BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dewasa ini masalah keamanan data dan kerahasiaan data adalah suatu hal yang sangat penting untuk diperhatikan. Data pribadi yang tersimpan dalam sebuah media *storage* (media penyimpanan seperti Hard disk, flashdisk, DVD) terkadang rentan terhadap pencurian sehingga data dapat dibaca/diketahui oleh orang lain, ataupun data yang ditransmisikan melalui jaringan internet yang rentan akan penyadapan oleh pihak-pihak yang tidak berwenang. Jika hal ini terjadi, maka akan sangat merugikan bagi pemilik data karena tidak adanya sistem pengamanan terhadap data tersebut. Dengan kondisi seperti ini maka penyimpanan data pada media *storage* dan pengiriman data melalui transmisi jaringan menjadi tidak aman lagi.

Permasalahan keamanan data tersebut dapat diatasi dengan menggunakan enkripsi data, yang merupakan salah satu komponen utama dalam bidang ilmu kriptografi. Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (plainteks) menjadi sebuah kode yang tidak bisa dimengerti (cipherteks). Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi. Dalam penelitian ini digunakan algoritma kriptografi RSA untuk enkripsi data. Algoritma ini termasuk algoritma *asymetris* yaitu algoritma yang

mempunyai sepasang kunci, diantaranya kunci publik *(public key)* yang digunakan untuk mengenkripsi pesan dan dapat diketahui oleh umum, serta kunci privat *(private key)* yang digunakan untuk mendekripsi pesan dan hanya pemilik kunci saja yang dapat mengetahuinya. Dalam menggunakan algoritma RSA, terdapat permasalahan terhadap data yang terenkripsi, yaitu ukurannya yang lebih besar dari pada data asli (plainteks). Hal ini tentu membutuhkan ruang yang besar untuk penyimpanan data. Maupun kebutuhan *bandwidth* saat proses pengiriman melalui jaringan internet, sehingga membutuhkan waktu yang lama dan biaya yang besar. Untuk mengatasi hal tersebut maka digunakanlah teknik pemampatan data (kompresi data). Pada penelitian ini digunakan algoritma Huffman untuk memampatkan data.

Berdasarkan permasalahan keamanan diatas, dalam penelitian ini penulis mengambil judul "Aplikasi Keamanan Data Menggunakan Algoritma RSA Serta Algoritma Huffman Untuk Pemampatan".

1.2 Rumusan Malasah

Masalah yang akan diteliti adalah Bagaimana membangun sebuah aplikasi keamanan data menggunakan algoritma RSA serta memanfaatkan algoritma Huffman untuk memampatkan data menjadi ukuran yang lebih kecil. Sehingga data akan terjamin keamanannya dengan ukuran data yang lebih kecil.

1.3 Ruang Lingkup

Ruang lingkup yang akan dibahas pada penelitian ini meliputi:

1 Dalam penelitian ini hanya membahas mengenai penyandian data meliputi proses pembangkitan kunci, proses enkripsi dan dekripsi menggunakan algoritma RSA serta memanfaatkan algoritma Huffman untuk pemampatan data (kompresi data). Tidak membahas mengenai keamanan dari data yang terenkripsi.

2 Pembagian blok plainteks menggunakan dua mode yaitu pembagian berdasarkan byte dan biner.

3 Data yang di enkripsi terbatas untuk data dalam karakter ASCII 128 byte.

4 Dalam penelitian ini hanya membahas mengenai proses enkripsi dan dekrispi data dalam format *.txt , *.html, *.rtf. Tidak mengenkripsi file selain file teks.

5 Untuk data yang telah di enkripsi di simpan dalam format *.enc.

6 Untuk data yang telah di enkripsi dan di mampatkan disimpan dalam format *.huf.

7 Pada proses pembangkitan kunci, *user* dapat memilih panjang kunci yang telah di tentukan yaitu antara 64 bit hingga 2048 bit dengan jarak antar kunci 64 bit.

8 Aplikasi dibuat menggunakan bahasa pemrograman Java dan UML sebagai bahasa pemodelan.

Dengan diberikan ruang lingkup seperti ini diharapkan permasalahan yang dibahas tidak akan melebar ke hal-hal yang lain.

1.4 Tujuan

Adapun tujuan dari penelitian ini adalah merancang dan mengembangkan sebuah aplikasi untuk mengamankan data pada media *storage* (penyimpanan) dan data yang ditransmisikan melalui jaringan internet dari penyadapan oleh pihak yang tidak berwenang dengan menggunakan algoritma RSA, serta memanfaatkan algoritma Huffman untuk memampatkan data yang telah dienkripsi.

Mengetahui perbandingan proses enkripsi dan dekripsi yang ditinjau dari segi waktu, ukuran plainteks dan cipherteks, rasio kompresi, dengan menggunakan dua mode pembagian blok plainteks byte dan biner.