BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi saat ini semakin cangkih dan telah memberikan kemudahan dalam penyampain informasi yang dapat dikirimkan melalui jaringan internet dengan menggunakan media komputer. perkembangan tersebut secara langsung maupun tidak langsung dapat mempengaruhi sistem keamanan data dan sistem informasi terutama di era internet semua komputer dapat tersaring dan informasi terkirim dengan bebas melalui keamanan yang relatif rendah untuk itulah peranan keaman data sangat di butuhkan.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan data dan merupakan salah satu teknik untuk melindungi data menggunkan kriptografi asimetri dengan menetukan kunci publik dan kunci privat. Dan kemudian melakukan pengubahan pesan biasa (plainteks) menjadi kode-kode tertentu disebut sebagai enkripsi dan hasilnya disebut chipertext , dan proses pengubahan kode-kode chipertext menjadi pesan semula plaintext disebut dekripsi

Dalam algoritma ini terdapat banyak metode yang dapat digunakan dalam kriptografi salah satunya adalah dengan metode Algoritma RSA yang di temukan oleh 3 (tiga) orang algoritmik yaitu (Ron Rivest-Adi Shamir-Leonard Adleman) dan RC2*CryptoServiceProvider* pada komponen .NET framework. Metode ini mengubah setiap karakter menjadi sekumpulan bilangan bulat dengan menggunakan kunci-kunci tertentu.

Keamanan pada komputer menjadi isu penting pada era teknologi informasi saat ini. Banyak kejahatan *cyber* yang ditulis dalam media massa (terutama yang ditulis dalam portal berita di internet). Sebuah informasi umumnya hanya ditujukan bagi segolongan individu atau komunitas tertentu.

Oleh karena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak yang tidak berkepentingan maka untuk mengatasi persoalan keamanan data penulis memberikan sebuah solusi dalam penulisan skripsi ini dengan judul "Implementasi enkripsi dan dekripsi data menggunakan metode algoritma RSA dan memanfaatkan RC2*CryptoServiceProvider* komponen .NET framework".

B. Rumusan Masalah

Berdasarkan latar belakang diatas secara umum dapat dirumuskan masalah yang akan di bahas dalam penulisan skripsi ini adalah :

1. Membuat sebuah perangkat lunak untuk mengenkripsi dan mendekripsikan data berbasis file *.txt, gambar (BMP atau JPG) dan file PDF.
2. Mengubah data tersebut menjadi kode-kode rahasia (plainteks) dan sebaliknya kode-kode rahasia tersebut (palinteks) di ubah ke bentuk data semula.
3. Melindungi kerahasian data dari pihak-pihak yang tidak berhak membaca atau merusak data menggunakan algoritma RSA dan RC2*CryptoServiceProvider* pada komponen .NET framework sehingga data tersebut dapat dijaga kerahasiaanya.

C. Batasan Masalah

Berdasarkan rumusan masalah diatas adapun batasan masalah dalam penulisan skripsi ini yaitu pada lingkup permasalahan hanya dibatasi pada penggunaan algoritma RSA sampai dengan 5 digit angka untuk pengolahan data berbasis file *.txt dan memanfaatkan *RC2CryptoServiceProvider* pada komponen .NET Framework 2.0 untuk pengolahan *file* gambar (BMP atau JPG) dan *file* PDF pada proses enkripsi dan dekripsi.

Program aplikasi ini berjalan pada sistem operasi Windows vista, perangkat lunak yang dikembangkan menggunakan program Visual Basic 2005 dan .NET Framework 2.0.

D. Tujuan Penelitian

Tujuan yang ingin dicapai dalam penulisan skripsi ini adalah:

1. Mengimplementasikan algoritma RSA ke dalam suatu perangkat lunak untuk mengamankan suatu data berbasis *.txt dengan menggunakan algoritma RSA dan *RC2CryptoServiceProvider* pada komponen .NET Framework 2.0 untuk *file* gambar dan *file* pdf.
2. Sebagai tinjauan enkripsi dan dekripsi yang sudah ada dengan algoritma enkripsi yang dibuat akan menjadi acuan dalam pembentukan ide logika dan algoritma yang dikembangkan.

E. Manfaat Penelitian

Manfaat yang diharapkan dalam penulisan skripsi ini adalah :

1. Manfaat teoritis

Secara teoritis manfaat yang diperoleh dari penulisan skripsi ini adalah dapat memahami proses enkripsi dan dekripsi menggunakan algoritma RSA dan *RC2CryptoServiceProvider*.

2. Manfaat praktis

Manfaat praktis dari hasil penulisan skripsi ini adalah dapat mengetahui betapa pentingnya mengamankan sebuah data dan mempermudah proses enkripsi dan dekripsi RSA menggunakan program komputer.

F. SISTEMATIKA PENULISAN

BAB I : PENDAHULUAN

Bab ini akan menguraikan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II : TINJUAN PUSTAKA DAN DASAR TEORI

Bab ini akan diuraikan mengenai pengenalan sistem secara umum yaitu perangkat lunak atau software yang digunakan dalam pembuatan program skripsi ini.

BAB III : ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan membahas gambaran umum tentang analisis kebutuhan sistem dan perancangan sistem yang termasuk diagram alir data, flowchart dan rancangan form manual.

BAB IV : STRUKTUR, UJI COBA, PEMBAHASAN DAN PETUNJUK PENGGUNAAN PERANGKAT LUNAK

Bab ini berisi tentang struktur aplikasi, uji coba, pembahasan fungsi-fungsi pengopersian rancangan sistem yang di usulkan dan petunjuk penggunaan perangkat lunak.

BAB V : PENUTUP

Bab ini merupakan penutup yang terdiri atas kesimpulan dan saran-saran dari perangkat lunak yang di buat.