BAB I

PENDAHULUAN

I.1. Latar Belakang

Pemakaian teknologi komputer sebagai salah satu aplikasi dari teknologi informasi sudah menjadi suatu kebutuhan, karena banyak pekerjaan yang dapat diselesaikan dengan cepat, akurat, dan efisien. Dengan berkembangnya teknik telekomunikasi dan sistem pengolahan data yang berkaitan erat dengan komunikasi antar pengguna komputer yang satu dengan komputer yang lain yang berfungsi untuk menyalurkan data sehingga masalah keamanan merupakan salah satu aspek penting. Akhirnya orang-orang pun mengembangkan berbagai cara untuk mengatasi persoalan keamanan data yang pada intinya adalah bagaimana agar orang yang tidak berhak, tidak dapat membaca atau bahkan merusak data yang bukan ditujukan kepadanya. Permasalahan umum yang terjadi selama ini adalah kurangnya kesadaran dari user untuk mengamankan data-data yang dimilikinya baik itu data yang bersifat rahasia dan penting maupun yang yang sifatnya tidak terlalu penting, sehingga memungkinkan untuk orang lain mengambil data.

Dalam komunikasi data, terdapat sebuah metode pengamanan data yang dikenal dengan nama kriptografi. Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data, serta keaslian pengiriman. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum tidak dapat diketahui atau dimanfaatkan oleh orang yang tidak berkepentingan atau yang tidak berhak

menerimanya. Metode kriptografi yang dapat digunakan untuk mengamankan data ada bermacam-macam. Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Namun, yang menjadi permasalahan dalam memilih metode kriptografi yang cocok adalah bagaimana mengetahui dan memahami cara kerja dari metode kriptografi tersebut. Dalam proses komunikasi data, walaupun data telah dienkripsi kemungkinan data tersebut dapat diketahui oleh orang lain. Salah satu kemungkinan tersebut adalah orang tersebut menyadap media komunikasi yang digunakan oleh kedua orang yang sedang berkomunikasi. Hal ini adalah merupakan masalah yang utama bagi setiap user dalam mengamankan data-datanya. Maka untuk menghindari hal-hal tersebut maka perlu pengamanan data. Salah satunya dengan menggunakan kriptografi baik itu dengan sifat klasik maupun modern.

Berdasarkan latar belakang tersebut maka penulis akan mengangkat sebuah judul **"Aplikasi Keamanan Folder Menggunakan Kriptografi Dengan *Algoritma One Time Pad* (OTP)".**

1.2. Ruang Lingkup Permasalahan

1.2.1. Idenifikasi Masalah

1. Rentannya sistem keamanan data, sehingga perlu dicari pemecahannya. Pemecahan masalah ini dapat dipecahkan dengan menggunakan suatu metode yaitu metode enkripsi dengan menggunakan algoritma kriptografi *one time pad*.
2. Banyaknya penyusup didalam jaringan komunikasi data, mengakibatkan penggunaan password saja menjadi kurang efektif dalam proses pengamanan

folder(termasuk isi keseluruhan) karena mudahnya untuk ditembus dengan waktu yang relatif singkat.

3. Adanya pihak yang tidak berhak untuk mengetahui privasi atau kerahasiaan data.

I.2.2. Rumusan Masalah

Berikut ini beberapa rumusan masalah tentang penelitian ini yang akan dicari penyelesaiannya antara lain:

1. Bagaimana cara merancang sebuah aplikasi pengamanan *folder* (isi folder) menggunakan algoritma *One Time Pad* ?
2. Bagaimana cara kerja metode algoritma *One Time Pad* untuk proses enkripsi dan dekripsi*?*
3. Bagaimana mengimplementasikan bahasa pemrograman Visual Basic dalam pembuatan aplikasi pengamanan *folder* dengan algoritma *One Time Pad?*

I.2.3. Batasan Masalah

Untuk menghindari kesimpangsiuran dalam penulisan skripsi ini serta karena keterbatasan waktu, biaya dan tenaga penulis, maka dari itu penulis membatasi masalah yang akan dibahas dalam skripsi ini diantaranya:

1. File yang akan dienkripsi kedalam program berupa isi keseluruhan didalam *folder*.
2. Proses enkripsi dan dekripsi yang digunakan adalah algoritma *One Time Pad*.
3. Menggunakan bahasa pemrograman Visual Studio 2010 dalam pembuatannya.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui kinerja perangkat lunak terhadap *folder* yang akan dienkripsi.
2. Untuk mengetahui dan menerapkan metode algoritma *One Time Pad* untuk pengamanan *folder*.
3. Untuk mengetahui proses enkripsi dan dekripsi *folder* dengan menggunakan algoritma *One Time Pad*.
4. Untuk keamanan dan kerahasiaan data /file agar tidak mudah untuk diakses pihak-pihak yang tidak berwenang.

I.3.2. Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Dapat menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya dalam hal proses enkripsi dan deskripsi didalam pengamanan dan kerahasiaan keamanan *folder* menggunakan kriptografi *One Time Pad* (OTP).
2. Dengan adanya sistem ini, proses pengamanan *folder* lebih aman dan terhindar dari pencurian data.
3. Sebagai dasar atau referensi dalam penerapan algoritma kriptografi *one time pad* untuk penelitian selanjutnya.

I.4. Metode Penelitian

Metode penelitian yang dipakai oleh penulis adalah metode penelitian deskriptif atau disebut juga metode penelitian analitis.

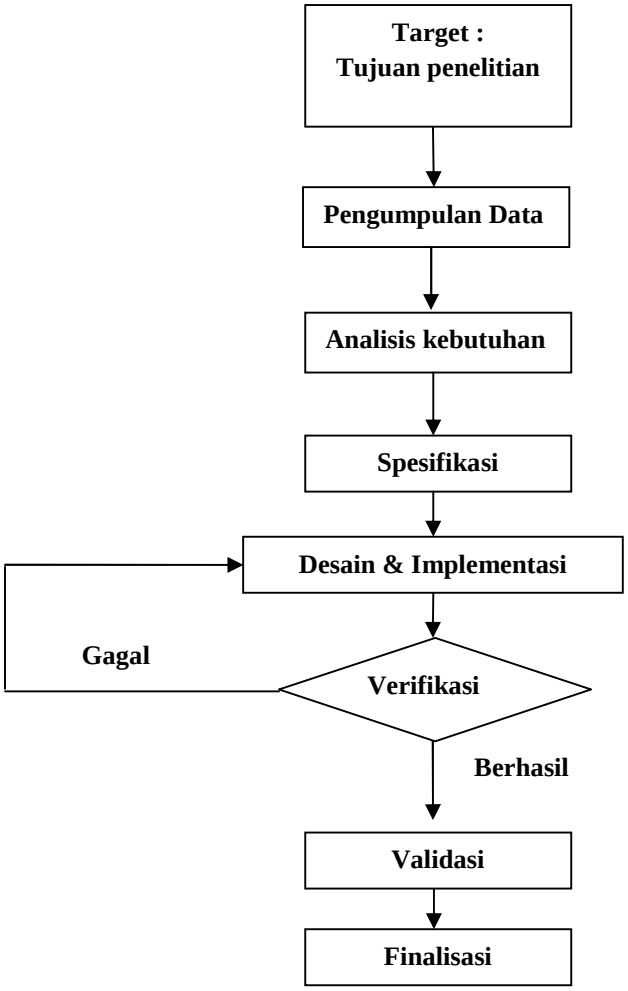
Dalam metode penelitian deskriptif ini digunakan teknik-teknik analisis, klasifikasi masalah, survei, studi kepustakaan terhadap masalah-masalah yang berhubungan dengan skripsi yang penulis susun, wawancara (*interview*) dengan narasumber, observasi, dan teknik *Test* terhadap objek penelitian yang telah ada.

Penulis menggunakan metode penelitian deskriptif dikarenakan pemecahan masalah yang aktual yaitu masalah yang berkembang pada bidang *artifisial intelligence* yang sekarang sedang berkembang pesat. Dengan metode deskriptif, aplikasi yang telah penulis kumpulkan mula-mula disusun, dijelaskan, dianalisis, dan kemudian diimplementasikan dalam sebuah perangkat lunak.

Dalam melaksanakan penelitian ini terdapat beberapa cara atau teknik yang penulis gunakan untuk menyelesaikan suatu masalah diantaranya diperoleh dengan cara sebagai berikut:

1. **Prosedur Rancangan.**

   Langkah – langkah yang diperlukan untuk mencapai tujuan perancangan, yaitu :



Gambar I.1. Prosedur Perancangan

2. Pengumpulan Data

Dalam metode penelitian deskriptif ini digunakan teknik-teknik analisis, klasifikasi masalah, survei, studi kepustakaan terhadap masalah-masalah yang berhubungan dengan skripsi yang penulis susun, wawancara (*interview*) dengan narasumber, observasi, dan teknik *Test* terhadap objek penelitian yang telah ada.

3. Analisis Kebutuhan

Untuk mencapai penyelesaian dalam merancang aplikasi ini adapun kebutuhan pokok yang diperlukan adalah:

a. *Hardware*

1) PC *(Personal Computer) / Laptop*

b. *Software*

1) *Visual Studio 2010*

4. Spesifikasi dan Desain

Spesifikasi minimum *hardware* dan *software* yang dibutuhkan untuk membangun aplikasi ini adalah:

a. Hardware

1) *Processor Core* i3 2,4 Ghz
2) *Harddisk* 500GB
3) *RAM* 2GB

b. Software

1) Sistem operasi PC : *Windows* 7
2) *Visual Studio 2010*

5. Implementasi dan Verifikasi

Setelah analisis dan perancangan, maka perlu dilakukan implementasi atau uji coba terhadap aplikasi yang telah selesai dibuat. Hal ini dilakukan untuk pengembangan atau perbaikan pada aplikasi tersebut apakah sudah bekerja sesuai dengan rancangan.

6. Validasi

Setelah melewati tahap implementasi dan verifikasi maka tahap selanjutnya adalah validasi. Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh. Dari validasi ini dapat diketahui kesesuaian hasil perancangan dengan analisis kebutuhan yang diharapkan.

7. Finalisasi

Pada tahapan ini adalah tahapan hasil dari aplikasi yang sudah dirancang dan berjalan sesuai rencana.

I.5. Keaslian Penelitian

Tabel I.1. Keaslian Penelitian

No.	Judul	Hasil Penelitian Terdahulu	Hasil Penelitian Penulis
1.	***Pembangunan Perangkat Lunak untuk Enkripsi Folder dengan Algoritma Serpent***	**1.** Pada enkripsi suatu file yang terdapat di dalam folder dirubah menjadi berekstensi *.dac. dengan menghapus folder aslinya lalu file di *hash* pada kunci yang dimasukkan **2.** ukuran folder semula dengan folder yang terenkripsi lebih besar setelah folder dienkripsi dengan algoritma *serpent*	**1.** Enkripsi yang dilakukan adalah dengan membuat suatu folder baru dengan berekstensi ._ENKRIPSI. Dengan folder semula tetap berada pada *diretory.* **2.** Ukuran folder semula dengan folder terenkripsi sama pada saat di enkripsi dengan algoritma *One Time Pad.*
2.	***Perangkat lunak pengamanan data menggunakan algoritma message digest-5 (md-5)***	**1.** Aplikasi yang dibuat dapat melakukan enkripsi folder dengan menggabungkan seluruh isi folder dengan di	**1.** Aplikasi yang diterapkan dengan mengubah susunan bit pada setiap file yang berada di dalam folder dengan kunci

		rubah menjadi satu file. **2.** Dalam perangkat lunak diperlukan suatu struktur header khusus yang selalu diakses ketika akan menambahkan (mengenkripsi) suatu file atau folder sehingga tidak perlu melakukan dekripsi terhadap keseluruhan isi folder.	yang di masukan. **2.** Dalam aplikasi tidak menyandikan header atau struktur file yang digunakan untuk pengamanan folder
3.	***Kombinasi Algoritma OTP Chiper dan Algoritma BBS dalam Pengamanan File***	**1.** Dapat melakukan pengamanan file teks. Dengan cara mem *parsing* isi file yang akan di enkripsi. **2.** Enkripsi pada algoritma BBS yang memfaktorkan n. Nilai n sebagai bilngan prima untuk perhitungan enkripsi.	**1.** Isi keseluruhan folder dapat di enkripsi dengan membuat perhitungan yang sama pada setiap file. **2.** Pada enkripsi Algoritma One Time Pad dengan perhitungan modulo 256.
4.	***Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web***	**1.** Memperlihatkan bahwa algoritma enkripsi ini dapat mengenkripsi citra dengan baik dan mendekripsinya kembali tepat sama seperti citra semula. **2.** Sistem chaos yang sensitif terhadap nilai awal memang memberikan keamanan yang bagus dari serangan exhaustive attack.	1. Pengembalian folder saat dekripsi sangat baik karena dengan perhitungan yang sangat rumit . 2. Sistem OTP memberikan nilai yang berdeda pada saat enkripsi serta memberikan keamanan yang sangat baik .

Berdasarkan dari kelima judul tersebut penulis akan mencoba untuk membandingkannya dengan yang akan dibahas oleh penulis.

1. Pada peneliti pertama membahas tentang enkripsi *folder* dengan algoritma serpent tetapi hanya file tertentu saja, sedangkan pada penelitian yang saya lakukan dapat mengenkripsi folder (isi file) dengan tidak ada batasan jenis file .
2. Pada peneliti kedua pengamanan data dengan MD-5 dan keseluruhan isi *folder* , penelitian yang penulis lakukan sama dengan penelitian yang ketiga tetapi yang membedakan adalah algoritma yang digunkan dan proses perhitungan nya.
3. Pada peneliti ketiga menggunakan metode yang sama dengan penulis tetapi dibandingkan dengan metode yang lain dalam pengamanan file, pada penelitian penulis lakukan menggunakan satu algoritma tanpa adanya kombinasi dengan algoritma lain.
4. Pada peneliti keempat menggunakan metode yang sama dengan penulis, namun hanya saja aplikasi yang digunakan untuk menyandikan file yang berupa teks sedangkan pada penelitian yang penulis lakukan dengan mengamankan isi keseluruhan data didalam folder.

I.6. Sistematika Penulisan

Langkah dan tahapan yang ditempuh dalam menyelesaikan penulisan ini adalah :

BAB I PENDAHULUAN

Dalam BAB ini di bahas mengenai Latar Belakang, Identifikasi Masalah, Batasan Masalah, Tujuan dan Manfaat Penelitian, Metodologi yang digunakan serta Sistematika Penulisan ini sendiri.

BAB II TINJAUAN PUSTAKA

Pada BAB ini dijelaskan teori-teori yang berkaitan dengan pembuatan, desain dan tampilan rancangan aplikasi enkripsi folder, serta teori-teori yang mendukung analisa penelitian.

BAB III ANALISIS DAN DESAIN SISTEM

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

BAB IV HASIL DAN PEMBAHASAN

Pada BAB ini berisikan tentang tampilan hasil, pembahasan, kelebihan dan kekurangan dari sistem yang dirancang.

BAB V KESIMPULAN DAN SARAN

BAB ini merupakan penutup dari penulis laporan Skripsi ini yang berisikan kesimpulan atas hasil analisa dan perancangan serta berisikan saran-saran.