

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada jaman dewasa ini, teknologi telah semakin berkembang dibidang telekomunikasi dan informasi yang memungkinkan setiap orang untuk dapat berkomunikasi dengan jarak yang berjauhan. Dengan kemajuan teknologi maka diperlukan sebuah pengamanan terhadap kerahasiaan sebuah informasi dalam proses komunikasi yang terjadi. Dalam hal ini komunikasi atau pertukaran data yang menggunakan layanan dalam pengiriman file/data.

Salah satu dukungan yang ada untuk pengamanan atau penyandian file, dengan pemanfaatan algoritma yang sedang banyak digunakan pada saat ini, yaitu salah satunya algoritma Blowfish. Perancangan aplikasi layanan penyandian file telah banyak beredar, dimana file atau data yang kita simpan atau pun kita kirim di enkripsi menjadikan file di lindungi dengan penyandian atau pengkodean yang sudah dirancang. Saat ini masih banyaknya pihak-pihak yang dengan sengaja membuka file seseorang yang bisa dikatakan file pribadi yang dicoba untuk dibobol oleh orang yang tidak bertanggung jawab.

Di dalam keamanan komputer dikenal sebuah teknik kriptografi, yang difungsikan untuk penyandian pesan atau juga file. Masih kurangnya perhatian atas keamanan data atau file yang tanpa disadari dapat menyulitkan kita untuk Berdasarkan kepentingan dan kerahasiaan sebuah data diperlukannya sebuah cara untuk mengamankan suatu data atau file dengan menggunakan teknik kriptografi. Saat ini sudah banyak berkembang algoritma kriptografi yang mendukung untuk

mengamankan suatu pesan atau informasi yang ada dari orang atau pihak yang tidak berhak untuk mengakses data atau informasi tersebut.

Penulis mencoba untuk membangun sebuah aplikasi yang dapat mengamankan sebuah file dengan algoritma Blowfish. Seperti dengan latar belakang yang dijelaskan sebelumnya, penelitian dalam perancangan ini diberi judul “**Perancangan Aplikasi Layanan Penyandian File Dengan Implementasi Algoritma *Blowfish***”.

1.2. Ruang Lingkup Permasalahan

1.2.1. Identifikasi Masalah

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

1. Mudahnya penyalinan data oleh pihak yang tidak berhak karena tidak memiliki keamanan data yang tersimpan.
2. Tidak ada penerapan sistem pengamanan file teks di suatu folder penyimpanan yang telah dibuat.
3. Masih sedikitnya aplikasi yang mendukung pengamanan file yang diimplementasikan dengan pemrograman *PHP*.

1.2.2. Rumusan Masalah

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

1. Bagaimana merancang dan mengimplementasikan keamanan dalam penyandian file teks?

2. Bagaimana membangun aplikasi untuk menjadikan file menjadi bentuk pengkodean dengan pemrograman *PHP*?

1.2.3. Batasan Masalah

Batasan masalah dibuat agar pembahasan terfokus dalam penulisan skripsi ini, yaitu sebagai berikut :

1. Perancangan aplikasi keamanan ini hanya pengkodean untuk file teks.
2. Perancangan yang dibuat mengimplementasikan *Algoritma Blowfish*.
3. Bahasa pemrograman yang digunakan adalah *PHP* dengan *enkripsi* pemrograman menggunakan algoritma *Blowfish*.

1.3. Tujuan dan Manfaat

1.3.1. Tujuan Penelitian

Adapun tujuan dari penulisan skripsi ini adalah sebagai berikut:

1. Untuk menerapkan konsep kriptografi dalam proses pengamanan *file* teks.
2. Untuk membuat sebuah aplikasi pengamanan *file* teks dengan implementasi algoritma *Blowfish*
3. Untuk menyediakan perangkat lunak pendukung penyandian *file* teks yang dapat mudah digunakan untuk pengamanan.

1.3.2. Manfaat Penelitian

Adapun manfaat dari penulisan skripsi ini adalah sebagai berikut:

1. Memberikan kemudahan kepada pengguna untuk pengamanan penyandian file teks.

2. Menyajikan aplikasi yang dikhususkan untuk mengamankan *file* teks. Dengan kemudahan enkripsi dan dekripsi menggunakan teknik kriptografi.
3. Memahami bagaimana proses algoritma *Blowfish* dalam melakukan enkripsi dan deskripsi terhadap *file* teks.

1.4. Metodologi Penelitian

Adapun teknik-teknik pengumpulan data yang dilakukan penulisan adalah sebagai berikut :

1. Studi perpustakaan yaitu mencari bahan buku bacaan, jurnal, artikel yang berhubungan dengan masalah yang akan dibahas yang berasal dari akademik ataupun dari luar akademik, terutama yang berkaitan dengan prosedur, implementasi bahasa pemrograman PHP dalam sistem komputer.
2. Analisa Permasalahan.
Tahapan ini berupa proses pembelajaran lebih lanjut mengenai permasalahan yang ada menggunakan analisa sebab akibat sebagai dasar penentuan analisa kebutuhan.
3. Analisa Kebutuhan
Pada tahapan ini dilakukan analisa sehingga dapat didefinisikan kebutuhan-kebutuhan sistem meliputi sistem, operasi, dan *resources* sehingga dapat terbentuk suatu sistem baru yang lebih handal.
4. Analisa Keputusan
Tahapan ini bertujuan untuk menentukan solusi yang paling layak di dalam memecahkan permasalahan yang ada. Dalam hal ini berkaitan dengan perangkat keras dan perangkat lunak yang akan digunakan.

5. Desain Sistem

Tahapan ini meliputi desain model, desain basis data, desain masukan dan keluaran, dan rancangan penyandian.

6. Pembuatan Sistem

Berdasarkan desain yang telah dibuat pada tahap sebelumnya dilakukan proses pembuatan sistem menggunakan perangkat yang telah ditentukan pada tahapan analisa keputusan.

7. Implementasi Sistem

Tahapan ini tidak akan dikerjakan seluruhnya, hanya tahap pengujian program. Hal ini disebabkan oleh keterbatasan waktu.

1.5. Keaslian Penelitian

Adapun keaslian penelitian yang telah dikumpulkan dalam perancangna ini adalah terdapat penelitian terdahulu terdapat pada Tabel.1 sebagai berikut :

Tabel 1. Keaslian Penelitian

No	Penulis	Judul	Hasil
1	Suriski Sitinjak (2010)	Aplikasi Kriptografi File Menggunakan Algoritma Blowfish	Berdasarkan keseluruhan proses yang dilakukan untuk membangun Aplikasi Kriptografi File menggunakan Algoritma Blowfish ini dapat disimpulkan bahwa aplikasi ini telah berhasil dibangun dan dapat berfungsi sesuai tujuan, yaitu mengamankan data ataupun informasi yang berupa file (plainteks) dengan mengacak file tersebut sehingga tidak dapat dibaca atau dimengerti.
2	Rohmat Nur Ibrahim (2012)	Kriptografi Algoritma Des, Aes/Rijndael, Blowfish Untuk Keamanan Citra Digital Dengan Menggunakan Metode Discrete Wavelet Transformation (dwt)	Sistem yang dibangun untuk Pengamanan citra digital menggunakan Kriptografi <i>Algoritma Des, Blowfish dan Rijndael</i> Dapat mengenkripsi dan mendekripsi citra digital, terbukti menghasilkan beberapa karakteristik dari mulai kecepatan proses, MSE, NPCR dan PSNR (db).

1.6. Sistematika Penulisan

Susunan dan sistematika penulisan skripsi 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 penyandian serta teori-teori yang mendukung analisa penelitian.

BAB III : ANALISA DAN PERANCANGAN PROGRAM

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