BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi 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. Karena banyak kemudahan yang di tawarkan, teknologi informasi tidak dapat lepas dari berbagai aspek kehidupan manusia, yang memungkinkan dapat berkomunikasi dan saling bertukar informasi atau data.

Seiring dengan kemajuan teknologi informasi maka sangat di perlukan sebuah keamanan data terhadap kerahasiaan informasi yang saling di pertukarkan, apa lagi jika data tersebut dalam suatu jaringan komputer yang terhubung/terkoneksi dengan jaringan lain. Hal tersebut tentu saja menimbulkan resiko bila informasi yang sensitif dan berharga tersebut di akses oleh orang yang tidak bertanggung jawab. Yang mana jika hal tersebut sampai terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang akan mengirim pesan, maupun organisasinya. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu data yang di bajak tersebut kemungkinan rusak atau hilang yang menimbulkan kerugian material yang besar.

Algoritma kriptografi klasik dibagi menjadi dua jenis yakni algoritma substitusi dan algoritma transposisi. Sesuai namanya, algoritma substitusi

menyembunyikan isi pesan/dokumen dengan cara mengganti karakter-karakter yang menyusun pesan/dokumen tersebut, menurut aturan tertentu. Variasi aturan substitusi ini melahirkan berbagai jenis algoritma spesifik, yang biasanya dinamai menurut penemunya.

Beberapa contoh algoritma substitusi diantaranya Algoritma *Caesar*, Algoritma *Vigenere*, dan Algoritma *Affine*. Namun, biasanya yang lebih sering dipakai sebagai sebutan bukanlah algoritmanya melainkan hasil dari algoritma kriptografi tersebut yakni *Cipher* (pesan yang telah tersandikan). Jadi, contoh-contoh sebelumnya akan diacu sebagai *Caesar Cipher*, *Vigenere Cipher*, dan *Affine Cipher*.

Jenis algoritma kriptografi klasik yang kedua ialah algoritma berbasis transposisi. Cara kerja algoritma ini ialah dengan mengubah susunan/urutan karakter-karakter di dalam dokumen. Pada umumnya hal ini dilakukan dengan cara menuliskan plainteks dengan pola tertentu, kemudian dibaca menggunakan pola / aturan yang berbeda sehingga dihasilkan suatu cipherteks.

Contoh teknik transposisi yang cukup populer dalam sejarah kriptografi adalah *scytale* yang berasal dari zaman Romawi Kuno. *Scytale* ialah sebuah silinder dengan diameter tertentu. Sebuah pita kertas dililitkan ke silinder tersebut, kemudian pesan ditulis ke pita dalam arah sejajar poros silinder. Pita kemudian diurai dari silinder sehingga huruf-huruf dalam pesan mengalami transposisi.

Oleh karena itu untuk menghindari agar hal tersebut tidak terjadi, penulis menggunakan algoritma kriptografi untuk proses enkripsi dan deskripsi data. Kriptografi telah menjadi suatu bagian yang tidak dapat di pisahkan dari sistem

keamanan jaringan. Salah satu metode enkripsi data adalah *Data Encryption Standard (DES)*. *Data Encryption Standard (DES)* merupakan algoritma *cipher* blok yang populer karena dijadikan standar algoritma enkripsi kunci-simetri. Dari latar belakang di atas penulis mencoba untuk membuat rancangan keamanan data dengan menggunakan algoritma kriptografi, dengan mengambil judul "**Perancangan Aplikasi Enkripsi Gambar dengan menggunakan Alogaritma Transposisi**".

I.2. Identifikasi Masalah

Berdasarkan penjelasan dari latar belakang diatas maka perumusan masalah yang akan di bahas adalah :

1. Bagaimana menganalisis data dengan menggunakan Aplikasi Enkripsi gambar dengan Alogaritma Transposisi.
2. Bagaimana merancang keamanan data dengan menggunakan Aplikasi Enkripsi gambar dengan Alogaritma Transposisi.

I.3. Rumusan Masalah

Dari latar belakang diatas dapatlah diambil rumusan masalah : Bagaimana membuat aplikasi enkripsi dengan menggunakan algoritma transposisi?

1.4. Batasan Masalah

Agar penelitian ini lebih terarah dan tidak menyimpang dari rumusan masalah yang ada, maka batasan masalah dari penelitian ini adalah :

1. Proses penyandian data meliputi proses enkripsi data menggunakan Aplikasi Enkripsi Gambar dengan Algoritma Transposisi.
2. Proses penyandian data meliputi proses deskripsi data menggunakan Aplikasi Enkripsi Gambar dengan Algoritma Transposisi

I.5. Tujuan dan Manfaat Penelitian

Sesuai dengan konsep yang ada, untuk menyelesaikan penelitian maka tujuan dari penelitian ini adalah :

1. Menganalisis keamanan data menggunakan algoritma transposisi
2. Merancang keamanan data menggunakan algoritma transposisi.

Adapun manfaat dari penelitian ini adalah :

1. Dapat menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya.
2. Mengetahui proses enkripsi dan deskripsi didalam pengamanan dan kerahasiaan keamanan data menggunakan kriptografi *Data Encryption Standard (DES)*.

I.6. Metodologi Penelitian

1. Studi Pustaka dan Literatur

Pada tahap ini dilakukan pengumpulan informasi yang diperlukan untuk sistem alogaritma transposisi. Informasi dapat diperoleh dari literature, buku-buku dan internet.

2. Diskusi

Berupa konsultasi dengan dosen pembimbing dan rekan-rekan mahasiswa mengenai masalah yang dihadapi penulis selama menyelesaikan penelitian.

I.6.1. Sistem Yang Akan Dirancang.

1. Sistem yang dirancang adalah system Alogaritma Transposisi.
2. Sistem teknik dasar yang dirancang menghasilkan Perancangan Aplikasi Enkripsi Gambar dengan menggunakan Alogaritma Transposisi.

I.6.2. Pengujian/Uji Coba Sistem Yang Dibuat

Pada tahapan ini penulis akan menguji dan menilai hasil implementasi serta menguraikan kebutuhan minimum dari perangkat lunak yang dibangun baik software maupun hardware.

I.7. Sistematika Penulisan

Adapun penelitian ini berjudul "Perancangan Aplikasi Enkripsi Gambar dengan menggunakan Alogaritma Transposisi memiliki alur penyusunan sebagai berikut:

BAB I. PENDAHULUAN

Bagian pendahuluan ini berisi latar belakang pembuatan, permasalahan, pembatasan masalah, tujuan dan manfaat, metodologi, serta sistematika penulisan tugas akhir.

BAB II. DASAR TEORI

Bagian ini berisi tentang pembahasan mengenai pembuatan rancangan keamanan data dengan menggunakan algoritma kriptografi.

BAB III. ANALISA DAN PERANCANGAN SISTEM

Bagian ini berisi tentang analisa-analisa pendukung pembuatan sistem, rancangan-rancangan untuk membuat aplikasi ini termasuk diagram konteks dan flowchart program, serta perancangan antar muka program.

BAB IV. PEMBAHASAN DAN IMPLEMENTASI SISTEM

Bagian ini berisi penerapan atau implementasi rancangan yang dibuat, pembahasan aplikasi program, dan pembuatan dialog menu utama. Hasil pembuatan aplikasi diimplementasikan pada proses enkripsi dan diskripsi gambar. Setelah diuji kemudian dibahas juga tentang analisa hasil program.

BAB V. PENUTUP

Bagian ini berisi kesimpulan dari pembahasan yang dilakukan, yang tidak terlepas dari tujuan pembuatan aplikasi dan saran-saran untuk perbaikan aplikasi ini.