.

2. Bagi Perkembangan Ilmu Pengetahuan

   Penulis berharap aplikasi yang dirancang ini, dapat ikut andil dan menjadi pelopor diciptakannya aplikasi-aplikasi baru tentang pengamanan dokumen-dokumen yang sangat penting.

3. Bagi Masyarakat

   Sebagai referensi bagi pembaca yang ingin mengetahui langkah-langkah dari proses enkripsi dan dekripsi dokumen, dan berbagi wawasan dibidang ilmu kritografi.

1.6 Metodologi Penelitian

Langkah - langkah dalam melakukan penelitian yang berjudul "*Hybrid cryptosystem* untuk pengamanan e-dokumen menggunakan algoritma RC4, RSA dan MD5" ini adalah sebagai berikut :

1. Pengumpulan data
   a. Metode kepustakaan

      Metode pengumpulan data yang dilakukan dengan cara membaca, mempelajari, mencari bahkan menulis dari sebuah buku, artikel, jurnal ilmiah, majalah baik dari media cetak maupun media elektronik yang berkaitan dengan topik yang dibahas dalam pembuatan aplikasi.

   b. Metode observasi

      Metode ini adalah metode pengumpulan data yang dilaksanakan dengan mengadakan pengamatan langsung terhadap data-data yang akan diamankan.

2. Analisis data

   Melakukan analisis data yang telah dikumpulkan untuk penyusunan laporan kemudian merancang dan membuat aplikasi. Analisis data dalam penelitian meliputi :

   a. Analisis kebutuhan fungsional

      Merupakan pendefinisian fungsi sistem yang harus disediakan, bagaimana reaksi sistem terhadap input dan apa yang harus dilakukan sistem pada situasi khusus.

b. Analisis kebutuhan non fungsional

Menganalisis kebutuhan pendukung bagi sistem.

3. Perancangan aplikasi

Perancangan aplikasi meliputi perancangan antarmuka.

4. Implementasi aplikasi

Mengimplementasikan aplikasi yang telah dibuat.

5. Evaluasi aplikasi

Melakukan evaluasi terhadap aplikasi yang telah diimplementasikan.

1.7 Sistematika Penulisan

Sistematika penulisan disusun menggunakan dasar-dasar penulisan karya ilmiah. Sistematika penulisan laporan skripsi adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan yang digunakan dalam penyusunan skripsi.

BAB II LANDASAN TEORI

Bab landasan teori merupakan tinjauan pustaka, berisi dasar-dasar teori yang digunakan dalam penyusunan skripsi. Pada bab ini juga berisi tentang *software* / *tools* yang digunakan dalam pembuatan aplikasi.

BAB III ANALISIS DAN PERANCANGAN

Bab ini berisi tentang analisis terhadap kasus yang diteliti dan perancangan program yang akan dibuat.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini memaparkan hasil-hasil dari tahapan penelitian, mulai dari analisis, desain, implementasi desain, hasil testing dan implementasi.

BAB V PENUTUP

Bab ini menyajikan kesimpulan dari penelitian serta saran guna memperbaiki kelemahan dan kekurangan yang ada pada aplikasi.