BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan sistem keamanan sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Teknologi juga memberikan kemudahan untuk bertukar informasi sehingga keamanan data tidak dapat lepas dari berbagai aspek kegiatan manusia yang memungkinkan dapat menjaga kerahasiaan informasi tersebut, namun dalam implementasinya masih terdapat kecurangan dan ancaman terhadap data khususnya pada data file word. Akibat dari maraknya pencurian data, maka diperlukan aplikasi keamanan data *file Word* (isi file) yang memberikan kerahasiaan data lebih terjaga dan kurangnya keamanan kerahasian data *file Word* (isi file) maka diperlukan sebuah aplikasi kriptografi untuk melakukan enkripsi pada data *file Word* (isi file) yang penyembunyiannya dapat diperkuat dengan sistem penguncian.

Terdapat banyak metode pengamanan data yang bisa dimanfaatkan untuk mencegah adanya kecurangan ataupun manipulasi data salah satunya menggunakan kriptografi ataun teknik penyamaran lainnya. Kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.

RSA (Rivest Shamir Adleman) merupakan salah satu algoritma public key yang populer dipakai dan bahkan hingga saat ini Algoritma RSA masih dianggap aman dan Affine cipher adalah perluasan dari caesar cipher, yang menggalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran.

Kecurangan data file word (isi file) tersebut dapat diatasi dengan memanfaatkan metode RSA dan Afiine Chiper secara enkrip dan deskrip.

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 dan Affine chiper ini system akan mengenkripsi data asli yang diinputkan pengguna menjadi chipertkes dengan menggunakan key, kemudian mengirimkan kepada orang lain ataupun rekannya. Untuk penerimaan data asli dideskripsi menjadi plainteks menggunakan key juga oleh penerima sehingga pengiriman informasi atau pemanfaatan informasi melalui keamanan algoritma RSA dan Affine chiper menjadi lebih muda dipahami oleh penerima ataupun pengguna file word tersebut.

Berdasarakan pembahasan latar belakang diatas maka penulis melakukan penelitian dengan judul **"*Penerapan Algoritma RSA dan Affine Cipher dalam Keamanan File MS Word*".**

I.2 Ruang Lingkup Permasalahan

I.2.1 Identifikasi Masalah

Berdasarkan latar belakang tersebut, penulis mengidentifikasi masalah sebagai berikut :

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

I.2.2 Rumusan Masalah

Rumusan masalah dalam pembahasan dan permasalahan yang akan dihadapi dalam perancangan aplikasi ini :

1. Bagaimana merancang aplikasi keamanan data *file Word* (isi file) dengan menerapkan *Algoritma RSA dan Affine Chiper* ?
2. Bagaimana cara melakukan enkripsi dan deskripsi terhadap data File (isi file) dengan menerapkan *Algoritma RSA dan Affine Chiper*?
3. Bagaimana mengimplementasikan aplikasi *keamanan* data File dengan menerapkan *Algoritma RSA dan Affine Chiper* untuk pengamanan data file (isi file) Ms Word berbasis *Web*?

I.2.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini agar tidak menyimpang dari tujuan semula adalah :

1. Studi kasus yang akan diuji cobakan dalam penelitian ini adalah penguncian data *file Word* (isi file) dengan menggunakan kata kunci.
2. Pengamanan data *MS Word* menggunakan kriptografi dengan Algoritma *RSA dan Affine Cipher*
3. Sistem yang dirancang menggunakan bahasa pemrograman *HTML* dan *PHP*.
4. Sistem yang akan diamankan adalah *file* (isi file) data *MS. Word*.
5. Sistem yang dibangun masih bersifat *basic alone / Web.*

I.3 Tujuan dan Manfaat

I.3.1 Tujuan Penelitian

Adapun tujuan dari penelitian penulis ini adalah :

1. Untuk membangun aplikasi keamanan data dengan penerapan *Algoritma RSA dan Affine Chiper* dalam mengamankan data *file* (isi file) berbasis *Web*.
2. Memberikan hasil enkripsi dan dekripsi data *file Word* (isi file) dengan penerapan *Algoritma RSA dan Affine Chiper* berbasisi *Web*.
3. Menerapkan *Algoritma RSA dan Affine Chiper* kedalam pengamanan data *file Word* (isi file) berbasis *Web.*

I.3.2 Manfaat Penelitian

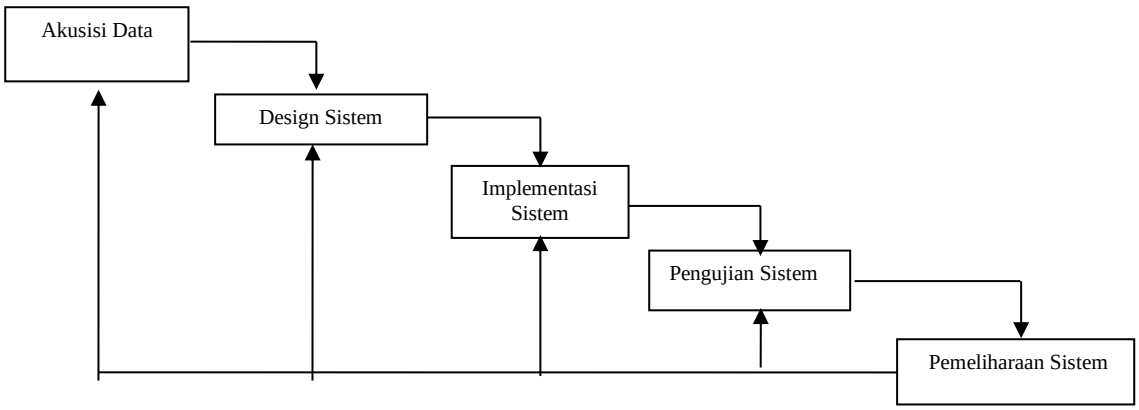
Adapun dilakukannya penelitian ini adalah :

1. Membantu pengguna menjaga kerahasiaan informasi dari data file word (isi file).

2. Dengan adanya penerapan algoritma RSA dan Affine Chiper pada keamanan data file word (isi file) pengguna lebih mudah untuk bertukar informasi.
3. Penerapan algoritma RSA dan Affine Chiper ini membantu pengguna memberikan hasil keamanan data file Word (isi file) 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 III.1 di bawah ini.



Gambar III.1 : Model Waterfall

Sumber* : *(Budi Satrio: 2018)

Penjelasan gambar III.1 Perancangan pengamanan data file word menggunakan Algoritma *RSA dan Affine Chiper* 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 word menggunakan Algoritma *RSA dan Affine Chiper* 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 yang menjadi kontribusi penelitian ini pada sistem yang dirancang oleh penulis dapat dilihat sebagai berikut :

1. Penelitian Heri Santoso, M. Fakhriza (2018) yang berjudul Perancangan Aplikasi Keamanan File Audio Format Wav (Waveform) Menggunakan Algoritma Rsa" Menghasilkan penelitian Perangkat lunak (software) dapat melakukan penyandian data audio dengan menerapkan algoritma RSA dan struktur data audio WAV. Ukuran berkas audio WAV menjadi bertambah besar setelah dilakukan enkripsi menggunakan algoritma RSA berdasarkan besar kunci yang digunakan. Sedangkan penelitian yang saya buat menerapkan sebuah algoritma yang belum pernah digunakan sebelumnya untuk melakukan enkripsi dan dekripsi terhadap data *file* MS Word yaitu *Algoritma RSA dan Affine Cipher*.
2. Penelitian dari Raja Nasrul Fuad, Haikal Nando Winata, dkk (2017) yang berjudul Aplikasi Keamanan File Audio Wav (Waveform) Dengan Terapan

Algoritma Rsa menghasilkan Perangkat lunak (software) dapat melakukan penyandian data audio dengan menerapkan algoritma RSA dan struktur data audio WAV. Ukuran berkas audio WAV menjadi bertambah besar setelah dilakukan enkripsi menggunakan algoritma RSA berdasarkan besar kunci yang digunakan sedangkan penelitian saya menerapkan sebuah algoritma yang belum pernah digunakan sebelumnya untuk melakukan enkripsi dan dekripsi terhadap data *file* MS Word yaitu *Algoritma RSA dan Affine Cipher*.

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.