BAB 1

PENDAHULUAN

1.1.Latar Belakang Masalah

Kemajuan teknologi informasi dan komunikasi saat ini telah memberikan pengaruh yang sangat besar bagi kehidupan manusia. Melalui pemanfaatan teknologi informasi dan komunikasi, semua kegiatan dapat dilakukan secara digital, seperti bertukar informasi yang tidak perlu lagi dilakukan dari mulut ke mulut atau melalui surat namun bisa dengan menggunakan pesan dari *software* pertukaran pesan yang saat ini telah banyak dibuat.

Pesan adalah seperangkat karakter berupa huruf, angka, tanda atau simbol yang dibuat untuk tujuan tertentu dan harapan bahwa dengan menyampaikan tanda atau simbol tersebut akan menghasilkan suatu informasi. Dalam pengiriman pesan melalui implementasi jaringan komputer, selalu ada ancaman yang mengganggu proses pengiriman yaitu penyerang. Seorang penyerang dapat mengamati, menguping, mengambil dan memodifikasi pesan yang akan dikirim. Ini sangat berbahaya karena penyerang dapat menggunakan data yang ditangkap untuk kepentingannya sendiri.

Menurut Mukhtar (2018) terdapat empat ancaman dalam keamanan data, yaitu yang pertama *Interruption* merupakan ancaman terhadap kerusakan data yang biasanya disebabkan oleh media penyimpanan yang rusak dan kelalaian pengguna. Yang kedua *Interception* yang merupakan kebocoran data dimana orang yang tidak berhak dapat memiliki informasi yang tersimpan dalam komputer. Yang ketiga *Modification* yaitu perubahan data oleh orang-orang yang tidak berhak atas data tersebut. Yang terakhir *Fabrication* yaitu meniru atau memalsukan informasi atau data dalam komputer.

Untuk itu diperlukan suatu sistem keamanan untuk mengamankan pesan yang ada di dalam jaringan komputer. Kriptografi yaitu ilmu yang mempelajari teknik-teknik matematika yang terkait dengan aspek keamanan data dan informasi, integritas data, serta autentikasi data.

Kriptografi merupakan ilmu yang bertujuan untuk mengamankan dan merahasiakan data dengan melakukan proses enkripsi dan dekripsi. Enkripsi adalah suatu proses perubahan data menjadi bentuk sandi yang tidak bisa dibaca. Dekripsi merupakan proses pengembalian data yang telah disandikan ke dalam bentuk semula yang dapat dibaca dan dipahami (Zulfikar et al., 2019).

Dalam sebuah jaringan, data atau pesan yang dikirimkan tanpa dienkripsi dapat dikatakan bahwa pesan tersebut adalah terbuka. Hal ini karena pesan yang tidak dienkripsi dapat di lihat dan dibaca oleh siapa saja. Namun dengan menerapkan proses enkripsi untuk merubah pesan menjadi chipertext, pesan tersebut akan menjadi rahasia dan hanya bisa dibaca oleh orang-orang yang memiliki kunci untuk mendekripsikan pesan tersebut.

Dalam ilmu kriptografi terdapat banyak jenis algoritma yang dapat digunakan untuk mengamankan pesan. Salah satu contohnya adalah Algoritma RSA (Rivest–Shamir–Adleman) yang merupakan salah satu jenis algoritma kriptografi asimetri. Algoritma kriptografi asimetri dinilai lebih aman dibandingkan dengan kriptografi simetri. Hal ini dikarenakan algoritma kriptografi asimetri akan menggunakan dua kunci yang berbeda untuk proses enkripsi dan dekripsi. Oleh karena itu, dalam penelitian ini akan digunakan Algoritma RSA dengan panjang bit 256 untuk proses pengamanan pesan.

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah yang diambil adalah:

1. Bagaimana mengamankan pesan dengan menggunakan algoritma RSA?
2. Bagaimana merancang aplikasi berbasis desktop untuk pertukaran pesan dengan menerapkan algoritma RSA?

1.3. Batasan Masalah

Untuk terfokusnya penelitian ini, maka batasan masalah pada penelitian ini:

1. Algoritma yang digunakan adalah RSA.
2. Penelitian ini hanya menerapkan teknik kriptografi pada pesan.

3. Menggunakan bahasa pemrograman Java.

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengamankan pesan agar aman selama proses pengiriman sehingga jika ada seseorang mencuri pesan dan tidak memiliki kunci untuk membuka pesan tersebut, maka pesan itu akan tetap aman karena tidak akan bisa dibaca.
2. Mengamankan pesan menggunakan dua kunci yang berbeda untuk proses penyandian dan pembacaan sandi sehingga tidak akan ada yang bisa membuka pesan yang telah disandikan.
3. Mengetahui algoritma RSA dan perancangan aplikasi pertukaran pesan berbasis desktop.

1.5. Manfaat Penelitian

Manfaat yang bisa diambil dari penelitian ini adalah:

1. Mengetahui dan memahami penggunaan Algoritma RSA.
2. Mengamankan data pengguna dalam proses pengiriman pesan melalui jaringan komputer yang tidak aman.
3. Sebagai sistem kriptografi yang nantinya dapat digunakan sebagai media belajar dan juga sebagai bahan penelitian untuk menganalisa celah keamanan pada data digital khususnya pada sistem keamanan pesan bagi peneliti lain.