BAB I. PENDAHULUAN

1.1 Latar Belakang

Di zaman modern seperti sekarang, perkembangan teknologi sangat berpengaruh besar terhadap segala aspek kehidupan. Banyak sekali manfaat dan kemudahan yang didapat dengan adanya teknologi yang terus berkembang, salah satunya di bidang informasi dan komunikasi. Dengan adanya internet, perkembangan teknologi informasi yang pesat menyebabkan akses informasi yang mudah dan cepat. Kemudahan dalam mengakses informasi inilah yang kemudian menuntut pemilik informasi untuk dapat menjaga data-data atau informasi penting dan rahasia agar tidak mudah diketahui oleh pihak lain yang tidak memiliki kewenangan sehingga dapat mencegah terjadinya penyalahgunaan informasi atau data-data tersebut.

Namun, hal tersebut juga memiliki dampak buruk karena rawan terjadi pencurian data. Hal ini tentu akan merugikan banyak pihak, terutama bagi perusahaan salah satunya perusahaan perseroan Telekomunikasi Indonesia di Bojonegoro yaitu Telkom Bojonegoro yang memiliki dokumen rahasia. Oleh karena itu, keamanan informasi merupakan faktor penting yang harus dipenuhi. Berbagai cara telah dilakukan untuk mengamankan informasi rahasia tersebut. Salah satu cara yang ditempuh adalah dengan mengubah informasi tersebut menjadi sandi-sandi yang sulit dibaca dan hanya bisa dibaca oleh pihak tertentu, metode ini disebut kriptografi.

Kriptografi merupakan studi matematis yang terkait dengan aspek-aspek yang berhubungan dengan keamanan informasi seperti menyembunyikan isi data, mencegah data dapat dirubah tanpa terdeteksi, 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). ataupun mencegah data digunakan tanpa otoritas yang cukup. Kriptografi dilakukan untuk menyembunyikan konten dari suatu informasi dengan mengubah informasi tersebut menjadi sandi dengan menggunakan kunci, dan untuk membacanya diperlukan kunci pula. Berdasarkan kerahasiaan kuncinya, algoritma dari kriptografi dapat dibedakan menjadi algoitma sandi kunci rahasia (*private key*) dan algoritma sandi kunci publik (*public key*). Pembuatan kunci tersebut dilakukan dengan memilih bilangan prima acak yang besar. Berdasarkan uraian di atas, penulis tertarik untuk mengkaji lebih lanjut algoritma kriptografi RSA (*Rivest-Shamir-Adleman*).

Oleh karena itu, penulis mengambil judul "Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro untuk Meningkatkan Keamanan Sistem Jaringan" yang dirancang dan diimplementasikan untuk membangun sistem yang dapat mengirim *file* data penting secara aman melalui jaringan *public* khususnya pada Telkom Bojonegoro yang bebas dari jangkauan orang-orang yang tidak berhak. Baik bebas jangkauan secara fisik maupun secara sistem sehingga amat sulit untuk ditembus oleh *hacker*.

1.2 Rumusan Masalah

Berdasarkan latar berlakang yang telah dijelaskan di atas, terdapat rumusan masalah yang nantinya akan di selesaikan dalam penelitian ini adalah

1. Bagaimana membangun sistem yang dapat mengirim *file* data penting secara aman melalui jaringan *public* khususnya pada Telkom Bojonegoro?
2. Bagaimana mengimplementasikan kriptografi RSA untuk mengamankan data penting pada Telkom Bojonegoro?

1.3 Batasan Masalah

Batasan masalah dalam Skripsi penulis yang berjudul Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro Untuk Meningkatkan Keamanan Sistem Jaringan adalah sebagai berikut:

1. Penelitian sebagian tidak menggunakan data asli karena alasan kepentingan perusahaan.
2. Penelitian menggunakan *socket port file transfer protocol/ftp.*
3. Aplikasi dirancang untuk Telkom Bojonegoro.

1.4 Tujuan

Tujuan yang ingin dicapai dalam penelitian ini adalah membuat aplikasi dengan menerapkan Algoritma Kriptografi RSA *(Rivest-Shamir-Adleman)* sebagai pengamanan *file* pada *Transport Layer* TCP/IP untuk jaringan *publik* maupun lokal.

1.5 Sistematika Penulisan

Dalam menyusun penulisan ini, sistem penulisan yang digunakan oleh penulis yaitu dengan cara membagi masalah menjadi beberapa tahapan, dimana pembahasan setiap babnya sebagai berikut.

BAB I PENDAHULUAN

Bab ini menguraikan latar belakang masalah, rumusan masalah, sistematika penulisan mengenai perlunya penelitian mengenai "Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro Untuk Meningkatkan Keamanan Sistem Jaringan".

BAB II LANDASAN TEORI

Bab ini berisikan teori-teori pendukung dan bahan penelitian yang diimplementasikan pada penelitian ini. Teori yang diambil dalam penelitian ini yaitu mengenai Kriptografi, Metode *Rivest Shamir Adleman* (RSA), TCP/IP, FTP, JAVA.

BAB III METODOLOGI PENELITIAN

Berisi tentang langkah-langkah yang dijalankan dan metode yang digunakan dalam proses. Beberapa uraian yang ada didalam metodologi penelitian antara lain metode pengembangan sistem, fase-fase pengembangan sistem.

BAB IV ANALISIS dan PERANCANGAN

Pada bagian ini diuraikan dengan jelas mengenai Implementasi Algoritma Kriptografi RSA Process Pada Sistem Komunikasi data Jaringan Pada Transport Layer TCP/IP dan penggunaan Port FTP. Sedangkan rancangan sistem akan direpresentasikan dengan Arsitektur Sistem, Data Flow Diagram, dan rancangan antarmuka.

BAB V IMPLEMENTASI dan PENGUJIAN

Bab ini Memaparkan secara detil sesuai rancangan komponen bahasa pemrograman yang dipakai dan uraian mengenai proses implementasi dan pengujian yang dilakukan dalam penelitian ini "Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro untuk Meningkatkan Keamanan Sistem Jaringan".

BAB VI HASIL dan PEMBAHASAN

Bab ini membahas mengenai hasil dari pengujian yang dilakukan dalam penelitian ini dari sistem yang telah dirancang juga penerapan dari hasil yang telah dianalisis dan dirancang sebelumnya.

BAB VII KESIMPULAN dan SARAN

Berisi Kesimpulan dan saran yang merupakan hal hal penting dari keseluruhan uraian bab-bab sebelumnya dari hasil peneitian yang telah dilakukan dan saran yang dapat memberikan gambaran bermanfaaat serta mungkin dapat menambah