BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan file yang tersimpan pada komputer perlu diberikan pengamanan dan sudah menjadi persyaratan mutlak yang diperlukan untuk melindungi file yang kita buat terkait beragam ancaman seperti dapat dengan mudah seseorang melihat, merusak, atau menyalahgunakan data atau informasi penting dari suatu instansi atau perusahaan melalui jaringan komputer, (Yudi Wiharto, 2018).

Konsep perlindungan data informasi dapat dilakukan dengan sistem enkripsi dan deskripsi menggunakan algoritma yang telah ditentukan sebelumnya. Proses enkripsi di sini dapat diartikan sebagai proses pengubahan plaintext menjadi chipertext, proses dimana informasi yang dikirim menjadi bentuk yang hampir tidak dikenali., sedangkan untuk proses dekripsi adalah suatu proses mengubah bentuk tersamar menjadi informasi awal. Pada kedua proses tersebut dibutuhkan pengaman yang ketat bahwa pesan tersebut terlindungi pada setiap prosesnya, pengaman tersebut dinamakan key. Fungsi dari key ini adalah kunci untuk membuka atau mengawali tiap proses pada saat melakukan proses enkripsi dan deskripsi. File dokumen yang di enkripsi hanya bisa dibuka saat sudah memasukkan sandi yang sudah dibuat, (Asri Prameshwari, 2018 :139).

Untuk mengamankan data dalam pengiriman file document saat ini penulis menggunakan metode *Advanced Encryption Standard* (AES). *Advanced Encryption Standard* (AES) merupakan salah satu algoritma simetri dan akan digunakan sebagai algoritma enkripsi dan deskripsi pada dokumen. Algoritma ini juga memiliki fungsi untuk menyembunyikan data agar data tidak dapat terbaca orang lain.

Pada penelitian ini proses enkripsi dan dekripsi yang dilakukan dalam perlindungan data informasi berbasiskan algoritma kriptografi yaitu Algoritma *Advanced Encryption Standard* (AES), (Yudi Wiharto, 2018).

Berdasarkan penelitian mengenai Kombinasi Algoritma Kriptografi AES Dan Des Untuk Enkripsi File Dokumen Proposal, Candra irawan,dkk.[1]

Berdasarkan penelitian mengenai Implementasi Kriptografi AES pada File, Sheila Maulida Intani,dkk.[2]

Berdasarkan penelitian mengenai Implementasi Algoritma AES Dan Algoritma XOR Pada Aplikasi Pengaman Teks Berbasis Mobile, Resti Amalia,dkk.[3]

Berdasarkan penelitian mengenai Analisis Algoritma AES Dalam Mengamankan Data Pada Kantor Walikota PematangSiantar, Eko Hartato,dkk [4]

Berdasarkan penelitian mengenai Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi, Dian Widyawan,dkk.[5]

Berdasarkan latar belakang yang sudah dipaparkan , Maka penulis tertarik untuk memilih judul :“**Aplikasi Keamanan File Document Dengan Menggunakan Metode Algoritma AES Berbasis Web”.**

1.2. Ruang lingkup permasalahan

1.2.1. Perumusan Masalah

Berdasarkan latar belakang dalam penulisan skripsi ini, rumusan masalahnya adalah :

1. Bagaimana mengamankan file dokumen dengan menggunakan metode AES sehingga file dokumen yang kita buat dapat aman?
2. Bagaimana merancang sebuah aplikasi enkripsi menggunakan algoritma *Advanced Encryption Standard* (AES) untuk mengamankan data file?
3. Bagaimana menerapkan Algoritma *Advanced Encryption Standard* (AES) dalam pengenkripsian data sehingga data yang telah dienkripsi tidak dapat dibaca atau dimengerti oleh pihak lain?

1.2.2. Batasan Masalah

Batasan masalah pada skripsi berikut ini adalah :

1. Membuat sandi atau memasukkan sandi agar file yang di enkripsi dapat terjaga keamanannya.
2. File dokumen yang di enkripsi hanya bisa dibuka saat sudah memasukkan sandi yang sudah dibuat.
3. Sistem aplikasi yang dibuat untuk mengamankan file dokumen agar file tersebut tidak bisa dibuka oleh orang lain.

1.3. Tujuan dan Manfaat

Tujuan dan manfaat aplikasi enkripsi file *document* dalam megamankan file document dengan menggunakan metode AES berbasis Web yaitu :

1.3.1. Tujuan

Tujuan yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut :

1. Untuk mengetahui bagaimana cara mengaplikasikan metode AES untuk mengenkripsikan file dokumen yang kita inginkan.
2. Mengimplementasikan metode *Advanced Encryption Standard* (AES) untuk enkripsi file dokumen dengan menggunakan bahasa pemrograman PHP dan MYSQL.
3. Merancang sebuah aplikasi enkripsi untuk mengamankan file dokumen yang kita inginkan agar tidak bisa dibaca oleh orang lain.

1.3.2. Manfaat

Manfaat yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut .

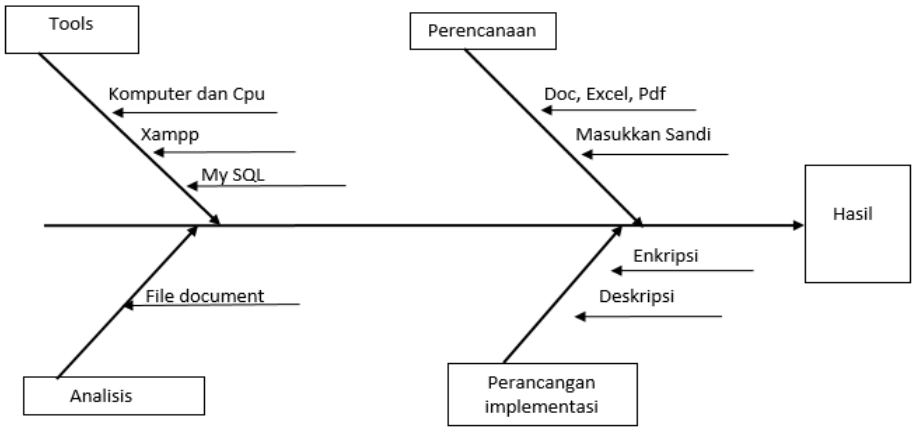
1. Dapat mengetahui bagaimana proses dari pengenkripsian file dokumen.
2. Mengetahui keakuratan aplikasi pengaman data File Dokumen dengan menggunakan Metode *Advanced Encryption Standard* (AES).
3. Dengan menggunakan aplikasi pengaman data file dokumen ini, kita dapat mengamankan suatu informasi yang terdapat di dokumen tersebut.

1.4. Metodologi Penelitian

Merupakan tata cara dan langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Langkah-langkahnya adalah :

1.4.1. Metode Perancangan Sistem

Dalam merancang sistem dilakukan tahap-tahap sebagai berikut :



Gambar 1.1. Diagram Fishbone

Keterangan :

1. **Perencanaan**

   Dalam tahap ini merupakan perencanaan awal memasukkan file yang kita pilih terlebih dahulu, setelah itu memasukkan sandi.

2. **Analisis**

Pada tahap ini merupakan analisa aplikasi terhadap kebutuhan yang meliputi file.

3. **Perancangan**

Pada tahap ini merupakan kemampuan untuk mengenkripsi dan deskripsi kan file yang kita pilih tersebut.

4. **Tools**

Pada tahapan ini penulis menggunakan web browser dan Xampp, Database yang digunakan adalah MySQL.

I.5. Kontribusi Penelitian

Adapun Kontribusi penelitian ini adalah :

Berdasarkan penelitian dari Wahyu Pramusinto , dkk (2019) dengan judul "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman" Tujuan penelitian ini adalah untuk membuat aplikasi mengamankan sebuah file document. Metode yang digunakan adalah dengan cara di enkripsi dengan metode AES.

Berdasarkan penelitian dari Imelda Asih Rohani Simbolon, dkk (2020) dengan judul "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar". Tujuan penelitian ini adalah untuk membuktikan penggunaan algoritma AES 128-bit mampu menyandikan isi header dari file terkompresi sehingga dapat mengamankan file tersebut.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam penelitian ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang Ringkasan, latar belakang, tujuan dan manfaat, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori yang dibahas mengenai sistem UML dan memberi gambaran umum dari sistem yang akan berjalan.

BAB III : ANALISIS DAN PERANCANGAN

Pada bab mengaji teori-teori tang didapatkan dari sumber-sumber yang relevan. digunakan sebagai panduan perancangan, sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini dihasilkan uji coba dan beberapa revisi. Jika terjadi kesalahan dan kekurangan terhadap perangkat lunak yang telah selesai dibuat sehingga menghasilkan output yang diharapkan.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini penulis menguraikan tentang kesimpulan dan saran untuk pemecahan suatu masalah.