BAB I

PENDAHULUAN

1.1. Latar Belakang

Keamanan dan kerahasiaan data merupakan salah satu faktor penting yang harus diperhatikan dalam komunikasi terutama dengan kemajuan dan perkembangan teknologi pada masa kini. Pesatnya perkembangan teknologi memberikan banyak dampak positif bagi masyarakat seperti kemudahan memperoleh informasi, pertukaran data dan pesan penyebaran informasi, pengiriman pesan, dan sebagainya. Namun, dengan kemudahan-kemudahan yang didapatkan, para pemilik data harus lebih sadar dalam menjaga data penting agar isi data tidak diketahui atau dimanipulasi oleh pihak-pihak tidak berkepentingan yang tidak seharusnya memiliki data tersebut. (Tampubolon, 2017)

File teks merupakan salah satu bentuk file yang berisi informasi-informasi dalam bentuk teks. Data yang berasal dari dokumen pengolah kata, angka yang digunakan dalam perhitungan, nama dan alamat dalam basis data merupakan contoh masukan data teks yang terdiri dari karakter, angka dan tanda baca. Masalah penyandian data teks merupakan salah satu aspek paling penting dalam dunia teknologi informasi. Setiap orang memerlukan suatu aplikasi yang dapat mengamankan suatu teks rahasia dan penting agar teks tersebut hanya dapat dilihat dan dibaca oleh orang tertentu saja. Beberapa cara telah dikembangkan untuk menangaini masalah ini, Salah satu cara untuk mengamankan data teks adalah menggunakan sistem kriptografi yaitu dengan penyandian isi informasi atau *plaintext* tersebut menjadi isi yang tidak dipahami melalui proses enkripsi

dan untuk memperoleh kembali informasi yang asli, dilakukan proses dekripsi disertai dengan menggunakan kunci yang benar. (Manullang, 2018)

Dibutuhkan sebuah metode yang dapat digunakan untuk mengamankan dan merahasiakan data. Salah satu ilmu yang diterapkan untuk menjaga keamanan dan kerahasiaan data, adalah kriptografi. Komunikasi dan kriptografi merupakan topik yang berhubungan erat dalam bidang telekomunikasi. Dengan kriptografi, teks asli akan diubah menjadi sandi yang hanya dapat diartikan oleh pihak yang memiliki kunci yang akan digunakan untuk mengubah sandi menjadi teks asli kembali, sehingga meskipun file diperoleh pihak lain, mereka hanya akan mendapatkan karakter-karakter acak tidak bermakna. (Tampubolon, 2017)

Salah satu algoritma dari kriptografi adalah Algoritma *Rivest Shamir Adleman* (RSA) merupakan algoritma kriptografi kunci publik. Algoritma RSA terdiri atas tiga proses, yaitu proses pembentukan kunci, enkripsi, dan dekripsi. Algoritma RSA memiliki kekuatan yang terletak pada proses eksponensial, dan pemfaktoran bilangan menjadi 2 bilangan prima yang hingga kini perlu waktu yang lama untuk melakukan pemfaktorannya. Algoritma RSA akan digunakan sebagai pengaman dari file teks. Algoritma ini sulit untuk dipecahkan karena ukuran hasil enkripsi yang besar dengan faktor pembangkitnya adalah dua bilangan prima yang berbeda. (Kaban, 2017)

Kriptografi algoritma RSA memiliki hasil enkripsi berupa *ciphertext* dengan ukuran yang paling besar dibandingkan dengan kriptografi algoritma yang lain, maka diperlukan metode kompresi sebagai solusi untuk menghasilkan ukuran hasil enkripsi atau *ciphertext* yang lebih kecil.

Perkembangan *software* saat ini menghasilkan ukuran data *output* yang semakin besar, sehingga memerlukan ruang penyimpanan yang semakin besar. Semakin besar ukuran data, semakin banyak ruang dan waktu yang diperlukan, untuk mengatasi permasalahan tersebut diperlukan suatu mekanisme yang disebut kompresi data atau *data compression*. Apabila ukuran data dapat dikompresi menjadi lebih kecil dari ukuran aslinya, maka secara otomatis memori dapat menyimpan data lebih banyak dan pengiriman data lebih cepat (Ujianto, 2010).

Salah satu algoritma kompresi yang dikenal adalah Algoritma *Huffman*. Algoritma *Huffman* sendiri merupakan algoritma yang digunakan untuk mengkompresi berbagai tipe data. Proses kompresi algoritma *Huffman* memiliki tiga fase, yaitu fase pembentukan pohon *Huffman*, kedua fase *encoding* dan fase *decoding*. (Kaban, 2017)

Hasil pengujian algoritma *Huffman* dan *Shannon Fano* pada file teks yang berisi *string* heterogen menunjukkan bahwa pada algoritma *Huffman* diproses dengan pembentukan pohon biner dari bawah ke atas. Sebaliknya, pada *Shannon Fano* pohon biner dibentuk dari atas ke bawah. Secara rata-rata algoritma *Huffman* menghasilkan rasio pemampatan lebih baik (61,3%) dari pada *Shannon-Fano* (76,9%). (Silaen, 2016).

Berdasarkan pemaparan diatas, maka dilakukan penelitian untuk membuat aplikasi enkripsi dan dekripsi teks dengan mengkombinasikan kriptografi algoritma RSA dan kompresi algoritma *Huffman* untuk melakukan proses pengamanan data pada file teks, serta untuk mengetahui hasil kinerja kombinasi kedua algoritma dalam hal pengamanan data dan kompresi data..

1.2. Rumusan Masalah

Berdasarkan dari latar belakang masalah, maka permasalahan yang didapat:

1. Bagaimana menerapkan kriptografi algoritma RSA dan kompresi algoritma *Huffman* untuk enkripsi dan dekripsi sebagai sarana pengamanan file teks?
2. Bagaimana menguji kriptografi algoritma RSA dan kompresi algoritma *Huffman* pada enkripsi dan dekripsi file teks?

1.3. Batasan Masalah

Batasan masalah penelitian ini adalah :

1. Objek file yang dapat diproses oleh aplikasi berupa file teks bertipe .txt
2. Algoritma kriptografi yang digunakan adalah algoritma RSA.
3. Algoritma kompresi yang digunakan adalah algoritma *Huffman*.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Membuat aplikasi enkripsi dan dekripsi file teks dengan menggunakan kriptografi algoritma RSA dan kompresi algoritma *Huffman*.
2. Menguji kriptografi algoritma RSA dan kompresi algoritma *Huffman* pada enkripsi dan dekripsi file teks.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah membantu bagi pengguna yang menggunakan aplikasi ini dalam mengamankan file berbentuk teks yang bersifat rahasia agar tidak disalahgunakan oleh pihak yang tidak berhak. Aplikasi ini membutuhkan kunci rahasia untuk mengembalikan file hasil enkripsi kebentuk semula dan menghasilkan ukuran hasil enkripsi yang lebih kecil.

1.6. Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah metode eksperimental. Tahapan metode experimental yang dilakukan untuk merealisasikan aplikasi yang akan dibuat adalah sebagai berikut:

1. Rumusan Masalah

   Proses perumusan masalah merupakan kumpulan pertanyaan utama dari permasalahan yang dicari dan akan dijawab dalam penelitian. Pada penelitian ini terdapat beberapa rumusan masalah yang terdiri dari bagaimana mengamankan file teks yang bersifat pribadi, bagaimana melakukan implementasi kriptografi algoritma RSA dan kompresi algoritma *Huffman* dalam aplikasi enkripsi dan dekripsi serta bagaimana menguji algoritma RSA dan algoritma *Huffman* yang telah dibangun.

2. Pengumpulan Data

   Pada tahap ini dilakukan proses pengumpulan data dengan menggunakan studi pustaka dan telaah jurnal baik berupa tulisan dan elektronik yang membahas tentang studi yang berkaitan dengan pengamanan file teks, kriptografi algoritma RSA dan kompresi algoritma *Huffman*.

3. Pengembangan Perangkat Lunak

   Pada proses ini akan dibangun sebuah aplikasi enkripsi dan dekripsi file teks menggunakan kriptografi Algoritma RSA dan kompresi Algoritma *Huffman*. Proses pengembangan perangkat lunak menggunakan Metode *Extreme Programming* yang terdiri dari 4 tahapan yaitu *planning, design*, *coding* dan *testing.*

4. Penilaian Kompresi

Proses penilaian kompresi merupakan proses untuk menilai kualitas kompresi algoritma *Huffman* yang telah di implementasikan dengan algoritma RSA dalam aplikasi enkripsi dan dekripsi file teks. Penilaian kompresi menurut Solomon dalam buku *Handbook Data Compression* edisi 10 terdapat beberapa faktor atau variabel digunakan untuk mengukur kualitas dari suatu teknik kompresi data. Variabel penilaian terdiri dari *Ratio of Compression* (RC), *Compression Ratio* (CR), *Redundancy* (RD) dan Waktu Kompresi serta Dekompresi.

5. Evaluasi

Proses evaluasi dilakukan untuk menilai kinerja aplikasi enkripsi dan dekripsi file teks menggunakan kriptografi algoritma RSA dan kompresi algoritma *Huffman* yang dibuat sesuai dengan fungsinya.

6. Hasil dan Kesimpulan

Proses memaparkan hasil penelitian yang dilakukan mengenai implementasi kriptografi algoritma RSA dan kompresi algoritma *Huffman* dalam aplikasi enkripsi dan dekripsi yang merupakan hasil akhir keseluruhan proses metode penelitian yang telah dilakukan.

1.7. Sistematika Penulisan

Sistematika penulisan dibuat untuk lebih memperjelas alur sehingga dapat lebih mudah memahami materi. Laporan tugas akhir ini dibagi menjadi lima bab yang dilengkapi dengan penjelasan pada setiap bab, yaitu sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, yang menjadi dasar dibuatnya penelitian, identifikasi masalah yang berisi mengenai latar belakang masalah yang ditemukan, rumusan masalah mengenai permasalahan yang terjadi, batasan masalah, tujuan penelitian sebagai hasil dari langkah penyelesaian masalah, manfaat penelitian, metodologi penelitian atau cara menyelesaikan masalah.

BAB II LANDASAN TEORI

Bab ini membahas teori-teori yang berhubungan dengan penelitian Tugas Akhir sebagai penunjang landasan atau acuan penelitian yang dilakukan.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan garis besar perancangan perangkat lunak yang dilibatkan dalam perancangan aplikasi.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan pengujian aplikasi beserta analisa kinerja dengan menggunakan beberapa contoh file.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas tentang kesimpulan yang merupakan jawaban dari tujuan penelitian. Saran yakni mengenai keterbatasan yang ada dalam sistem.