BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi yang semakin pesat telah mempengaruhi seluruh aspek kehidupan dan memberikan banyak sekali keuntungan. Selain itu ada juga aspek – aspek dari sisi negatif dari kemajuan sistem informasi tersebut. Pada dasarnya melakukan pengiriman data tanpa melakukan pengamanan pada konten dari data yang dikirim, dapat menyebabkan adanya penyadapan pada jalur pengirimannya.

Salah satu teknik untuk pengamanan data adalah dengan Salah satu teknik untuk pengamanan data adalah dengan menggunakan algoritma penyandian data. Algoritma penyandian data saat ini semakin banyak jumlahnya, sejalan dengan berkembangnya ilmu yang mempelajari penyandian data tersebut. Ilmu ini biasa disebut Kriptografi. [1]

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut di kirim dan di terima oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih *authenticity*. Pesan, data, atau informasi akan tidak berguna lagi apabila di tengah jalan informasi itu di sadap atau di bajak oleh orang yang tidak berhak atau berkepentingan

Algoritma *One Time Pad* merupakan algoritma sederhana dan *unbreakable* yang sampai saat ini dinyatakan aman karena masih belum ada serangan yang benar-benar dapat mematahkan algoritma ini. Hal ini dikarenakan algoritma *One Time Pad* memiliki barisan kunci acak yang ditambahkan ke pesan *plaintext* yang tidak acak untuk menghasilkan *chipertext* yang seluruhnya acak.[2]

Data penting yang berformat .txt seperti berkas teks biasa, skrip, kode sumber program (*source code* program), berkas konfigurasi atau gambar (ASCII art) mudah sekali untuk disadap ketika proses pengiriman dikarenakan tidak adanya sistem untuk penyandian berkas tersebut. Untuk data berformat .doc dapat disandikan menggunakan *password* karena *Miscrosoft Word* memiliki fitur enkripsi. Namun fitur enkripsi *Miscrosoft Word* tersebut memiliki kelemahan yaitu adanya aplikasi yang dapat digunakan untuk membobol file yang telah terenkripsi.[3]

Algoritma *Scytale* Merupakan salah satu algoritma tradisional, yang menggunakan media perkamen atau kain yang dililitkan ke sebuah batang atau stik kayu. Digunakan untuk mengirimkan pesan yang terenkripsi. Harus diketahui besarnya keliling dari batang atau stik kayu yang menjadi media penulisan untuk dijadikan acuan proses enkripsi. Proses enkripsi dimulai dengan melilitkan media tulis pada batang, dan kemudian menuliskan pesan asli baris demi baris secara mendatar. Ketika lilitan media tulis dilepaskan dari batang, maka akan didapatkan hasil enkripsi [5].

Berdasarkan uraian di atas, penulis tertarik untuk mengajuka skripsi yang berjudul :

Implementasi Enkripsi dan Dekripsi Dokumen Menggunakan Metode *One Time Pad* Dan Metode *Scytale.*

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berdasarka dari latar belakang masalah yang telah dikemukakan , maka dapat di identifikasi hal-hal sebagai berikut :

1. Isi file dokumen tidak memiliki keamanan yang baik.
2. Dibutuhkan sebuah metode yang dapat mengabungkan isi file dokumen.
3. Dibutuhkan membangun aplikasi Implementasi Enkripsi dan Dekripsi Dokumen Menggunakan Metode *One Time Pad* Dan Metode *Scytale.*

I.2.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka yang menjadi rumusan masalah adalah sebagai berikut :

1. Bagaimana mengamankan isi file dokumen ?
2. Bagaimana menerapkan metode *One Time Pad* (OTP) dan *Scytale* untuk mengamankan isi file dokumen?
3. Bagaimana membangun aplikasi Implementasi Enkripsi dan Dekripsi Dokumen Menggunakan Metode *One Time Pad* Dan Metode Scytale?

I.2.3. Batasan masalah

Batasan masalah yang penulis kemukakan dalam sistem ini adalah:

1. Data yang di kemukakan berupa data file yang di enkripsi/deskripsi dalam bentuk *Text*.
2. Metode dan Algoritma yang di gunakan adalah *One Time Pad* Dan Metode *Scytale.*
3. Bahasa Pemrograman *Visual Basic*.

I.3. Manfaat dan Tujuan Penelitian

I.3.1. Manfaat Penelitian

1. Memahami mengenai pengamanan isi file dokumen.
2. Memahami penerapan metode *One Time Pad* dan *Scytale* untuk mengamankan isi file dokumen.
3. Mendapat wawasan pembuatanperangkat lunak keamanan file.

I.3.2. Tujuan Penelitian

1. Mengamankan isi file dokumen .
2. Menerapkan metode *One Time Pad* (OTP) dan *Scytale* untuk mengamankan isi file dokumen.
3. Membangun aplikasi Implementasi Enkripsi dan Dekripsi Dokumen Menggunakan Metode *One Time Pad* Dan Metode *Scytale.*

I.4. Metodologi Penelitian

1. Studi Literatur

Untuk dapat memperoleh kunci private maka dilakukan proses algoritma enkripsi kunci sesi yang di *input*-kan oleh *user*. Mengenal prinsip enkripsi dan dekripsi sebagai pengetahuan dasar untuk memecahkan masalah. Mengenal dan memahami Algoritma *One Time Pad* dan proses kerjanya. Mengenal dan memahami Metode *Scytale* dan proses kerjanya.

2. Analisis Sistem

Pada perancangan ini dilakukan dalam dua proses, yaitu proses enkripsi dan dekripsi. Kedua proses sama-sama melalui pemrosesan file sebelum melakukan enkripsi dan dekripsi. Setelah melakukan proses enkripsi, perlu dilakukan proses dekripsi yaitu proses pengembalian file dalam bentuk file awal dan kunci awal. Dekripsi juga bertujuan sebagai proses yang digunakan sebagai tolak ukur keberhasilan proses enkripsi. Membuat gambaran mengenai data dan proses serta kebutuhan sistem yang diperlukan dalam mengimplementasikan program.

3. Perancangan Sistem

Perancangan meliputi : desain *form – form* yang digunakan beserta tombol – tombol yang digunakan pada setiap *form*.

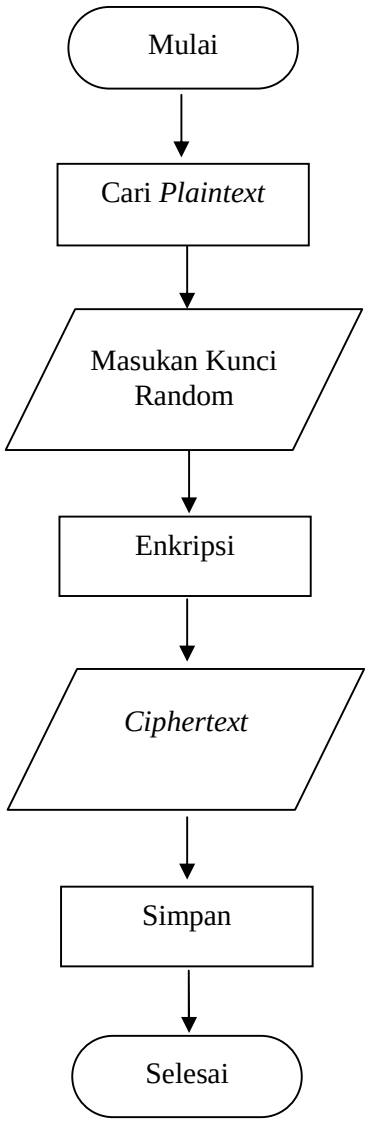
4. Pembuatan Program

Tahap ini adalah penerapan desain ke dalam bentuk program dengan memanfaatkan bahasa pemrograman yang ada, yaitu *Visual Basic*.

5. Uji Coba Program

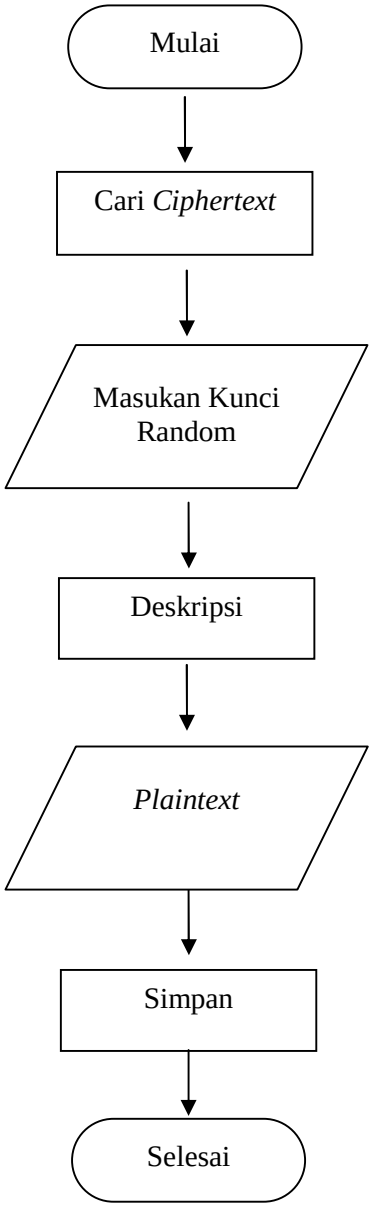
Menganalisis apakah program sesuai dengan algoritma yang digunakan dan dapat berjalan dengan baik untuk mengekripsi dan mendekripsi berkas dokumen (.txt,.doc).

Gambar I.1 adalah diagram alir dari sistem enkripsi yang dimulai dengan mencari *plaintext* berkas asli kemudian memasukkan kunci random setelah itu dilakukan proses enkripsi yang menghasilkan *ciphertext* lalu disimpan.



Gambar : I.1 Diagram Alir Enkripsi

Gambar I.2 adalah diagram alir dari sistem dekripsi yang dimulai dengan mencari *chipertext* kemudian memasukkan kunci random setelah itu dilakukan proses dekripsi yang menghasilkan *plaintext* lalu disimpan.



Gambar : I.2 Diagram Alir Deskripsi

I.5. Sistematika Penulisan

BAB I : PENDAHULUAN

Berisi latar belakang masalah, rumusan masalah, tujuan penulisan, batasan masalah, metodologi penulisan, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Berisi tentang pengertian kriptografi, algoritma kriptografi, algoritma *One Time Pad* dan *Scytale.*

BAB III : ANALISIS DAN PERANCANGAN

Berisi tentang perancangan sistem berupa diagram alir enkripsi dan dekripsi menggunakan Algoritma *One Time Pad*. Bab ini juga berisi tentang rancangan desain *user interface,* serta dukungan *hardware* dan *software* terhadap program yang telah dibuat.

BAB IV : ANALISIS DAN PERANCANGAN

Berisi tentang cara kerja untuk melakukan enkripsi dekripsi dokumen menggunakan algoritma *One Time Pad* dan *Scytale*.

BAB V : ANALISIS DAN PERANCANGAN

Berisi tentang kesimpulan atas analisa dan saran berdasarkan hasil yang telah dilaksanakan.