BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Dalam hal ini, sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi tidak berguna lagi apabila ditengah jalan informasi tersebut disadap atau dibajak oleh orang yang tidak berhak. Sebab, kalau hal ini sampai terjadi kemungkinan data yang dikirim bisa rusak, tercuri, terubah dan bahkan hilang sehingga ditak lagi bernilai informasi.

Keamanan dan kerahasiaan data sangat diperlukan baik dalam suatu organisasi maupun pribadi. Apalagi kalau data tersebut berada dalam suatu sistem komputer yang terhubung dalam jaringan komputer, atau dalam jaringan internasional yang sering disebut internet.

Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankkan dan sistem-sistem setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep *open*

system-nya sehingga siapapun, dimanapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.

Pada garis besarnya, masalah keamanan data dapat dibagi menjadi empat bidang yang saling berhubungan: kerahasiaan, keaslian, pengakuan dan kontrol integritas. Kearahasiaan harus dilakukan dengan menjauhkan informasi dari orang-orang yang tidak behak. Hal ini merupakan sesuatu yang harus diperhatikan ketika orang membahas keamanan data komputer. Keaslian berkaitan dengan siapa anda berbicara sebelum memberikan informasi yang sangat penting. Pengakuan berkaitan dengan dengan tanda tangan digital atau sertifikat digital sedangkan kontrol integritas adalah terkait dengan kontrol terhadap perubahan informasi.

Untuk menjaga keamanan dan kerahasiaan data dalam suatu sistem komputer, maka diperlukan metode enkripsi guna membuat data agar tidak dapat dibaca atau dimengerti oleh orang yang tidak berkepentingan. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak dapat dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau *cipher*. Sebuah sistem pengkodean menggunakan suatu table atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau yang merupakan bagian dari informasi yang dikirim. Sebuah cipher menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (*stream*) bit dari sebuah pesan menjadi *cryptogram* yang tidak dimengerti (*unintelligible*). Karena teknik cipher merupakan suatu sistem yang telah siap di

automasi, maka teknik ini digunakan dalam sistem keamanan komputer dan jaringan.

Pada sistem kriptografi digital pada saat int dikenal dua metode, yaitu konvensional dan kunci publik. Pada sistem kriptografi konvensional, proses untuk mengubah bentuk *plaintext* ke bentuk *ciphertext* dan proses kebalikannya memerlukan sebuah kunci yang sama, yang mutlak harus dijaga kerahasiannya. Pada sistem kriptografi kunci publik untuk proses tersebut diperlukan dua buah kunci, yaitu satu kunci untuk enkripsi data yang tidak dirahasiakan (disebut kunci publik) , dan satu kunci lagi untuk dekripsi data yang harus dijaga kerahasiaannya (disebut kunci privat).

Dalam pengamanan data, banyak sekali algoritma atau metode yang dapat digunakan, baik itu yang konvensional seperti DES, Blowfish, Twofish dan lain sebagainya, maupun yang berupa kunci publik atau yang sering disebut sebagai kriptografi asimetris seperti RSA, LUC, ECC dan lain sebagainya. RSA sebagai salah satu dari metode kriptografi asimetris adalah salah satu dari sekian banyak metode yang menjadi standar dalam keamanan data.

1.2 Rumusan Masalah

Dari latar belakang masalah diatas dapat diambil suatu perumusan masalah sebagai berikut:

a. Bagaimana menjelaskan konsep kriptograpfi.
b. Bagaimana menjelaskan konsep algoritma RSA
c. Bagaimana mengimplementasikan algoritma RSA untuk penyandian data.
d. Bagaimana mengetahui kinerja dan tingkat keamanan algoritma RSA.

1.3 Batasan Masalah

Adapun batasan masalah dalam pembahasan ini adalah:

a. Algoritma kriptografi yang akan dibahas adalah alagoritma RSA. Untuk aplikasinya menggunakan tool bahasa pemrograman Borland Delphi 7.
b. Penentuan bilangan prima dalam pembangkitan kunci adalah bilangan prima yang lebih kecil dari 100000
c. Aplikasi yang dibuat tidak dikombinasikan dengan program kompresi file

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

a. Memahami algoritma RSA dalam melakukan enkripsi/dekripsi.
b. Mengimplementasikan algoritma RSA untuk ekripsi dan dekripsi data.
c. Mengetahui kinerja dari algoritma RSA sebagai algoritma kriptografi.

1.5 Manfaat Penelitian

Adapaun manfaat dari penelitian ini adalah:

a. Aplikasi yang dibuat nantinya dapat digunakan oleh pengguna komputer yang akan mengirimkan data/pesan yang membutuhkan keamanan terhadap data yang dikirim sehingga data/pesan yang dikirim tidak disalah gunakan oleh pihak-pihak yang tidak berhak
b. Memberikan masukan kepada pengguna komputer agar memahami petingnya software kriptografi untuk pengamanan data.
c. Mengenalkan algoritma RSA kepada pengguna komputer.
d. Dapat mengetahui kinerja algoritma RSA dalam penyandian data.

1.6 Metode Penelitian

Dalam metode penelitian ini ada dua tahapan yang digunakan untuk penulisan tugas akhir, yaitu:

1.6.1 Pengumpulan Data

Metode pengumpulan data adalah metode yang digunakan untuk mengumpulkan data yang diperlukan dalam penelitian. Metode ini meliputi studi pustaka, yaitu pengumpulan data dengan cara melakukan studi, analisis dan dokumentasi literatur, serta sumber catatan lain yang berkaitan dengan permasalahan yang dibahas.

1.6.2 Pembuatan Sistem

Metode pembuatan sistem disusun berdasarkan hasil dari data yang sudah diperoleh. Metode ini meliputi:

a. Analisis sistem

   Analisa ini dilakukan untuk mengolah data yang sudah didapat dan mengelompokkan data sesuai dengan kebutuhan perancangan.

b. Perancangan sistem

   Tahap ini mendefinisikan kebutuhan yang ada, menggambarkan bagaimana sistem dibentuk dan persiapan untuk membangun aplikasi. Ada tiga atribut yang penting dalam proses perancangan , yaitu struktur data, arsitektur perangkat lunak dan prosedur rinci.

c. Implementasi sistem

Tahap ini adalah penerjemahan rancangan dalam tahap desain kedalam bahasa pemrograman komputer yang telah ditentukan sebelumnya.

d. Pengujian perangkat lunak

Tahap ini dilakukan untuk mengetahui bagaimana jalannya sistem apakah sudah berjalan dengan normal atau tidak dan bagaimana kinerjanya.

1.7 Sistematika Penulisan

Untuk memudahkan dalam memahami laporan tugas akhir, dikemukakan sistematika penulisan agar menjadi satu kesatuan yang utuh. Adapun penulisan laporan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sisitematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini memuat tentang teori-teori yang berhubungan dengan penelitian tugas akhir, antara lain keonsep kriptografi, model-model enkripsi, konsep algoritma RSA.

BAB III ANALISIS KEBUTUHAN SISTEM

Pada bab ini membahas sistem yag diterapkan, analisis masalah, masalah yang timbul, analisis sistem dan hasil analisis.

BAB IV PERANCANGAN SISTEM

Pada bab ini membahas tentang metode perancangan sistem yang memuat metode analisis perancangan sistem, desain sistem, juga memuat hasil perancangan yang dihasilkan perancangan sistem.

BAB V IMPLEMENTASI

Pada bab ini membahas batasan implementasi perangkat lunak dan dokumentasi implementasi perangkat lunak secara umum, bahasa yang digunakan dan implementasi antarmuka.

BAB VI ANALISIS KINERJA PERANGKAT LUNAK

Pada bab ini membahas kinerja dari perangkat lunak yang dibuat, yaitu penanganan kesalahan, analisis pembangkitan kunci, analisis input dan output, analisis perbandingan. Analisis algoritma RSA serta ananlisis tingkat keamanan.

BAB VII PENUTUP

Bab ini berisi kesimpulan dan saran.