BAB I

PENDAHULUAN

I.1. Latar Belakang

Data file merupakan salah satu bentuk data atau informasi berbentuk visual. Di zaman ini pengiriman data atau informasi dapat dilakukan dengan berbagai cara dan siapa saja. Namun, tidak semua isi dari informasi yang ada bersifat publik. Ada pesan yang bersifat rahasia sehingga keasliannya harus terjaga dalam proses pengirimannya.

Beberapa pengiriman data saat ini telah memanfaatkan media komunikasi digital sebagai media penyimpanan. Kondisi tersebut selain memberikan pengaruh positif juga dapat memberikan pengaruh negatif yang berimbas pada sistem keamanan data, khususnya untuk data yang memuat beberapa informasi rahasia. Sehingga informasi tersebut menjadi sangat rentan untuk diketahui, diambil, dimanipulasi dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Untuk mengatasi permasalahan yang berhubungan dengan keamanan data maka diperlukan suatu metode atau sistem yang dapat menjaga keutuhan informasi dan rahasia pada suatu data, salah satunya dengan menggunakan metode kriptografi.

Kriptografi berasal dari kata *crypto* dan *graphia* . *Crypto* berarti rahasia dan *graphia* berarti tulisan. Sehingga, kriptografi pada dasarnya adalah ilmu untuk menjaga keamanan pesan ketika pesan dikirim dari satu tempat ke tempat yang
lain. Salah satu jenis dari kriptografi adalah algoritma simetris. Algoritma simetris merupakan algoritma kriptografi yang menggunakan kunci yang sama baik dalam proses dalam enkripsi dan dekripsi nya. Kelebihan dari algortima simetris adalah kecepatan proses nya lebih cepat dibandingkan dengan algoritma asimetris. Salah satu algoritma simetris adalah algoritma *blowfish.*

Blowfish merupakan Algoritma Kriptografi dengan penggunaan kunci pada blok *cipher* simetris (*symmetric block cipher*) yakni kunci yang digunakan pada proses *enkripsi*

sama dengan kunci yang digunakan pada proses *dekripsi* dengan data masukan dan keluaran berupa blok-blok data berukuran 64 *bit*. *Blowfish* dirancang oleh *Bruce Schneier* pada tahun 1993 yang ditujukan untuk mikroposesor besar (32 bit ke atas dengan *cache* data yang besar). Algoritma *Blowfish* ini akan di kombinasikan dengan algoritma Rijndael.

Dengan kriptografi maka data yang terenkripsi akan berubah menjadi data yang abstrak atau data yang acak yang tidak bisa dimengerti. Hal ini menimbulkan kecurigaan Ketika hendak melakukan pengiriman pesan. Maka dari itu data file tersebut agar tidak mudah diketahui menggunakan dua algoritma yang berbeda.

Berdasarkan latar belakang masalah diatas, maka penulis tertarik merancang suatu sistem keamanan data, dan mengambil judul **"*Pemanfaatan Kriptografi Algoritma Blowfish Kriptografi Algoritma Rijndael dalam Pengamanan Data File*".**

I.2. Ruang Lingkup Permasalahan

Permasalahan dalam suatu penelitian harus mempunyai ruang lingkup permasalahan yang terdiri dari Identifikasi masalah, Rumusan masalah, dan Batasan masalah. Oleh sebab itu penulis akan menjelaskan dibawah ini :

I.2.1 Identifikasi Masalah

Berdasarkan latar belakang yang telah dikemukakan, identifikasi masalahnya adalah sebagai berikut :

1. Mudahnya penyalinan data oleh pihak yang tidak berhak karena tidak memiliki keamanan data yang tersimpan.
2. Tidak ada pemanfaatan sistem pengamanan data *file* di suatu folder penyimpanan yang telah dibuat.

I.2.2 Rumusan Masalah

Berikut rumusan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini :

1. Bagaimana membuat sistem keamaan data *file* dengan dua algoritma yang berbeda ?
2. Bagaimana merancang kemanan data *file* dengan *Algoritma Blowfish dan Algoritma Rijndael.*

I.2.3 Batasan Masalah

Untuk menghindari penyimpangan pembahasan dari tujuan awal maka diperlukan batasan masalah dalam Skripsi ini adalah sebagai berikut :

1. Metode Kriptografi yang digunakan *Algoritma Blowfish dan Algoritma Rijndael.*
2. *File* yang digunakan untuk di *enkripsi* diantaranya (**.txt, *.doc, *.pdf, *.jpg, *.png, *.mp3, *.mp4).*
3. Bahasa pemograman yang digunakan adalah *Visual Basic.Net 2017.*

I.3 Tujuan Dan Manfaat

Dalam suatu perancangan terdapat tujuan dan manfaat yang harus dicapai, supaya nantinya menghasilkan output yang diinginkan oleh pengguna.

I.3.1 Tujuan Penelitian

Adapun tujuan yang diperoleh dari sistem yang akan dibangun ini adalah sebagai berikut :

1. Mengkontruksi Progam Aplikasi untuk mempermudah proses dari pemanfaatan Algoritma Blowfish dan Algoritma Rijndael.
2. Menerapakan Algoritma Blowfish dan Algoritma Rijndael Untuk menciptakan aplikasi keamanan data *file.*
3. menghasilkan sistem kolaborasi antara algoritma Blowfish dengan Algoritma Rijndael dan mengimplementasikan dengan bahasa pemrograman Vb.net.

I.3.2 Manfaat Penelitian

Adapun manfaat yang diperoleh dari sistem yang akan dibangun ini adalah sebagai berikut :

1. Pemilik data *file* dapat mengamankan sebuah data *file* dari orang-orang yang tidak bertanggung jawab .
2. Dapat memberikan pembelajaran dalam bentuk simulasi mengenai cara kerja algoritma *Blowfish dengan Algoritma Rijndael.*
3. Penulis memahami pemanfaatan dan penerapaan *Algoritma blowfish* dan *Algoritma Rijndael.*

I.4. Metode Penelitian

Metode merupakan suatu cara atau teknik yang sistematik untuk mengerjakan suatu kasus. Di dalam menyelesaikan skripsi ini penulis menggunakan 2 (dua) metode studi yaitu :

a. Studi Lapangan (*Field Research*)

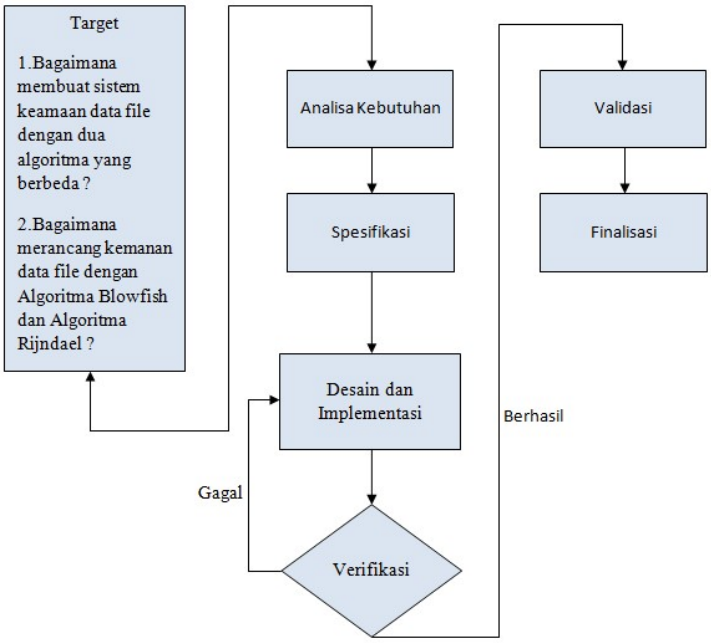
Merupakan metode yang dilakukan dengan mengumpulkan data. Adapun teknik pengumpulan data yang dilakukan penulis adalah dengan melakukan pengamatan (*observation*) yang merupakan salah satu metode pengumpulan data yang cukup efektif untuk mempelajari suatu sistem. Penulis melakukan pengamatan langsung terhadap kegiatan yang sedang berjalan.

b. Studi Kepustakaan (*Library Research*)

Penulis melakukan studi pustaka untuk memperoleh data-data yang berhubungan dengan penulisan skripsi dari berbagai sumber bacaan seperti: jurnal, internet, dan lain – lain.

I.4.1 Prosedur Perancangan

Tata cara dan langkah-langkah yang diperlukan untuk mencapai tujuan perancangan aplikasi, adalah sebagai berikut :



Gambar 1. Prosedur Perancangan

I.4.2 Analisa Kebutuhan

Sesuai penyelesaian masalah yang akan dilakukan, kebutuhan pokok yang harus ada, Mengimplemtasikan penggunakaan *VB.Net* dalam *Pemanfaatan Kriptografi Algoritma Blowfish Kriptografi Algoritma Rijndael dalam Pengamanan Data File*.

I.4.3 Spesifikasi dan Desain

Pada tahap ini, dilakukan spesifikasi dan desain perangkat lunak yang akan direalisasikan dalam perancangan sistem, yaitu sebagai berikut :

1. Desain Sistem

   Berisi spesifikasi alat yang dirancang, komponen, peralatan uji yang digunakan dan diagram blok peralatan yang akan dirancang.

   a. Desain

   - Pemodelan *UML* (*Unified Modeling Language*).

   b. Spesifikasi *Software*

   - *VB.net 2017.*

c. Spesifikasi *Hardware*

- *Intel Core i3.*
- *RAM* 4GB.
- *Hard Drive* 500 Gb.

d. Implementasi Sistem

- *VB.net 2017.*

I.4.4 Implementasi dan Verifikasi

Setelah jelas spesifikasi dan desain, selanjutnya dilakukan pembuatan aplikasi dengan memanfaatkan masing-masing komponen. Untuk mengetahui apakah pemanfaatan masing-masing komponen sudah dapat bekerja dengan baik perlu dilakukan verifikasi. Dengan demikian bila ada kesalahan atau kekurangan dapat diperbaiki terlebih dahulu sebelum dirangkai menjadi kesatuan aplikasi yang utuh dan siap pakai.

I.4.5 Pengujian Fungsional dan Ketahanan Sistem

Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem. Pengujian fungsional dilakukan untuk mengetahui bahwa aplikasi dapat bekerja dengan baik sesuai dengan prinsip kerjanya. Pengujian ketahanan berkaitan dengan kemampuan aplikasi untuk dapat berjalan pada sistem minimum yakni pada *PC* dengan *PC* dengan *Processor Core i3 3,7 Ghz, Memori 4GB*, Dari validasi ini dapat diketahui kesesuaian hasil perancangan dengan analisis kebutuhan yang diharapkan.

I.5. Kontribusi Penelitian

Terdapat beberapa kontribusi yang diberikan melalui penelitian yang sedang di laksanakan ini adalah berupa:

1. Menghasilkan sebuah penelitian yang mengharapkan penggunaan *Algoritma Blowfish* dan *Algoritma Rijndael* untuk mengamankan *file* dan mengembalikan *file* yang telah diproteksi ke dalam bentuk aslinya.
2. Aplikasi yang dihasilkan dari penelitian dapat digunakan sebagai media untuk pengamanan *file* yang berisi data-data rahasia sebelum dikirimkan ke yang bersangkutan.

I.6. Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini menguraikan latar belakang, identifikasi masalah, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian, serta sistematika penulisan skripsi.

BAB II TINJAUAN PUSTAKA

Bab ini dijelaskan teori-teori penujang yang digunakan sebagai dasar dalam proses perancangan dan pembuatan aplikasi, serta membahas tentang pengertian Kriptografi, Algoritma *Blowfish*, dan *Algoritma Rijndael*

BAB III ANALISIS DAN DESAIN SISTEM

Bab ini akan membahas tentang Perancangan Keamanan Kriptografi Dengan Menggunakan *Algoritma Blowfish* dan *Algoritma Rijndael* Untuk pengamanan data *File.*

BAB IV HASIL DAN UJI COBA

Bab ini akan membahas analisis hasil dan uji coba sistem yang akan penulis buat.

BAB V KESIMPULAN DAN SARAN

Bab ini menguraikan tentang kesimpulan, dan saran - saran dari hasil penelitian

yang penulis lakukan.