BAB II

TINJAUAN PUSTAKA

II. 1. Penelitian terkait

Berdasarkan penelitian yang dilakukan oleh Sheila Maulida Intani (2019) dengan judul “mengenai Implementasi Kriptografi AES Pada File Dokumen”.

Dari hasil penelitian ini, dibuktikan isi file yang telah *dienkripsi* merupakan isi file dari file aslinya, sehingga apabila akan dilakukan proses *deskripsi*, maka akan kembali seperti file semula.

Berdasarkan penelitian yang dilakukan oleh Eko Hartato dkk (2020) dengan judul “ Analisis Algoritma AES Dalam Mengamankan Data Pada Kantor Walikota PematangSiantar”.

Data merupakan salah satu bagian terpenting dalam berlangsungnya suatu perusaan, instusi-instusi, pendidikan , instansi-instansi pemerintahan, dan untuk pribadi. Sehingga memerlukan berbagai macam pertimbangan untuk melakukan penyimpanan data terlebih untuk masalah keamanan dan kerahasiannya.

Berdasarkan penelitian yang dilakukan oleh Asri Prameswari (2018) dengan judul “Implementasi Algoritma *Advanced Encryption Standard* (AES) 128 Untuk Enkripsi Dan Deskripsi File Dokumen”.

Pada penelitian ini proses enkripsi dan dekripsi yang dilakukan dalam perlindungan data informasi berbasiskan algoritma kriptografi yaitu Algoritma AES-128 dengan

Kunci Simetri. Penerapan algoritma ini akan dilakukan pada pengamanan jenis data berjenis dokumen dengan tipe doc. Pada proses pembuatan aplikasi perlindungan enkripsi dekripsi ini akan menggunakan software Microsoft Visual Studio 2012 sebagai bahasa pemrograman.

Berdasarkan penelitian yang dilakukan oleh Angga Aditya Permana, dkk (2018) dengan judul "Rancangan Aplikasi Pengaman Data Dengan Algoritma *Advanced Encryption Standard* (AES)".

Penulis berhasil mengamankan data dengan mengenkripsi file tersebut menggunakan algoritma *Advanced Encryption Standard* (AES).

II.2. Landasan Teori

Landasan teori peneliti kutip dari beberapa teori yang berkaitan dengan penelitian ini yaitu :

II.2.1. Implementasi

Implementasi merupakan bagian yang menjelaskan tentang pembuatan tampilan pada aplikasi.

II.2.2. Aplikasi

Aplikasi merupakan alat untuk mempermudah proses pekerjaan. aplikasi adalah unit satuan yang dibuat untuk membantu kebutuhan beberapa kegiatan seperti game, pelayanan masyarakat serta proses yang dilakukan manusia.

Aplikasi berguna untuk membuat pengolahan data seperti kegiatan pembuatan dokumen-dokumen pada pengolahan data. Aplikasi juga bergerak di atas sistem operasi.

II.2.3. Enkripsi

Enkripsi adalah proses pengubahan plaintext menjadi chipertext. Dan merupakan suatu proses yang dilakukan untuk mengubah pesan yang tersembunyi menjadi pesan asli disebut deskripsi. Enkripsi berproses dimana data atau informasi yang akan diteruskan diubah menjadi bentuk yang hampir tidak dikenal sebagai informasi dengan menggunakan algoritma tertentu agar menjadi pesan yang terlindungi. Kunci yang digunakan pada enkripsi dan deskripsi memiliki kunci yang sama.

II.2.4. Deskripsi

Deskripsi adalah teknik yang memperoleh kembali plaintext menjadi ciphertext, atau proses pengubahan kembali data yang berbentuk rahasia menjadi semula. Deskripsi *(Data Encryption Standard)* tergolong ke dalam blog chiper simetrik.

II.2.5. File

File merupakan objek data dari yang disimpan ke dalam sistem file yang di peroleh akses dan disusun oleh pengguna tersebut.

II.2.6. Web

aplikasi web berfungsi untuk melindungi file data pribadi pengguna internet yang mempertimbangkan faktor kecepatan proses chipering dan menambahkan satu jenis file yang dapat digunakan yaitu jenis file word sering digunakan untuk dapat bertukar informasi. Penyertaan faktor kecepatan aplikasi diharapkan meningkatkan kelayakan aplikasi sebagai aplikasi yang berbasis web dan meningkatkan kebermanfaatannya dengan menambahkan satu jenis file dalam penggunaannya.

II.2.7. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang dirancang oleh dua orang yang berasal dari Belgia yaitu Vincent Rijmen dan John Daemen.

Advanced Encryption Standard (AES) yang merupakan metode kriptografi yang bisa digunakan untuk menyelamatkan data dalam berbagai aplikasi. Algoritma *Advanced Encryption Standard* (AES) adalah blok *chipertext* blok simetrik yang dapat digunakan untuk mengenkripsi *(enchiper)* dan mendeskripsi (decipher) informasi.

Advanced Encryption Standard (AES) adalah *cryptographic* yang digunakan untuk mengamankan suatu data. Algoritma AES merupakan blok *ciphertext* simetrik yang berfungsi untuk mengenkripsi *(encipher)* dan deskripsi *(dechiper)* informasi.

II.2.8. Algoritma

Algoritma merupakan langkah-langkah urutan dalam menyelesaikan masalah yang disusun dengan valid dan terstruktur.

II.2.9. Bahasa Pemrograman PHP

PHP adalah pemrograman interpreter yaitu proses penerjemah baris kode sumber menjadi kode mesin yang dimengerti komputer secara langsung pada saat baris kode dijalankan. PHP disebut sebagai pemrograman *Server Side Programing.*

PHP dirancang agar menciptakan halaman web yang hidup, yaitu halaman yang membangun suatu tampilan, seperti memperlihatkan isi tampilan basis data yang dibuat ke dalam web.

PHP atau kependekan dari *Hypertext Preprocessor* adalah salah satu bahasa pemrograman *open source* yang sangat cocok atau dikhususkan untuk pengembangan web dan dapat ditanamkan pada sebuah skripsi HTML.

II.2.10. MySQL

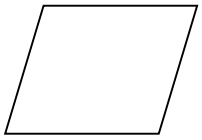
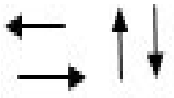
MySQL adalah suatu perangkat lunak database relasi (*Relation Database Management System* atau DBMS). MySQL didefinisikan sebagai suatu perintah-perintah tertentu atau bahasa program yang digunakan untuk mengelola suatu database. Pada MySQL, sebuah database mengandung satu atau sejumlah tabel. Tabel terdiri atas sejumlah baris dan setiap baris mengandung satu atau beberapa kolom (Priyo Sutopo, dkk:2017).

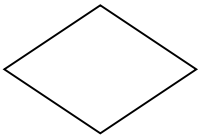
II.2.11. Flow Of Dokumen

Flowchart adalah diagram alir yang berhubungan dengan simbol grafis yang memberitahukan aliran dari proses yang meliputi langkah-langkah yang diberi simbol dan urutannya. Dengan mempertemukan dari masing-masing langkah dari aliran yang diberi tanda panah. Diagram berikut dapat memberikan kemudahan untuk menyelesaikan masalah yang ada dalam setiap proses tersebut.

Flowchart digunakan untuk mengelola atau memproses yang suatu program. Seperti halnya diagram , membantu dalam menjalankan apa yang terjadi dan membantu aktor dalam memahami proses alur tersebut. pada gambar I.1.

Tabel II.1. Simbol flowchart

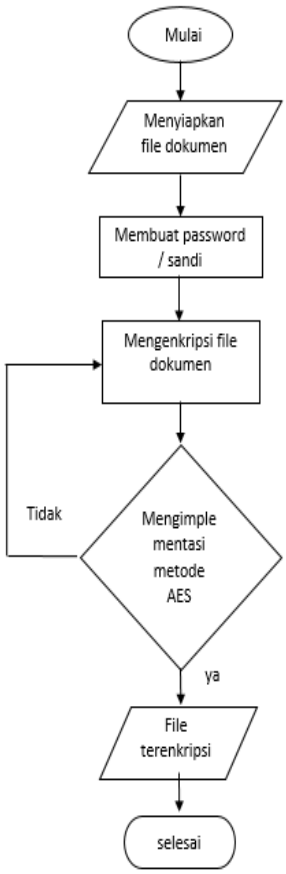
Simbol	Nama	Keterangan
	Terminal	Menyatakan awal atau akhir suatu program.
	Input / output	Menyatakan proses input / output.
	Proses	Menunjukkan kegiatan proses dari operasi program komputer.
	Flow	Menunjukkan arus dari proses.

	Decision	Menunjukkan suatu kondisi tertentu antara ya / tidak.

Tabel II.1.Simbol Flow Of Document (FOD)

II.3.1.*Flowchart* Implementasi AES

Berikut ini digambarkan suatu bentuk *flowchart* yang dapat dilihat pada gambar dibawah II.1. berikut :



Gambar II.1. kerangka kerja flowchart

Pada gambar prosedur perancangan sistem diatas diuraikan ke dalam beberapa tahap yaitu :

1. Menyiapkan file dokumen

   Pada tahap ini kita harus menyiapkan file dokumen yang akan di enkripsi.

2. Membuat sandi / password

   Masuk ke tahap ini, kita membuat sandi atau memasukkan sandi yang ada.

3. Mengenkripsi file dokumen

   Tahap selanjutnya adalah mengenkripsi file dokumen (Doc).

4. Implementasi

   Implementasi adalah bagian yang menjelaskan hal tentang pembuatan tampilan aplikasi yang sudah di enkripsi.

5. File terenkripsi

   File yang sudah terenkripsi artinya file yang kita jalankan sudah berhasil.