BAB I

PENDAHULUAN

I.1. Latar Belakang

Sebuah pesan yang dikelola oleh pengelola informasi umumnya berbentuk sebuah tulisan, sehingga pesan tersebut dapat dibaca dan dimengerti dengan mudah. Namun pesan yang tersimpan dapat dibaca oleh siapa saja walaupun tidak berhak mengetahui pesan tersebut termasuk pencuri pesan. Sehingga pencuri pesan dapat menggunakan pesan yang dicuri untuk dikelola menjadi informasi yang baru dan lebih bermanfaat dan merugikan pemilik pesan. Oleh karena itu dibutuhkan sebuah cara yang dapat mengamankan pesan ataupun informasi yang bersifat rahasia sehingga tidak dapat dimiliki oleh pihak yang tidak diinginkan.

Pada bidang ilmu komputer, untuk mengamankan informasi dalam bentuk tulisan dikenal sebagai teknik kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Kriptografi mengubah informasi asli (*plaintext*) melalui proses enkripsi menjadi informasi acak (*ciphertext*) menggunakan algoritma dan kunci tertentu, lalu setelah diterima oleh penerima informasi, *ciphertext* akan diubah kembali menjadi plaintext melalui proses dekripsi menggunakan algoritma dan kunci yang sama dengan proses enkripsi. (Rambe, dkk, 2018 : 724). Namun peneliti ingin memperkuat keamanan sebuah pesan dengan menyisipkan pesan yang telah dirahasiakan ke dalam sebuah gambar dengan teknik *steganography*, sehingga keamanan pesan menjadi lebih baik. *Steganography* adalah teknik

penyembunyian data dalam sebuah medium yang dapat berupa jenis data apapun seperti *file* citra gambar, *audio*, *video*, maupun jenis data yang lainnya. (Farid, dkk, 2016 : 110). Namun untuk menggunakan teknik kriptografi dibutuhkan sebuah metode yang baik dalam penyandian pesan. Peneliti menggunakan metode RSA untuk menyandikan pesan. Algoritma RSA melakukan pemfaktoran bilangan yang sangat besar, oleh karena alasan tersebut RSA dianggap aman. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. (Sekarwati dan Budiman, 2017 : 56). Dengan menggunakan teknik kriptografi menggunakan metode RSA akan dapat menyandikan sebuah pesan kemudian pesan yang telah disandikan disisipkan pada sebuah gambar menggunakan teknik *steganography*. Namun teknik *steganography* membutuhkan sebuah metode, oleh karena itu peneliti menggunakan metode *Least Significant Bit* (LSB). *Least Significant Bit* (LSB) merupakan metode *steganography* yang paling sederhana dan mudah untuk diimplementasikan ke sebuah aplikasi. Metode ini menggunakan citra digital sebagai *convertext*. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), bit yang paling kurang berarti (*least significant bit atau* LSB). (Harjo, dkk, 2016 : 14). Pada penelitian ini peneliti menambahkan niai dua pada hasil penyisipan pesan ke dalam gambar pada metode LSB, sehingga keamanan menjadi lebih baik. Dengan adanya penerapan dari dua teknik keamanan pesan yaitu kriptografi dan *steganography* maka pesan yang memliki informasi yang bersifat pribadi memiliki keamanan yang lebih baik. Dengan latar belakang tersebut maka peneliti menyimpulkan judul "**Perancangan Sistem Kombinasi Keamanan Pesan Menggunakan Algoritma RSA Dan Metode LSB+2**"**.**

I.2. Ruang lingkup Permasalahan

Ruang lingkup permasalahan yang dapat diberikan untuk penelitian ini adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Identifikasi masalah yang terdapat pada penelitian ini adalah sebagai berikut :

1. Kurangnya keamanan pada pesan yang bersifat rahasia.
2. Belum ada penerapan algoritma RSA dan metode LSB+2 dalam mengamankan sebuah pesan.

I.2.2. Perumusan Masalah

Perumusan masalah pada penelitian ini yaitu :

1. Bagaimana membangun aplikasi kombinasi keamanan pesan menggunakan algoritma RSA dan metode LSB+2 ?
2. Bagaimana mengamankan sebuah pesan yang bersifat rahasia ?
3. Bagaimana penerapan algoritma RSA dan metode LSB+2 dalam mengamankan sebuah pesan ?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini berdasarkan latar belakang adalah sebagai berikut :

1. Aplikasi hanya untuk mengamankan sebuah pesan teks.
2. Aplikasi hanya dapat berjalan pada sistem operasi *windows*.
3. *Input* aplikasi ini berupa teks.
4. *Output* aplikasi ini berupa teks tersandi dan gambar yang tersisip pesan.

5. Pembuatan Aplikasi ini menggunakan bahasa pemrograman *Visual Basic* 2010.
6. Perancangan Aplikasi ini menggunakan pemodelan UML.
7. Metode yang digunakan adalah metode RSA dan LSB+2.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Menerapkan keamanan pada sebuah pesan yang bersifat rahasia.
2. Menerapkan algoritma RSA dan metode LSB+2 dalam mengamankan sebuah pesan.
3. Membangun aplikasi kombinasi keamanan pesan menggunakan algoritma RSA dan metode LSB+2.

I.3.2. Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut :

1. Mendapatkan sistem keamanan baru untuk sebuah pesan yang bersifat rahasia.
2. Mendapatkan pengetahuan baru mengenai kombinasi algoritma RSA dan metode LSB+2 dalam mengamankan sebuah pesan.
3. Mendapatkan aplikasi yang dapat mengamankan pesan dengan dua metode.

I.4. Metodologi Penelitian

Beberapa tahapan yang digunakan dalam penelitian ini dijabarkan sebagai berikut :

I.4.1. Pengumpulan Data

Pengumpulan data yang peneliti lakukan menggunakan beberapa teknik ataupun cara sebagai berikut :

1. Sampel

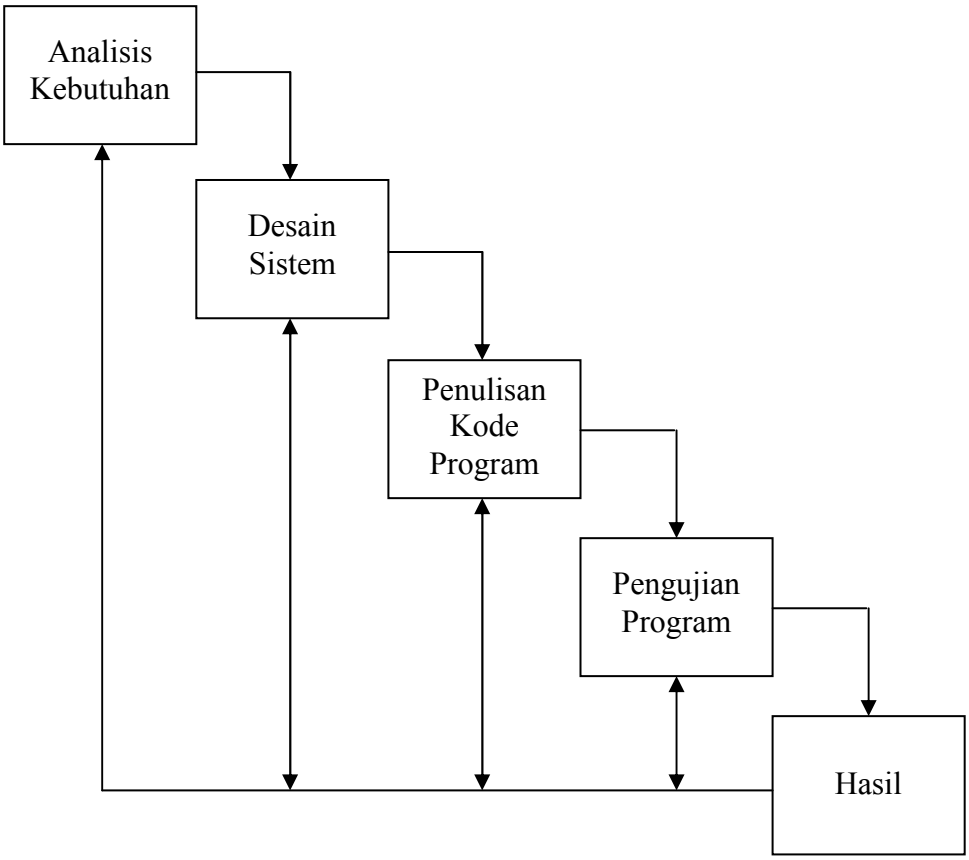
   Mengambil beberapa sampel ataupun contoh penelitian yang berkaitan dengan penelitian ini.

2. Penelitian Kepustakaan

   Pada metode ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi yang dikutip dapat berupa teori yaitu jurnal dan buku.

I.4.2. *Waterfall* Metode Penelitian

Peneliti menggunakan *Waterfall* untuk menggambarkan alur kerja yang peneliti lakukan untuk menyelesaikan penelitian ini.



Gambar I.1. *Waterfall* Metode Penelitian

Keterangan :

1. Analisa Kebutuhan

Peneliti menganalisa kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan pengumpulan data-data tentang kriptografi dan *steganography*.

2. Desain Sistem

Pada tahap ini dilakukan desain sistem menggunakan pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Penulisan kode program diterapkan pada beberapa bahasa pemrograman antara lain *Visual Basic* 2010.

4. Pengujian Program

Pengujian program dilakukan untuk mengetahui hasil dari perancangan sistem yang telah dibuat dan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik.

5. Hasil

Pada tahapan ini penelitian sudah memiliki hasil yang sesuai dengan perencanaan awal, sehingga sistem yang telah di buat dapat diterapkan. Tujuan akhir penelitian ini yaitu menghasilkan aplikasi kombinasi keamanan pesan menggunakan algoritma RSA dan metode LSB+2.

I.5. Kontribusi Penelitian

Kontribusi yang dihasilkan penelitian ini yaitu :

1. Penelitian ini dapat menjadi referensi terbaru bagi peneliti berikutnya.
2. Penelitian ini dapat menjadi ide baru untuk peneliti berikutnya.
3. Penelitian ini dapat memberikan keamanan pesan yang bersifat rahasia.

I.6. Sistematika Penulisan

Sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan Skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan serta perangkat yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisikan berbagai kesimpulan yang dapat dibuat berdasarkan uraian yang telah disimpulkan dan saran.