BAB I

PENDAHULUAN

I.1 Latar Belakang

Kerahasiaan data atau *file* yang dimiliki oleh seseorang merupakan hal yang sangat penting dalam pengiriman *file* agar *file* tersebut hanya dapat diberikan oleh orang tertentu saja, dan hanya orang yang menerima *file* yang dapat mengakses informasi tersebut. Untuk menjaga kerahasiaan data diperlukan pengamanan data atau dikenal sebagai kriptografi. Masalah pengamanan data *file* tersebut dapat diatasi dengan memanfaatkan metode *RSA* secara enkrip dan dekrip. Oleh karena itu dibutuhkan suatu sistem keamanan yang mampu menjaga kerahasiaan data dari ancaman lain yang dilakukan oleh pihak yang tidak bertanggung jawab. Dengan memanfaatkan algoritma *RSA* ini *system* akan mengenkripsi data asli yang diinputkan pengguna menjadi *chipertext*, kemudian mengirimkan kepada orang lain ataupun rekannya. Untuk penerimaan data asli di dekripsi menjadi *plaintext* oleh penerima sehingga pengiriman informasi atau pemanfaatan informasi melalui keamanan algoritma *RSA* menjadi lebih mudah dipahami oleh penerima ataupun pengguna *file pdf* tersebut.

Berdasarakan pembahasan latar belakang diatas maka penulis melakukan penelitian dengan judul **"*Implementasi Keamanan Dan Enkripsi Data Menggunakan Algoritma RSA Dalam Keamanan File PDF*".**

I.2 Ruang Lingkup Permasalahan

I.2.1 Identifikasi Masalah

Berdasarkan ruang lingkup permasalahan, penulis mengidentifikasi permasalahan yang ada sebagai berikut :

1. Akibat dari maraknya pencurian data, maka diperlukan aplikasi keamanan data *file* yang memberikan kerahasiaan data lebih terjaga.
2. Kurangnya keamanan kerahasian data *file Pdf* (isi *file*) maka diperlukan sebuah aplikasi kriptografi untuk melakukan enkripsi pada data isi *file Pdf.*
3. Sering terjadinya pengubahan data, maka diperlukan aplikasi keamanan data *file* agar dapat memberikan kerahasiaan atau keamanan pada data *file Pdf* .

I.2.2 Rumusan Masalah

Berdasarkan rumusan masalah yang ada berikut diantaranya adalah :

1. Bagaimana merancang aplikasi pengamanan data berupa teks pada *file pdf* dengan menggunakan algoritma *RSA*?
2. Bagaimana cara melakukan enkripsi dan dekripsi terhadap data berupa teks pada *file pdf* dengan menerapkan algoritma *RSA*?
3. Bagaimana mengimplementasikan aplikasi keamanan data berupa teks pada *file pdf* dengan menerapkan algoritma *RSA* untuk pengamanan data berupa teks pada *file pdf* berbasis *Web*?

I.2.3 Batasan Masalah

Berikut yang merupakan batasan masalah pada penelitian ini yaitu :

1. Aplikasi yang dibuat hanya berisi pengamanan data berupa teks pada *file pdf*.
2. Aplikasi yang dirancang hanya menggunakan algoritma *RSA*.
3. Informasi yang akan diamankan dalam aplikasi adalah dalam bentuk teks.
4. Implementasi aplikasi pengamanan data berupa teks pada *file pdf* berbasis *web*.

I.3 Tujuan Dan Manfaat Penelitian

I.3.1 Tujuan Penelitian

Berikut ini adalah merupakan tujuan dari penelitian ini yaitu adalah :

1. Untuk membuat aplikasi pengamanan data berupa teks pada *file pdf* dengan menggunakan Algoritma *RSA* berbasis *Web*.
2. Memberikan hasil enkripsi dan dekripsi data berupa teks pada *file pdf* dengan penerapan Algoritma *RSA* berbasis *Web*.
3. Menerapkan Algoritma *RSA* kedalam pengamanan data berupa teks pada *file pdf* berbasis *Web*.

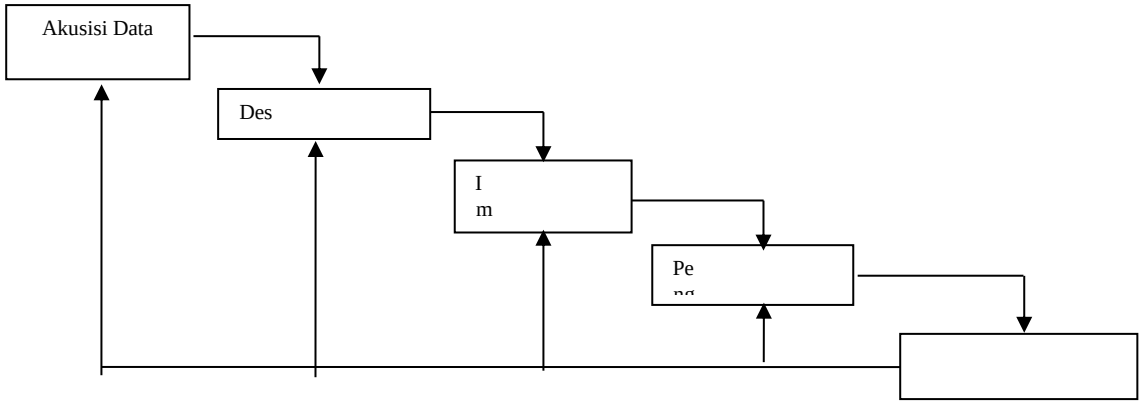
I.3.2 Manfaat Penelitian

Adapun beberapa manfaat dari penelitian ini adalah sebagai berikut :

1. Untuk lebih memudahkan pengguna dalam bertukar informasi.
2. Membantu pengguna menjaga kerahasiaan informasi dari data berupa teks pada *file pdf*.
3. Penerapan algoritma *RSA* ini membantu pengguna memberikan hasil keamanan data berupa teks pada *file pdf* yang lebih tepat dan akurat hingga pemanfaatan informasi selanjutnya dapat berjalan dengan baik.

I.4 Metodologi Penelitian

Dalam pengembangan suatu sistem ini peneliti menggunakan model *waterfall* kerena pengaplikasian menggunakan model ini mudah diimplementasikan dimana hal ini menggambarkan pendekatan yang sistematis dan juga berurutan pada pengembangan perangkat lunak. Tahapan metode *waterfall* dapat dilihat pada gambar I.4 di bawah ini.



Gambar I.1 : Model Waterfall

Sumber* : *(Budi Satrio: 2018)

Penjelasan gambar I.1 Perancangan pengamanan data *file pdf* menggunakan Algoritma *RSA* berbasis *desktop* pada model *waterfall:*

a. Akusisi Data

Akuisisi data merupakan metode yang dilakukan penulis dengan mengambil, mengumpulkan dan menyiapkan data yang berisi tentang Perancangan pengamanan data *file pdf* menggunakan Algoritma *RSA* berbasis *web*. Pada penelitian ini penulis memilih referensi dari jurnal, *web*, buku, perpustakaan dan skripsi yang berkaitan dengan penelitian ini.

b. Design Sistem

Pada tahapan ini, *design* sistem membantu dalam menentukan perangkat keras *(hardware)* dan mendefenisikan arsitektur sistem secara keseluruhan dengan menggunakan *use case* pada sistem yang akan dibangun.

c. Implementasi Sistem

Pada tahap ini, sistem pertama kali dikembangkan di program kecil yang disebut *unit*, yang terintegrasi dalam tahap selanjutnya. Setiap *unit* dikembangkan dan diuji untuk fungsionalitas yang disebut sebagai *unit testing*.

d. Pengujian Sistem

Dalam tahapan ini, sistem yang dirancang diuji kemampuan dan keefektifan nya dalam suatu *BlackBox Testing*. Sehingga didapatkan

kekurangan dan kelemahan sistem yang kemudian dilakukan pengkajian ulang dan perbaikan terhadap aplikasi.

e. Pemeliharaan Sistem

Tahap akhir dalam model *waterfall* ini perangkat lunak yang sudah jadi, dijalankan serta dilakukan pemeliharaan. Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya. Perbaikan implementasi *unit* sistem dan peningkatan jasa sistem sebagai kebutuhan baru.

I.5. Kontribusi Penelitian

Adapun kontribusi yang diberikan pada penelitian ini adalah sebagai berikut:

1. Aplikasi yang dihasilkan dari penelitian ini dapat memudahkan pengguna dalam bertukar informasi terutama informasi dalam bentuk *file pdf*.
2. Meningkatkan penggunaan teknologi dalam membangun aplikasi web dalam mengamankan kerahasiaan isi *file pdf*.
3. Penelitian yang akan dihasilkan dapat dijadikan rujukan bagi peneliti lainnya yang ingin mengembangkan sistem atau aplikasi yang lebih spesifik untuk diterapkan dalam bidang lainnya.

I.6. Sistematika Penulisan

Sistematika penulisan skripsi ini dibagi menjadi lima bab yang merangkum tiap tahapan yang penulis lakukan, antara lain :

BAB I : PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, ruang lingkup masalah, tujuan dan manfaat skripsi, serta metodologi skripsi.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menguraikan tentang beberapa penjelasan dan pengertian yang berdasarkan dengan judul.

BAB III : ANALISIS DAN DESAIN SISTEM

Pada bab ini berisikan analisa permasalahan dan kebutuhan alat, serta pemodelan sistem secara fungsional.

BAB IV : HASIL DAN UJI COBA

Bab ini berisikan tentang tampilan hasil yang dirancang, pembahasan uji coba dari sistem, dan kelebihan serta kekurangannya.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisikan bagian penutup yang berisi kesimpulan serta saran untuk pengembangan sistem alat selanjutnya.