BAB I
PENDAHULUAN

I.1. Latar Belakang

Pada saat ini, penyimpanan data menjadi sesuatu yang penting dalam berbagai kepentingan, baik bagi individu maupun suatu organisasi. Pada komputer seperti, *personal computer, laptop, netbook,* dan *smartphone,* data yang tersimpan berbentuk *file*. Data tersebut dapat diolah menjadi suatu informasi, yang belum tentu dapat diketahui semua pihak sehingga diperlukan suatu cara penyembunyian tertentu sehingga hanya dapat diketahui digunakan oleh pihak yang berhak saja dengan memanfaatkan kriptografi.

Pada umumnya, *file-file* yang dimiliki oleh pengguna disimpan dalam suatu wadah yang disebut dengan *folder*. Suatu *folder* dapat menampung banyak *file* dan *folder* sehingga membentuk struktur pohon. Untuk mendekripsi suatu *file* atau *folder* dalam yang berada dalam *folder* terenkripsi, perlu dilakukan pendekripsian pada seluruh isi dalam *folder* yang terenkripsi. Seringkali pengguna hanya ingin mendekripsi *file* saja dalam *folder* terenkripsi yang berukuran besar. Setelah melalui proses deskripsi, pengguna tersebut tidak hanya memperoleh *file* yang terdekripsi tetapi juga *file-file* lain yang tidak diperlukannya. Setelah didekripsi, seluruh isi *folder* tersebut harus dikembalikan dengan mengenkripsi kembali secara keseluruhan. Begitu pula jika ingin melakukan penambahan dan penghapusan *file* atau *folder* dalam *folder* terenkripsi.

Setiap aplikasi yang telah ada digunakan belum tentu menggunakan algoritma yang sama. Usaha untuk melakukan serangan kriptanalisis selalu ada.

Untuk mencegah serangan untuk kriptinalisis tertentu, diperlukan suatu algoritma yang dianggap masih aman dalam serangan kriptanalisis saat ini, yakni algoritma yang belum dilaporkan telah berhasil dipecahkan secara utuh.

Algoritma yang digunakan untuk membuat aplikasi pengenkripsi *folder* ini tentu saja dipilih berdasarkan belum adanya laporan serangan kriptanalisis yang berhasil memecahkan algoritma tersebut secara utuh. Acuan pemilihan algoritma adalah berdasarkan kandidat kompetisi AES yang lolos putaran kedua. Algoritma yang dipilih adalah algoritma *Serpent* karena diklaim lebih aman karena menggunakan 32 putaran meskipun akibatnya prosesnya menjadi lebih lambat. Maka dari itu, penelitian ini diangkat judul "**Perancangan Aplikasi Enkripsi Folder Menggunakan Algoritma Serpent**".

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah yang ada yaitu sebagai berikut:

1. Adanya pihak yang tidak berhak untuk mengetahui privasi atau kerahasian data.
2. Algoritma *serpent* digunakan untuk mengenkripsi *folder*.
3. Apakah dengan menggunakan algoritma *serpent* dapat mengamankan dan menjaga kerahasiaan data dalam *folder*.

I.2.2. Rumusan Masalah

Rumusan masalah yang dapat penulis ambil dari latar belakang yang telah diuraikan tersebut adalah:

1. Bagaimana merancang aplikasi keamanan data dalam *folder* dengan menggunakan algoritma *serpent*?
2. Bagaimana langkah-langkah untuk melakukan proses enkripsi pada algoritma *serpent*?
3. Bagaimana merancang sebuah keamanan data dalam *folder* menggunakan *Visual Basic .Net*?

I.2.3. Batasan Masalah

Batasan masalah yang penulis kemukakan dalam perancangan aplikasi enkripsi *folder* menggunakan algoritma *serpent* adalah:

1. Data yang dienkripsi hanya pada *folder* yang ditentukan.
2. Keluaran sistem yang ditargetkan pada penelitian ini yaitu file yang telah di enkripsikan dengan algoritma *serpent*.
3. Tidak membahas mengenai mekanisme pemecahan kunci sandi (kriptanalisis).
4. Bahasa pemrograman yang digunakan untuk membuat aplikasi yaitu *VB.Net*.
5. Kunci pada saat mengenkripsi sama dengan kunci pada saat dekripsi.
6. Ukuran *folder* yang dienkripsi maksimal 500 KB.
7. *Folder* tidak bisa kosong.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penulisan ini adalah:

1. Untuk merancang enkripsi *folder* menggunakan algoritma *serpent*.
2. Untuk mengetahui bagaimana cara kerja algoritma *serpent* dalam memberikan kerahasiaan data.
3. Untuk merancang keamanan *file* didalam *folder* menggunakan *Visual Basic .Net*.

I.3.2. Manfaat

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

1. Memberikan sebuah solusi untuk keamanan data didalam *folder* dengan menggunakan algoritma *serpent*.
2. Dapat menganalisis sejauh mana proses enkripsi dan dekripsi dapat diterapkan pada *folder* menggunakan algoritma *serpent*.
3. Agar data didalam *folder* dapat terjaga kerahasiannya.

I.4. Metodologi Penelitian

Berisi langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Adapun metodologi dalam pengumpulan data adalah sebagai berikut:

I.4.1. Analisis Tentang Sistem Yang Ada

1. Pengumpulan Data

   Yaitu mengumpulkan data dari buku, artikel dan karyah ilmiah maupun situs internet dan sumber lainnya yang menunjang dalam penulisan skripsi ini.

2. Pengujian dan analisis hasil

   Tahapan dimana penulis melakukan analisis terhadap cara kerja dari algoritma serta kekurangan dan kelebihan algoritma, setelah terlebih dahulu dilakukan uji coba terhadap algoritma tersebut dalam melakukan proses pengamanan data didalam *folder*.

3. Studi Kepustakaan (*Library Research)*

   Penulis melakukan studi pustaka untuk memperoleh data yang ada hubungannya dengan konsep keamanan data, *folder*, kriptografi, algoritma *serpent,* serta uraian teoritis bahasa pemrograman dengan *Visual Basic .Net*.

I.4.2 Prosedur Perancangan

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

a. Target/Tujuan Penelitian

   Target penelitian dilakukan untuk membuat suatu aplikasi untuk melakukan enkripsi pada suatu *folder* yang didalamnya berisi berupa *file-file* penting yang bersifat rahasia. Pada perancangan aplikasi enkripsi *folder* tersebut menggunakan algoritma *serpent.*

b. Analisis Kebutuhan

Analisis kebutuhan perangkat lunak merupakan awal dari siklus pengembangan perangkat lunak. Tahap analisis adalah tahapan pengumpulan kebutuhan dari semua elemen sistem perangkat lunak yang akan dibuat. Adapun analisis kebutuhan dalam rancangan sistem yang akan dibangun adalah sebagai berikut:

1. Data atau informasi apa yang akan diproses merupakan data langkah pembuatan aplikasi.
2. Program yang dirancang merupakan aplikasi menggunakan menggunakan algoritma *serpent*.

c. Spesifikasi Dan Desain

Spesifikasi kebutuhan perangkat lunak adalah sebuah dokumen yang berisi pernyataan lengkap dari apa yang dapat dilakukan oleh perangkat lunak, tanpa menjelaskan bagaimana hal tersebut dikerjakan oleh perangkat lunak. Adapun spesifikasi kebutuhan didalam membangun aplikasi yang akan dirancang adalah sebagai berikut:

a. Spesifikasi Perangkat Keras

Spesifikasi perangkat keras yang dibutuhkan yaitu:

i. *Processor ; Intel® core ™ i5-2430M*

ii. *Memory* DDR2 4 *GByte*

iii. *Harddisk* 500 *GByte*

b. Spesifikasi Perangkat Lunak

Adapun spesifikasi perangkat lunak yang dibutuhkan yaitu:

i. Sistem operasi *Windows xp/vista/7/8/8.1*

ii. *Microsoft Visual Studio 2010*

d. Implementasi dan Verifikasi

Implementasi merupakan tahap pengkodean yang merupakan suatu metode yang merupakan suatu proses translasi. Rancangan detil ditranslasikan ke dalam sutau bahasa pemrograman. Bahasa pemrograman adalah alat yang digunakan untuk komunikasi antara manusia dan komputer. Verifikasi program merupakan suatu metode yang digunakan untuk menjamin kebenaran suatu program. Metode ini mencegah terjadinya kesalahan dengan memberikan jaminan kebenaran berdasarkan komputasi matematis. Tentunya metode ini berbeda dengan testing yang menjamin program dengan mencari kebenaran dan kesalahan lewat sejumlah data sebagai masukan.

e. Validasi

Validasi merupakan proses untuk menunjukkan seberapa besar nilai keakuratan program terhadap kondisi-kondisi saat pemakaian sebenarnya. Proses ini menjalankan skenario berdasarkan data dan lingkungan yang merepresentasikan perangkat lunak yang telah selesai kedalam komputer pengguna.

f. Finalisasi

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

1.4.3 Pengujian / Uji coba sistem

Tahap ini merupakan tahap untuk indentifikasi kesalahan yang timbul setelah melakukan pengujian pada sistem perancangan yang telah dibuat. Setelah proses pengkodean selesai maka akan dilakukan proses pengujian terhadap program yang dihasilkan untuk mengetahui apakah program sudah berjalan dengan benar dan sesuai dengan perancangan yang dilakukan dan hasil/*output* sudah tepat dan akurat.

I.5. Keaslian Penelitian

Tabel dibawah ini merupakan perbandingan antara sistem yang lama dengan sistem yang baru:

Tabel I.1. Perbandingan Sistem Yang Lama dan Yang Akan Dirancang

No	Elemen Perbandingan	Sistem Yang Lama	Sistem Yang Dirancang
1	Dr. Ir. Rinaldi Munir, M.T, 2011	Aplikasi dibuat dengan memanfaatkan algoritma *Serpent* dengan antarmuka perangkat lunak mirip dengan Windows Explorer dalam menampilkan struktur *folder* berupa *tree* dan menampilkan isi *folder* yang diakses.	Aplikasi dibuat dengan memanfaatkan algoritma *Serpent* dengan antarmuka perangkat lunak berbasis desktop VB.Net tidak menampilkan isi struktrur *folder* secara detail.

I.6. Sistematika Penulisan

Sistematika penulisan skripsi ini dibagi menjadi lima bab yang merangkum tiap tahapan yang penulis lakukan, antara lain:

BAB I : PENDAHULUAN

Bab ini menjelaskan tentang Latar Belakang, Ruang Lingkup Permasalahan, Tujuan dan Manfaat, Metodologi Penelitian dan Sistematika Penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini dibahas mengenai teori-teori yang mendukung pembahasan bab selanjutnya, perancangan aplikasi untuk enkripsi folder dan perangkat-perangkat yang mendukungnya.

BAB III : ANALISIS DAN DESAIN SISTEM

Pada bab ini berisikan analisa permasalahan dan kebutuhan perancangan aplikasi, serta pemodelan sistem secara fungsional.

BAB IV : HASIL DAN UJI COBA

Bab ini berisikan tentang tampilan hasil yang dirancang, pembahasan uji coba dari sistem yang dirancang, dan kelebihan sistem yang dirancang serta kekurangannya.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisikan bagian penutup yang berisi kesimpulan untuk pemakai dari terbentuknya perancangan sistem aplikasi serta saran untuk pengembangan sistem aplikasi selanjutnya.