BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era globalisasi ini data atau informasi menjadi hal yang penting dan dibutuhkan oleh masyarakat. Kemapuan untuk menjaga kerahasiaan data atau informasi menjadi hal yang penting bagi sebuah organisasi, baik yang berupa perusahaan, perguruan tinggi, lembaga pemerintah atau lembaga – lembaga yang lainnya.

Keamanan merupakan kebutuhan umum pada jaringan komputer yang harus dipenuhi untuk kerahasiaan data. Keamanan jaringan komputer membutuhkan penanganan yang sangat besar, maka dari itu dibutuhkan sebuah mekanisme sistem keamanan yang dapat menangani masalah kerahasiaan sebuah data atau informasi. Untuk menjaga atas keamanan dan kerahasiaan sebuah data atau informasi dalam suatu jaringan komputer maka diperlukan metode enkripsi guna untuk membuat kerahasiaan data atau informasi.

Metode enkripsi adalah proses mengacak data atau informasi sehingga tidak dapat dibaca oleh pihak lain atau pihak yang tidak berhak menerima, kecuali untuk pihak yang berhak menerima serta dengan adanya metode enkripsi ini diharapkan dapat mencegah campur tangan dari orang – orang yang tidak berhak menghapus data atau informasi yang telah diterima. Informasi ini dibagi menjadi dua yakni informasi yang bersifat pribadi dan informasi yang bersifat umum. Informasi yang bersifat umum adalah informasi yang boleh diketahui oleh orang banyak atau sifatnya umum. Alur dari proses pengiriman sebuah data atau informasi tidak luput dari gangguan – gangguan dari pihak yang tidak berhak. Salah satu teknik untuk menjaga kerahasiaan data atau informasi adalah dengan menggunakan algoritma kriptografi.

Algorima kriptografi terdiri dari algoritma enkripsi dan algoritma deskripsi. Enkripsi adalah proses penguraian atau pengacakan informasi atau data agar tidak dapat dibaca, dilihat serta dimanipulasi atau dirubah. Sedangkan deskripsi adalah proses pengembalian dari proses pengacakan ke bentuk yang semula atau bentuk asal sebelum melakukan enkripsi. Ada beberapa model dari metode enkripsi ini salah satu diantaranya adalah algoritma RSA. RSA adalah singkatan dari nama para penemunya, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. RSA adalah salah satu algoritma penyandian yang paling banyak mengundang kontroversi, Sejauh ini belum seorang pun yang berhasil menemukan lubang sekuriti pada RSA, tetapi tak seorang pun juga yang berhasil memberikan pembuktian ilmiah yang memuaskan dari keamanan teknik sandi ini.

Enkripsi dapat diterapkan dengan berbagai algoritma. Secara umum algoritma enkripsi dapat dibagi menjadi dua golongan yaitu algoritma kunci umum (*public key algorithm*) dan algoritma kunci rahasia (*private key algorithm*), dimana kedua kunci tersebut memiliki kelebihan dan kekurangan.

Untuk menyandi informasi dan untuk menterjemahkan pesan tersandi sebuah algoritma penyandian memerlukan sebuah data biner yang disebut kunci. Tanpa kunci yang cocok orang tidak bisa mendapatkan kembali pesan asli dari pesan tersandi. RSA yang menggunakan algoritma asimetrik mempunyai dua kunci yang berbeda, disebut pasangan kunci (*key pair*) untuk proses enkripsi dan dekripsi. Kunci-kunci yang ada pada pasangan kunci mempunyai hubungan secara matematis, tetapi tidak dapat dilihat secara komputasi untuk mendeduksi kunci yang satu ke pasangannya. Algoritma ini disebut kunci publik, karena kunci enkripsi dapat disebarkan. Orang-orang dapat

menggunakan kunci publik ini, tapi hanya orang yang mempunyai kunci privat sajalah yang bisa mendekripsi data tersebut.

Telah banyak terdapat program – program yang mengimplementasikan kriptografi dengan berbagai algoritma dan menggunakan berbagai macam bahasa pemprograman, namun penulis belum melihat ada yang menggunakan algoritma RSA dalam bahasa pemprograman C#.NET. Hal inilah yang menjadi latar belakang penulis dalam penulisan skripsi ini penulis mengangkat judul "PEMBUATAN APLIKASI ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA KRIPTOGRAFI RSA MENGGUNAKAN C#.NET".

1.2 Perumusan Masalah

Dapat dirumuskan masalah yang ada adalah, sebagai berikut :

a. Sejauh mana proses kinerja dari algoritma *RSA* dalam melakukan enkripsi dan deskripsi sebuah informasi atau data.
b. Bagaimana cara melakukan pengamanan data atau informasi dengan menggunakan algoritma *RSA* ?
c. Bagaimana aplikasi enkripsi dapat memberikan perlindungan pada sebuah informasi atau data ?

1.3 Pembatasan Masalah

Pada penulisan ini dilakukan pembatasan masalah, yaitu :

a. Pembuatan aplikasi enkripsi menggunakan visual C #.NET.
b. Algoritma yang digunakan adalah algoritma *RSA*.
c. Merancang aplikasi dengan menggunakan algoritma *RSA* sebagai proses enkripsi dan deskripsi pesan atau informasi.
d. Enkripsi di implementasikan hanya pada penyandian pesan atau informasi hanya berupa teks atau tulisan pada file extensi (*.txt).
e. Aplikasi hanya berjalan pada sistem operasi windows.

1.4 Tujuan dan Manfaat

Tujuan :

a. Memberikan gambaran dalam proses enkripsi dan deskripsi pesan atau informasi secara detail.
b. Perencanaan pengimplementasian aplikasi algoritma *RSA* untuk melakukan proses enkripsi dan dekripsi pesan atau informasi.
c. Memberikan penjelasan tentang konsep kriptografi.
d. Membuat enkripsi dengan menggunakan algoritma tertentu untuk melindungi pesan atau informasi agar tidak diketahui oleh orang yang tidak berhak.
e. Menjadi jawaban atas permasalahan keamanan pesan atau informasi saat ini.

Manfaat :

a. Pesan atau informasi lebih aman dan terjaga kerahasiaannya.
b. Menjaga pesan atau informasi agar tidak dapat dimanipulasi atau dirubah, dihapus.
c. Memahami kegunaan dari enkripsi.
d. Dengan adanya enkripsi diharapkan menghindari penyalahgunaan oleh orang – orang yang tidak mempunyai hak akses.
e. Meningkatkan keamanan terhadap pesan atau informasi yang dianggap penting.

1.5 Metode Penelitian

Metode penyusunan laporan Tugas Akhir ini adalah sebagai berikut:

a. Literatur

Metode ini digunakan untuk mengumpulkan data teoritis dari sumber tertulis yang menguraikan dan menjelaskan konsep - konsep yang terkait dengan judul penelitian yang telah dilakukan.

b. Cara Kerja Algoritma RSA

Cara kerja algoritma RSA ini dilakukan dengan cara membangkitkan kedua kunci untuk melakukan proses penyandian data atau informasi. Tingkat keamanan penyandian algoritma RSA sangat bergantung pada ukuran kunci tersebut, karena makin besar ukuran kunci, maka makin besar kemungkinan kombinasi kunci yang bisa dijebol dengan metode pengacakan kombinasi satu per satu kunci atau yang lebih dikenal dengan istilah brute force attack. Jika dibuat suatu sandi RSA memiliki panjang kunci 256 bit, maka metode brute force attack akan menjadi tidak berguna dan sia – sia bagi para hacker untuk menjebol sandi tersebut.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini dibagi menjadi:

BAB I PENDAHULUAN

Membahas latar belakang, tujuan dan manfaat, perumusan masalah, identifikasi masalah, ruang linkup masalah, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Memuat kerangka teori dan tinjauan pustaka.Kerangka teori menjelaskan mengenai kerangka teoritis yang mendasari penelitian. Tinjauan pustaka berisi beberapa referensi dari hasil penelitian yang relevan dengan topik tugas akhir yang disajikan, yang diperoleh dari berbagai sumber.

BAB III METODE PENELITIAN

Bab ini mengemukakan tentang cara dan prosedur dalam melakukan penelitian.

BAB IV ANALISIS DAN PEMBAHASAN

Secara umum bab ini pembuatan program, mulai dari gambaran umum, rancangan tampilan program, langkah – langkah dalam pembuatan program.

BAB V KESIMPULAN DAN SARAN

Kesimpulan mengemukakan secara singkat hasil penting yang diperoleh dari penelitian sesuai dengan masalah dan tujuan penelitian. Saran merupakan sumbangan pemikiran peneliti berupa rekomendasi yang diambil dari hasil analisis dan pembahasan serta kesimpulan.