BAB I

PENDAHULUAN

I.1. Latar Belakang

Semakin berkembangnya teknologi khususnya di bidang informasi yang memungkinkan setiap orang untuk dapat berkomunikasi dan saling bertukar data. Dengan kemajuan teknologi maka diperlukan sebuah pengamanan terhadap kerahasiaan sebuah informasi dalam proses pertukaran data. Dalam hal ini komunikasi atau pertukaran data yang menggunakan layanan media jaringan local atau sering disebut LAN (*local area network*) maupun WLAN (*wireless local area network*). Dengan menggunakan media jaringan komputer lokal pengguna dapat berbagi atau bertukar data antara satu pengguna dengan pengguna lain dalam satu jaringan yang terhubung. Di dalam dunia informatika dikenal dengan cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau lebih dikenal dengan istilah Kriptografi.

Di dalam keamanan jaringan komputer khususnya jaringan komputer lokal baik LAN maupun WLAN, memungkinkan untuk berbagi dan transfer *document* penting dengan user yang lainnya. Maka untuk mengamankan dokumen atau data yang bersifat penting dan mengatasi hal – hal diatas diperlukannya sebuah cara untuk mengamankan suatu data atau informasi dengan menggunakan teknik kriptografi. Saat ini sudah banyak berkembang algoritma kriptografi yang mendukung untuk mengamankan suatu data atau informasi yang ada dari orang atau pihak yang tidak berhak untuk mengakses data atau informasi tersebut.

RC4 merupakan jenis aliran kode yang berarti operasi enkripsinya dilakukan per karakter 1 *byte* untuk sekali operasi. Algoritma kriptografi *Rivest Code* 4 (*RC4*) merupakan salah satu algoritma kunci simetris dibuat oleh *RSA* Data *Security Inc* (*RSADSI*) yang berbentuk stream *chipper*. Algoritma ini ditemukan pada tahun 1987 oleh *Ronald Rivest* dan menjadi simbol keamanan *RSA* (merupakan singkatan dari tiga nama penemu : *Rivest, Shamir*, dan *Adleman*).

Penulis mencoba untuk membangun sebuah aplikasi yang dapat mengamankan data *file* dengan algoritma kriptografi *Rivest's Chipper 4*. Seperti dengan latar belakang yang dijelaskan sebelumnya, penelitian dalam perancangan ini diberi judul "**Perancangan Aplikasi Transfer Data *File* Pada Jaringan Wifi Dengan Menggunakan Algoritma *Rivest Chipper* 4.**".

I.2. Ruang Lingkup Permasalahan

Ruang lingkup permasalahan merupakan penjelasan mengenai hasil analisa penelitian yang akan dilakukan, yang terdiri dari identifikasi masalah, rumusan masalah dan batasan masalah yang akan menjadi objek penelitian.

1.2.1 Identifikasi Masalah

Penulis mengidentifikasikan permasalahan yang ditemukan dalam perancangan ini adalah sebagai berikut :

1. Sangat mudahnya penyalinan data oleh pihak yang tidak berhak karena tidak memiliki keamanan data, dapat membuat data pribadi dari pengguna lain dapat mudah diambil oleh siapa saja.

2. Tidak ada penerapan sistem pengamanan data di dalam mengakses *file* dalam proses transfer melalui jaringan komputer lokal.
3. Masih sedikitnya aplikasi yang mendukung pengamanan data *file* yang diimplementasikan dalam proses transfer pada jaringan komputer.

1.2.2 Rumusan Masalah

Penelitian dan perancangan untuk pembuatan skripsi ini diperlukan perumusan masalah, yaitu sebagai berikut :

1. Bagaimana mengimplementasikan keamanan data pada *file*?
2. Bagaimana membuat kemanan dalam transfer *file* data dalam jaringan komputer lokal?
3. Bagaimana membangun aplikasi yang dapat dengan mudah digunakan oleh pengguna dengan penerapan algoritma *Rivest's Chipper 4*?

1.2.3 Batasan Masalah

Batasan masalah dibuat agar pembahasan terfokus dalam penulisan skripsi ini, adapun batasan masalah tersebut yaitu :

1. Merancang sebuah aplikasi yang dapat melakukan pengamanan data dalam transfer *file* pada jaringan lokal.
2. Akses data dengan enkripsi dan dekripsi *file* untuk pengamanan.
3. Implementasi kemanan data *file* menggunakan algorimta *Rivest's Chipper 4*, pemrograman yang digunakan adalah *Visual Studio* 2010, dengan koneksi jaringan lokal komputer.
4. Menggunakan sistem operasi *Windows XP/Seven,*

I.3. Tujuan dan Manfaat Masalah

Dalam penulisan skripsi ini tidak lepas dari tujuan dan manfaat yang akan dicapai, yang dapat dijelaskan dibawah ini.

1.3.1 Tujuan Penelitian

Adapun tujuan dari penulisan skripsi ini adalah sebagai berikut:

1. Untuk menerapkan konsep kriptografi dalam proses pengamanan data khususnya *file* dalam transfer melalui jaringa komputer lokal LAN ataupun WLAN.
2. Untuk membuat sebuah aplikasi pengamanan data *file* dengan implementasi algoritma *Rivest's Chipper 4*.

1.3.2 Manfaat Penelitian

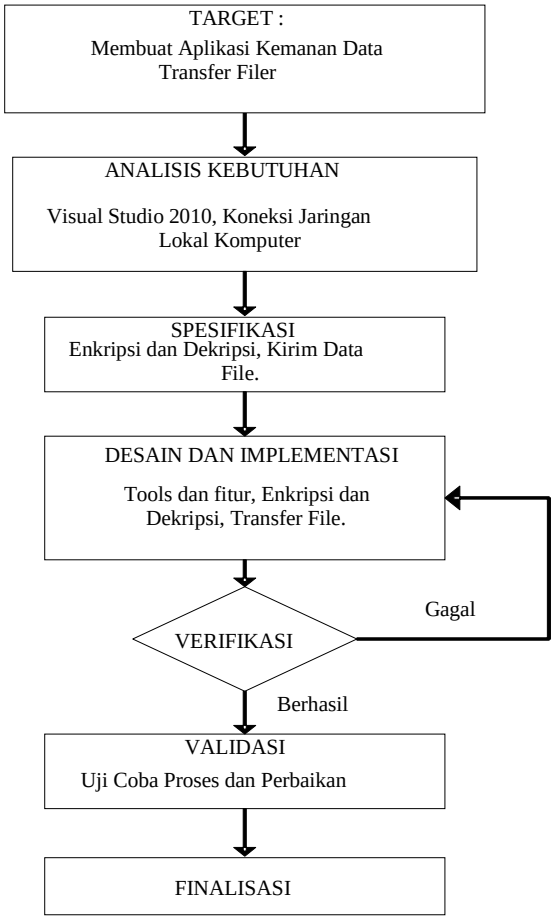
Adapun manfaat dari penulisan skripsi ini adalah sebagai berikut:

1. Memberikan kemudahan kepada pengguna untuk pengamanan data dalam proses transfer *file* dalam jaringan komputer lokal.
2. Menyajikan aplikasi yang dikhususkan untuk mengamankan data *file*. Dengan kemudahan enkripsi dan dekripsi dengan algoritma *Rivest's Chipper 4.*
3. Memahami bagaimana proses algoritma *Rivest's Chipper 4* dalam melakukan enkripsi dan deskripsi terhadap sebuah *file*.

I.4. Metodologi Penelitian

Tahapan-tahapan dalam melakukan penelitian ini dapat digambarkan sebagai berikut :

1. Penelitian ini bersifat teoritis, data yang diperoleh dari banyak sumber yaitu buku, jurnal, artikel yang berhubungan dengan implementasi algorimta *Rivest's Chipper 4* dan pengembangan aplikasi berbasis *Visual Studio* 2010 sebagai aplikasi transfer *file.*
2. Dalam proses perancangan terdiri dari beberapa prosedur yang dilakukan yaitu :
   a. Prosedur Perancangan, langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan dapat digambarkan seperti gambar I.1 dibawah ini.



Gambar I.1. Prosedur Perancangan

b. Analisis Kebutuhan, Menentukan kebutuhan apa yang diperlukan dalam perancangan, *tools* dalam perancangan dengan pemrograman *Visual Studio* 2010.
c. Spesifikasi dan Desain, spesifikasi hasil yang ditentukan adalah berbasis *client server* sehingga izin dan prosedur dapat ditentukan dalam penggunaan.
d. Implementasi dan Verifikasi, selanjutnya dilakukan pembuatan aplikasi dengan memanfaatkan masing-masing komponen. Untuk mengetahui apakah pemanfaatan masing-masing komponen sudah dapat bekerja dengan baik. Bila ada kesalahan atau kekurangan dapat diperbaiki.
e. Validasi, Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem.

I.5. Keaslian Penelitian

Satiap penelitian yang diadakan harus memiliki keaslian penelitian, untuk lebih jelasnya, berikut keaslian penelitian terdahulu dapat dilihat pada table I.1 berikut :

Tabel I.1. Keaslian Penelitian

No	Peneliti	Judul	Hasil	Perbedaan
1	Hanriyawan, (2004).	Enkripsi Data Menggunakan Algoritma RC4, Jurnal Elektro Politeknik Negeri Padang.	Hasil dari penyandian dengan menggunakan algoritma RC4 terlihat kuat yang terletak pada algoritma key.	Penggunaan algoritma RC4 menjadikan keamanan file yang dikirim dengan penerapan kriptografi.
2	Busran (2012)	Analisa komputasi enkripsi dan dekripsi data gambar, teks dan audio dengan menggunakan algoritma rc4 Berbasis visual basic 6.0	Dengan banyaknya file atau data yang dijalankan, maka proses enkripsi juga akan semakin lama.	Penyandian atau pengkodean terjadi setelah file dikirim dengan pemanfaatan jaringan Wifi.

I.6. Sistematika Penulisan

Susunan dan sistematika penulisan tugas akhir ini terdiri dari beberapa sub bab dapat dilihat sebagai berikut.

BAB I : PENDAHULUAN

Pada bab ini secara ringkas diterangkan mengenai latar belakang, identifikasi masalah, batasan masalah, tujuan penelitian dan manfaat penelitian, metodologi penyelesaian masalah, serta sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Sub bab ini tentang teori yang berkaitan dengan pembuatan, desain dan tampilan rancangan aplikasi transfer *file* dengan pengamanan algoritma *RC4*.

BAB III : ANALISA DAN PERANCANGAN PROGRAM

Berisi tentang analisa dan perancangan aplikasi, yang meliputi analisa masalah, perancangan *interface*, perangkat yang digunakan, metode serta ketentuan penggunaan.

BAB IV : HASIL DAN PEMBAHASAN

Berisi tentang tampilan hasil impelentasi program, beserta pembahasannya, serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini diuraikan kesimpulan dan saran yang dapat diberikan untuk pengembangan aplikasi yang dirancang.