BAB I
PENDAHULUAN

I.1. Latar Belakang

Dengan semakin berkembangnya pemanfaatan teknologi informasi dalam membantu pekerjaan manusia di berbagai jenis kegiatan yang melibatkan komputer sebagai medianya, maka keamanan menjadi aspek yang sangat penting dalam sistem informasi. Beberapa informasi umumnya hanya ditujukan bagi segolongan orang tertentu, oleh karena itu keamanan data sangat dibutuhkan untuk mencegah informasi tersebut sampai pada pihak-pihak lain yang tidak berkepentingan sehingga adanya kemungkinan kebocoran atau penyalahgunaan data dapat dihindari, maka dirancang suatu sistem keamanan yang berfungsi untuk melindungi sistem informasi tersebut.

Salah satu upaya pengamanan sistem informasi tersebut yang dapat dilakukan adalah dengan kriptografi. Kriptografi merupakan sebuah metode untuk menjaga kerahasiaan pesan dari pihak yang tidak berkepentingan. Pesan dirahasiakan dengan cara mengacak nilai-nilai yang terdapat didalamnya sehingga membuat pesan tersebut tidak memiliki arti lagi.

Pesan dalam kriptografi dapat berupa tulisan, citra, video, dan sebagainya. Citra digital dapat diartikan sebagai sebuah pesan karena didalamnya terdapat sejumlah informasi. Pada suatu saat, *file* citra dapat menjadi aset berharga yang tidak boleh dilihat selain oleh orang yang bersangkutan. Untuk mencegah terjadinya hal-hal yang tidak diinginkan, seperti bocornya pesan rahasia yang

terdapat dalam citra kepada publik, kita dapat melakukan enkripsi terhadap *file* citra agar *file* citra tersebut tidak dapat dilihat dan dimengerti pesan yang terkandung di dalamnya oleh orang yang tidak berhak. Kerahasiaan pesan yang terdapat dalam *file* citra juga dapat dijaga dengan metode kriptografi.

Dalam kriptografi, pesan yang belum disandikan disebut *plainteks*, sedangkan pesan yang telah disandikan disebut *cipherteks*. Terdapat dua proses pada kriptografi yang berguna untuk menyandikan dan mengekstraksi pesan yang telah disandikan. Proses tersebut antara lain enkripsi dan dekripsi. Enkripsi adalah proses menyandikan *plainteks* menjadi *cipherteks*. Sedangkan dekripsi merupakan proses mengembalikan *cipherteks* menjadi *plainteks* semula, agar dapat diketahui informasi yang terkandung didalamnya. Salah satu yang dapat dimanfaatkan adalah enkripsi dan dekripsi data atau dengan kata lain menyandikan data sehingga hanya orang yang bersangkutan saja yang dapat mengetahui isi data tersebut.

Banyak algoritma kriptografi yang bisa digunakan untuk memanipulasi warna yang terdapat dalam citra, salah satunya dengan algoritma kriptografi klasik seperti metode *vigenere cipher*. Metode *vigenere cipher* merupakan metode yang cukup kuat dan sampai saat ini dinyatakan aman. Berdasarkan berbagai pertimbangan tersebut maka dalam penyusunan skripsi ini, penulis memilih judul **"Membangun Perangkat Lunak Kriptografi Citra Digital Menggunakan Metode *Vigenere cipher*"**.

I.2. Ruang Lingkup Permasalahan

Untuk menentukan solusi yang tepat terhadap suatu permasalahan, lingkup permasalahan yang dibahas dalam skripsi ini adalah:

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang masalah diatas, identifikasi masalahnya adalah sebagai berikut :

1. Adanya pencurian data atau pesan khususnya citra digital oleh orang lain yang tidak berhak.
2. Bagaimana membangun suatu aplikasi kriptografi citra digital yang mengimplementasikan dengan metode *vigenere cipher*.
3. Bagaimana agar citra digital dapat disandikan menggunakan aplikasi kriptografi dengan metode *vigenere cipher*.

I.2.2. Perumusan Masalah

Berdasarkan identifikasi masalah diatas, dapat dirumuskan beberapa masalah yaitu :

1. Bagaimana agar sistem dapat mengenkripsi citra digital yang ingin dienkripsi sehingga ketika orang lain mencoba membuka citra digital tersebut, yang tampil adalah citra digital yang tidak jelas karena telah dienkripsi sistem ?
2. Bagaimana merancang suatu sistem enkripsi citra digital yang dapat mengenkripsi gambar sehingga *file* citra digital akan tampak samar setelah dienkripsi ?

I.2.3. Batasan Masalah

Agar permasalahan dalam penelitian ini tidak terlalu luas dan menyimpang dari topic yang ada, maka diperlukan batasan masalah sebagai berikut :

1. *File* yang dapat dienkripsi adalah citra digital dengan format jpg dan bmp.
2. Pada sistem keamanan yang akan dibangun menggunakan metode *Vigenere cipher*.
3. Sistem dibangun menggunakan bahasa pemrograman *VB.Net*.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penelitian ini adalah :

1. Mengimplementasikan kriptografi keamanan data berupa citra digital dengan metode *vigenere cipher*.
2. Membangun aplikasi keamanan data berupa citra digital.
3. Mempermudah seseorang untuk mengamankan *file* citra digital dari ancaman pihak-pihak yang tidak diinginkan.

I.3.2. Manfaat

Adapun manfaat dari penelitian ini adalah :

1. Menjaga keamanan data yang dalam hal ini berbentuk citra digital dari orang yang tidak berhak, agar sesuai dengan *file* aslinya.
2. Mempermudah dalam transaksi yang membutuhkan keamanan terhadap keamanan *file* citra digital.

3. Memberikan keamanan/kerahasiaan pada citra digital yang telah dibuat.

I.4. Metodologi Penelitian

Peneliti melakukan beberapa cara dalam menyelesaikan masalah yang dihadapi untuk mengenkripsi citra digital diantaranya adalah :

1. Studi literatur dan pemahaman sistem

   Pengumpulan data dari buku, artikel dan karya ilmiah maupun situs internet mengenai kriptografi khususnya metode *vigenere cipher* dan pengolahan citra digital yang digunakan untuk penyelesaian masalah.

2. Perancangan sistem

   Melakukan analisis kebutuhan sistem, pengkodean, implementasi dan pengujian terhadap sistem yang dibangun terhadap data-data yang ada menggunakan bahasa pemrograman *VB.Net*.

4. Implementasi

   Pembuatan aplikasi kriptografi citra digital berdasarkan perancangan yang telah dibuat sebelumnya ke dalam program komputer.

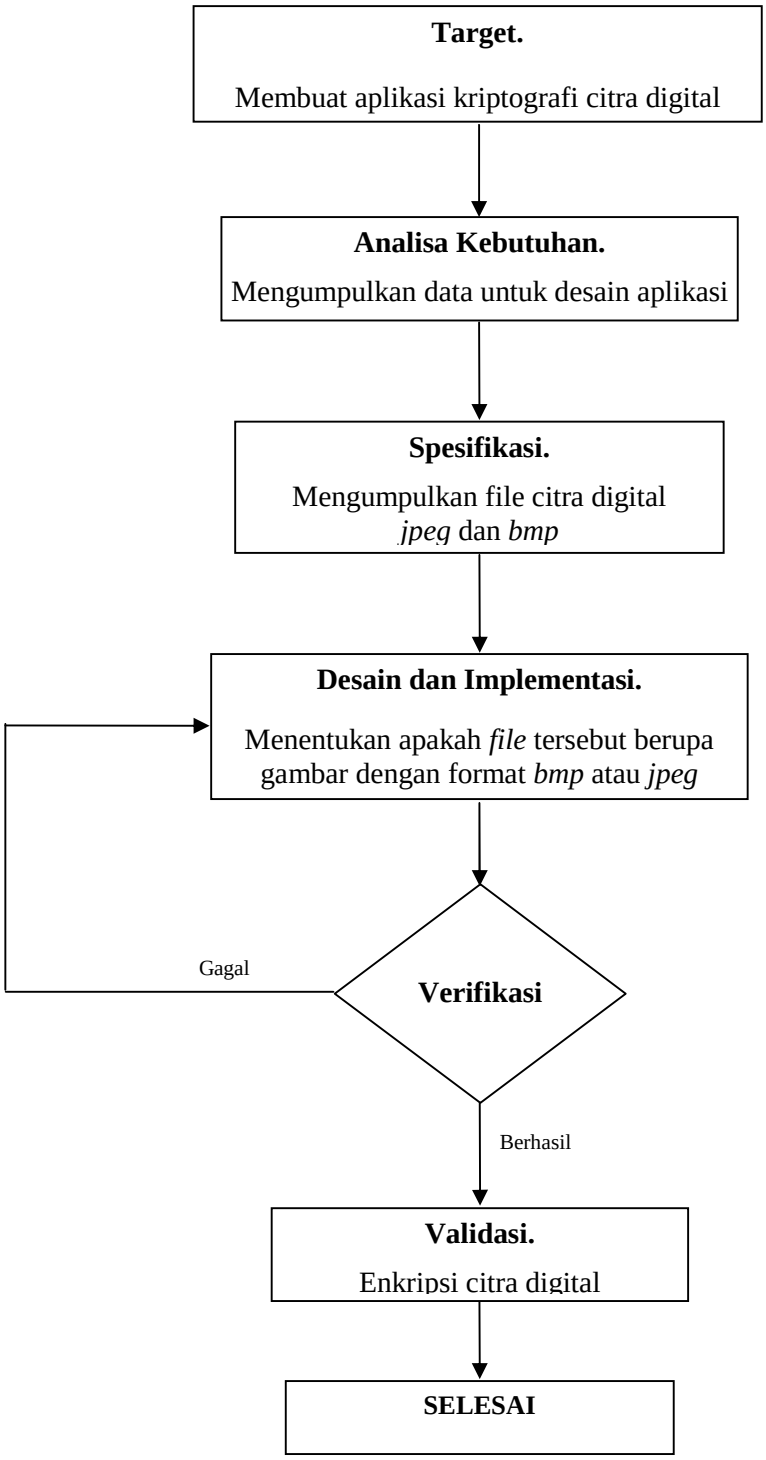
5. Uji coba sistem dan evaluasi.

   Tahap untuk menguji program yang telah dibuat untuk mencari kekurangan yang mungkin terdapat dalam program untuk pengembangan lebih lanjut.

I.4.1. Prosedur Perancangan

Perancangan aplikasi ini penulis melakuan beberapa tahap analisa, perencanaan, dan pengumpulan data. Pada tahap analisa penulis mempelajari metode *vigenere cipher* untuk penerapannya dalam bahasa pemrograman *VB.Net*, di tahap perencanaan penulis merancang desain dan merancang algoritma dari progam ataupun aplikasi ini dan penulis melakukan pengumpulan data melalui buku-buku di perpusatakaan dan Internet.

Berikut ini adalah langkah-langkah yang akan ditempuh oleh peneliti untuk mencapai tujuan perancangan yang dilakukan seperti yang terlihat pada gambar I.1 berikut :



Gambar I.1. Prosedur Perancangan

I.4.2. Analisis Kebutuhan

Kebutuhan-kebutuhan dalam pembuatan dan perancangan aplikasi ini yang dibutuhkan yaitu sebuah komputer yang bersistem operasi *Windows XP* dengan spesifikasi minimum *intel pentium* 2.8Ghz, memori 512Mb, bahasa pemrograman khususnya *VB.Net*.

I.4.3. Spesifikasi dan Desain

Pada tahap spesifikasi dan desain ini penulis akan mencoba menerangkan desain apa-apa saja yang diperlukan dalam pembuatan aplikasi ini. Pada tampilan awal terdapat 1 menu yang berfungsi sebagai *upload file.* Kemudian terdapat 2 menu enkripsi dan dekripsi, dimana berfungsi sesuai kebutuhan untuk apa yang akan dilakukan untuk mengenkripsi atau mendekripsi *file* citra yang berekstensi *jpeg* atau *bmp*. Setelah terdapat menu enkripsi dan dekripsi selanjutnya terdapat menu *save* dan *Load* untuk menyimpan atau mengambil *file* hasil dari enkripsi dan dekripsi.

I.4.4. Implementasi dan Verifikasi

Sebagai implementasi aplikasi, aplikasi ini dijalankan pada bahasa pemrograman *VB.Net*. Pada tahap pertama yang dilakuan adalah pemilihan *file* berekstensi *jpeg* atau *bmp* yg telah disediakan sebelumnya untuk di enkripsi atau di didekripsi. Selanjutnya *file* di *upload* terlebih dahulu ke dalam sistem dan sistem tersebut siap melakukan proses mengenkripsi atau mendekripsi *file jpeg* atau *bmp* tersebut ke bentuk yang tampak samar atau kembali ke keadaan semula.

I.4.5. Validasi

Untuk pengujian aplikasi ini penulis akan menjelaskan tentang alur dari program apakah program dapat bekerja dengan baik dan sesuai spesifikasi. Pada saat di halaman *upload file*, pilih *file* berbentuk *jpeg* atau *bmp* karena aplikasi ini hanya bisa dijalankan dengan *file* yang berekstensi *jpeg* atau *bmp* saat melakukan enkripsi atau dekripsi. Setelah di *upload* berikutnya tekan tombol enkripsi untuk melakukan enkripsi. Maka *file jpeg* atau *bmp* tersebut akan berubah menjadi *file jpeg* atau *bmp* dengan gambar akan menjadi samar dan tidak jelas.

I.4.6. Uji Coba Sistem

Melakukan uji coba sistem yang telah dibuat dengan menggunakan metode *black box*, melakukan perhitungan manual. Kemudian melakukan evaluasi terhadap kekurangan program dan memperbaikinya.

I.5. Sistematika Penulisan

Untuk memberikan gambaran isi laporan ini, penulis akan menguraikan susunan laporan secara garis besar yang terdiri dari lima bab, dimana setiap babnya akan dibagi menjadi beberapa sub bab. Sistematika penulisan ini dibuat tersusun dengan tujuan agar mudah dipahami oleh semua pihak. Adapun susunannya sebagai berikut :

BAB I PENDAHULUAN

Pendahuluan berisi tentang latar belakang, identifikasi masalah yang dihadapi, batasan masalah, maksud dan tujuan pembuatan aplikasi, kegunaan pembuatan aplikasi, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Meliputi uraian dari teori-teori yang akan digunakan sebagai dasar pada perencanaan dan pembuatan aplikasi tersebut.

BAB III ANALISA DAN DESAIN SISTEM

Pada bab ini memaparkan tentang perancangan aplikasi kriptografi citra digital menggunakan metode *vigenere cipher*.

BAB IV HASIL DAN UJICOBA

Pada bab ini berisi hasil dari ujicoba tersebut. Dan kelebihan dan kekurangan dari aplikasi kriptografi citra digital tersebut.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini penulis menyimpulkan mengenai pembuatan aplikasi yang telah dilakukan serta memberikan saran yang mungkin dijadikan sebagai bahan pertimbangan.