

BAB I

PENDAHULUAN

I.1. Latar Belakang

Di zaman era globalisasi, teknologi informasi dan komunikasi sudah sering digunakan dalam kehidupan sehari-hari, seperti internet, *e-commerce*, telepon bergerak dan ATM pada bank. Beberapa contoh tersebut merupakan aktivitas yang sangat memerlukan keamanan. Sehingga diperlukan sistem yang dapat mengamankan data ketika bertransaksi. Enkripsi adalah salah satu sistem yang dapat digunakan untuk mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.

Menampilkan enkripsi dan kebalikannya dekripsi, digunakan algoritma yang biasa disebut *cipher* dengan menggunakan metode serangkaian langkah yang terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah *encipherment*. Informasi yang asli disebut sebagai *plaintext*, dan bentuk yang sudah dienkripsi disebut sebagai *ciphertext*. Pesan *ciphertext* berisi seluruh informasi dari pesan *plaintext*, tetapi tidak dalam *format* yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekanisme yang tepat untuk melakukan dekripsi.

Ada banyak sekali variasi pada tipe enkripsi yang berbeda. Algoritma yang digunakan pada awal sejarah kriptografi sudah sangat berbeda dengan metode *modern*, dan *cipher modern* dan diklasifikasikan berdasar pada bagaimana *cipher* tersebut beroperasi dan *cipher* tersebut menggunakan sebuah atau dua buah

kunci. Sejarah *cipher* pena dan kertas pada waktu lampau sering disebut sebagai *cipher klasik*. *Cipher klasik* termasuk juga *cipher* pengganti dan *cipher transposisi*.

Berdasarkan latar belakang diatas maka penulis berinisiatif mengambil judul **“Perancangan Aplikasi Enkripsi Gambar Menggunakan Algoritma Transposisi**

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

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

1. Bagaimana cara mengenkripsi gambar sehingga *file* gambar akan terlihat samar setelah di enkripsi ?
2. Bagaimana cara mengenkripsi *file* gambar menggunakan algoritma transposisi?

I.2.2. Perumusan Masalah

Berdasarkan identifikasi masalah diatas, dapat dirumuskan beberapa masalah yaitu :

1. Sistem enkripsi gambar yang dapat mengenkripsi gambar sehingga *file* gambar akan terlihat samar setelah dienkripsi.
2. Sistem keamanan *file* gambar menggunakan algoritma transposisi.

I.2.3 Batasan Masalah

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

1. *File* yang dapat dienkripsi adalah gambar yang dengan format *jpg* dan *bmp*.
2. Bentuk gambar setelah dienkripsi adalah gambar terlihat samar dan tidak jelas.
3. Menggunakan bahasa pemrograman *VB.Net*.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari judul ini adalah:

1. Untuk merahasiakan *file* gambar dari orang yang *plagiator*
2. Untuk membantu pengguna dalam mengamankan data
3. Untuk mengetahui sistem enkripsi dan dekripsi khususnya gambar.

I.3.2. Manfaat

Adapun manfaat dari penelitian ini adalah:

1. Menjaga keamanan informasi yang dalam hal ini berbentuk gambar dari orang yang tidak berhak.
2. Aplikasi ini dapat digunakan untuk kepentingan pribadi maupun umum.
3. Mempermudah transaksi yang membutuhkan keamanan terhadap keamanan gambar.

I.4 Metodologi Penelitian

Dalam mengerjakan pembuatan aplikasi ini penulis hanya menggunakan metode *literatur* yaitu mengumpulkan data yang dipergunakan untuk memperoleh data secara teoritis dengan mempelajari buku-buku, catatan kuliah, dan buku referensi yang lain yang berkaitan erat dengan judul penulis.

a. Prosedur Perancangan

Perancangan aplikasi ini penulis melakukan beberapa tahap analisa, perencanaan, dan pengumpulan data. Pada tahap analisa penulis mempelajari algoritma transposisi untuk penerapannya di bahasa *VB.Net*, di tahap perencanaan penulis merancang desain dan merancang algoritma dari program ataupun aplikasi ini dan penulis melakukan pengumpulan data melalui buku-buku di perpustakaan dan *Internet*.

b. 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*, *VB.net*.

c. 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 empat menu tombol yaitu tombol buka *file*, tombol enkripsi, tombol dekripsi dan tombol tutup dimana berfungsi sesuai kebutuhan untuk apa yang akan dilakukan seorang *user* apakah dia ingin mengenkripsi

file gambar atau mendekripsikannya. Setelah memilih salah satu menu maka *user* akan dihadapkan pada halaman *browse file* untuk memilih *file* gambar yang akan dienkripsi atau dekripsi. Lalu pilih *list file* yang akan di *upload*. Setelah dipilih akan tampil halaman untuk mengenkripsi *file* dan tombol enkripsi untuk mengenkripsi *file* tersebut.

d. Implementasi dan Verifikasi

Sebagai implementasi aplikasi, aplikasi ini dijalankan pada *VB.Net*. Pada tahap pertama yang dilakukan adalah pemilihan *file* berekstensi *bmp* yang telah disediakan sebelumnya untuk di enkripsi atau di didekripsi. Selanjutnya *file* yang telah tampil di *form*, kemudian tekan tombol enkripsi maka *file* gambar tersebut telah terenkripsi. Setelah terenkripsi *file* gambar tersebut dapat disimpan ke folder tertentu.

e. Validasi

Untuk pengujian program ini penulis akan menjelaskan tentang alur dari program apakah program dapat bekerja dengan baik dan sesuai spesifikasi. Pada saat di *form* tampil *file* gambar, pilih *file* gambar, saat di *upload* dan telah tersimpan maka pada perintah berikutnya tekan tombol enkripsi untuk melakukan enkripsi. Maka *file* gambar tadi setelah dienkripsi akan kelihatan menjadi samar.

I.5 Sistematika Penulisan

Sistematika penulisan ini terdiri dari 5 bab, dengan tujuan untuk mempermudah dalam pembahasan. Adapun sistematika penulisan tersebut adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi Latar Belakang Masalah, Tujuan Penulisan, Rumusan Masalah, Pembahasan Masalah, Metode Penelitian dan Sistematika Penulisan.

BAB II LANDASAN TEORI

Pada bab ini berisikan tentang teori-teori penunjang yang berkaitan dengan analisa dan perancangan keamanan bahan ajar dengan algoritma *mime base64* yang penulis buat yang membahas tentang algoritma base64 dan teori-teori pendukung lainnya.

BAB III ANALISIS DAN DESAIN SISTEM

Pada bab ini penulis menganalisa aplikasi keamanan bahan ajar yang sedang berjalan dan mendesain aplikasi keamanan bahan ajar dengan menjelaskan tentang diagram blok dan flowchart dari perancangan keamanan bahan ajar.

BAB IV HASIL DAN UJI COBA

Pada bab ini menjelaskan dan membahas hasil dari analisa dan perancangan keamanan bahan ajar dengan algoritma transposisi yang didapat dari hasil percobaan yang dilakukan oleh penulis selama beberapa kali.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi analisa dan kesimpulan atas pembahasan laporan penulisan dan kesimpulan mengenai analisa dan perancangan keamanan bahan ajar dengan algoritma transposisi, kemudian penulis juga akan memberikan saran-saran sebagai acuan pengembangan lebih lanjut.