BAB I

PENDAHULUAN

I.1. Latar Belakang

Umumnya para pencuri mengambil pesan penting berupa teks yang terdapat pada sebuah data. Dengan mendapatkan informasi dari pesan yang telah dicuri, maka hal ini dapat menguntungkan pihak pencuri pesan dan merugikan pihak pemilik pesan. Masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik pesan. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, sering kali keamanan dikurangi atau ditiadakan. Oleh karena itu dibutuhkan sebuah cara agar pesan yang bersifat penting dapat terlindungi dari tindakan pencurian.

Cara yang dapat digunakan yaitu merahasiakan isi pesan dengan merubah pesan asli menjadi pesan rahasia dan cara isi dapat menggunakan kriptografi. Kriptografi adalah merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Kriptografi adalah proses penggunaan berbagai teknik dan atau ilmu dan seni untuk menjaga keamanan pesan. (Fauzi, dkk, 2017 : 2). Namun peneliti ingin memperkuat kerahasiaan sebuah pesan dengan menyisipkan pesan yang telah disandikan ke dalam sebuah gambar dengan teknik steganografi, sehingga kerahasiaan pesan menjadi lebih baik. Steganografi 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 algoritma yang baik dalam penyandian pesan. Peneliti menggunakan algoritma *Vernam Cipher* dan ROT13 untuk merahasiakan pesan. *One Time Pad* yang dikenal dengan algoritma *Vernam*, ditemukan oleh Gillbert Vernam di Major Joseph Mauborge and AT & T's. Konsep dasar algoritma *One Time Pad* hampir sama dengan algoritma *Vigenere*, hanya saja pada algoritma ini, kunci dibangkitkan secara acak, dan kecil kemungkinan kunci akan saling sama satu dengan lainnya. (Harahap, 2016 : 63). ROT13 (*Rotate* 13) adalah enkripsi substitution pada sistem enkripsi ROT13 sebuah huruf digantikan dengan huruf yang letaknya di atas 13 posisi darinya. (Sinaga dan Mesran, 2017 : 38). Dengan menggunakan teknik kriptografi menggunakan algoritma ROT13 akan dapat menyandikan sebuah pesan kemudian pesan yang telah disandikan disisipkan pada sebuah gambar menggunakan teknik steganografi. Namun teknik steganografi membutuhkan sebuah algoritma, oleh karena itu peneliti menggunakan algoritma *Least Significant Bit* (LSB) untuk menyisipkan sebuah pesan ke dalam gambar. *Least Significant Bit* (LSB) merupakan algoritma stegnografi yang paling sederhana dan mudah untuk diimplementasikan ke sebuah aplikasi. Algoritma ini menggunakan citra digital sebagai *convertext*. Pada susunan *bit* di dalam sebuah *byte* (1 byte = 8 *bit*), ada *bit* yang paling berarti (*most significant bit* atau MSB) dan *bit* yang paling kurang berarti (*least significant bit* atau LSB). (Harjo, dkk, 2016 : 14). Dengan latar belakang tersebut maka peneliti

menyimpulkan judul **"Penerapan Algoritma Vernam Cipher Dan ROT13 Untuk Pesan Rahasia Serta Penyisipan Gambar Menggunakan LSB".**

I.2. Ruang lingkup Permasalahan

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

I.2.1. Identifikasi Masalah

Identifikasi masalah berdasarkan latar belakang yang telah dijelaskan di atas adalah sebagai berikut :

1. Pesan yang bersifat penting dapat dicuri oleh pencuri informasi.
2. Belum ada penerapan algoritma *Vernam Cipher*, ROT13 dan algoritma LSB untuk merahasiakan sebuah pesan yang bersifat penting.
3. Dibutuhkan sebuah aplikasi yang dapat merahasiakan pesan yang bersifat penting.

I.2.2. Perumusan Masalah

Perumusan masalah pada penelitian ini yaitu :

1. Bagaimana merahasiakan pesan dari pencuri informasi ?
2. Bagaimana menerapkan algoritma *Vernam Cipher*, ROT13 dan algoritma LSB dalam merahasiakan sebuah pesan ?
3. Bagaimana menghasilkan aplikasi penerapan algoritma *vernam cipher* dan ROT13 untuk pesan rahasia serta penyisipan gambar menggunakan LSB ?

I.2.3. Batasan Masalah

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

1. Aplikasi hanya untukmemberikan kerahasiaan pesan teks.
2. Aplikasi hanya dapat berjalan pada sistem operasi *windows*.
3. *Input* aplikasi ini berupa pesan teks dan gambar.
4. *Output* aplikasi ini berupa *ciphertext* 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 algoritma *Vernam Cipher*, ROT13 dan algoritma LSB.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Merahasiakan pesan dari pencuri informasi.
2. Menerapkan algoritma *Vernam Cipher*, ROT13 dan algoritma LSB dalam merahasiakan sebuah pesan.
3. Menghasilkan aplikasi penerapan algoritma *vernam cipher* dan ROT13 untuk pesan rahasia serta penyisipan gambar menggunakan LSB.

I.3.2. Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut :

1. Pesan yang bersifat penting mendapatkan kerahasiaan yang baik.
2. Mengetahui dan memahami penerapan algoritma *Vernam Cipher*, ROT13 dan algoritma LSB.

3. Mendapat wawasan dalam pembuatan perangkat lunak kriptografi dan steganografi.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :

I.4.1. Pengumpulan Data

Berikut ini adalah beberapa teknik pengumpulan data yang peneliti lakukan untuk melengkapi bahan penelitian :

1. Sampel

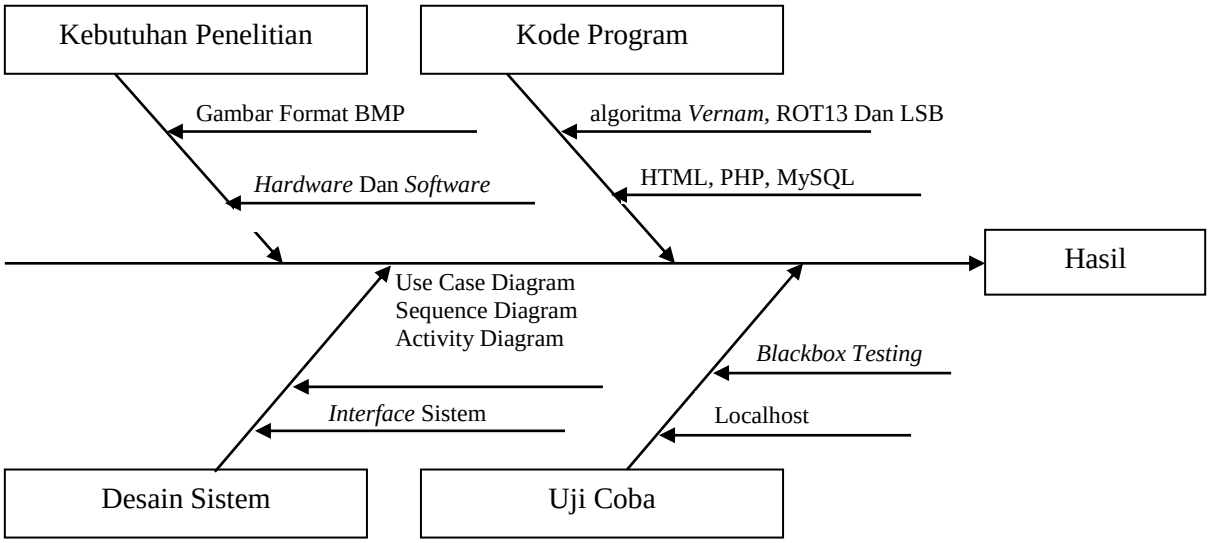
   Sampel yang digunakan yaitu aplikasi kriptografi dan steganografi terdahulu dan beberapa referensi mengenai pembuatan aplikasi kriptografi dan steganografi.

2. Penelitian Kepustakaan

   Penelitian kepustakaan yang digunakan yaitu jurnal-jurnal penelitian terdahulu.

I.4.2. *Fish Bone*Metode Penelitian

Berikut adalah *fish bone* metode penelitian yang digunakan dalam penulisan skripsi ini dapat dilihat pada gambar I.1.



Gambar I.1. *Fish Bone*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 steganografi.

2. Desain Sistem

Pada tahap ini dilakukan desain sistem menggunakan pemodelan UML yaitu *use case 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 yaitu menghasilkan aplikasi penerapan algoritma *vernam cipher* dan ROT13 untuk pesan rahasia serta penyisipan gambar menggunakan LSB.

I.5. Kontribusi Penelitian

Kontribusi penelitian dari aplikasi penerapan algoritma *vernam cipher* dan ROT13 untuk pesan rahasia serta penyisipan gambar menggunakan LSB yaitu :

1. Hasil penelitian ini dapat menghasilkan kerahasiaan pesan yang lebih baik.
2. Hasil penelitian ini dapat menjadi referensi baru bagi peneliti berikutnya.
3. Hasil penelitian ini dapat menjadi referensi baru di Universitas Potensi Utama.

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.