BAB I

PENDAHULUAN

I.1. Latar Belakang

Salah satu bentuk penyimpanan pesan rahasia adalah berupa *file musik*. Tujuan penyimpanan musik yaitu untuk menyimpan hasil rekaman musik penting. Untuk menjaga hasil rekaman yang di dapat dari kegiatan yang bersifat rahasia di perlukan sistem pengamanan *file musik* hasil rekaman tersebut. Bisa jadi file rahasia yang kita simpan bisa dijiplak oleh orang lain jika penyimpanan file dibuat tanpa keamanan. Penjiplakan/Plagiarisme adalah hal yang berbeda dengan penggunaan lagu tanpa izin penciptanya. Plagiarisme artinya lagu ciptaan seseorang telah diambil beberapa bagian/seluruhnya & diakui menjadi milik orang lain. Plagiarisme menyangkut hak moral oleh karenanya juga merupakan pelanggaran hak cipta juga. Jika terjadi plagiarisme, seorang pencipta harus memiliki bukti yang mendukung pengakuannya mengenai *originality* atau asal usul dari karya yang dipersoalkannya. Penggunaan lagu tanpa izin diatur dalam pasal 9 Undang Undang Dasar nomor 28 tahun 2014 tentang hak cipta.. Hal ini di sebabkan pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan munculnya suatu teknik-teknik yang baru yang di salahgunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Ironisnya, teknik yang di gunakan untuk mengancam keamanan data selalu setingkat lebih maju dari pada teknik yang di gunakan untuk mengamankan data. Karena itu timbul suatu gagasan yang mengacu kepada permasalahan tersebut, yakni untuk membuat suatu sistem keamanan yang

dapat melindungi data yang di anggap penting dengan cara menyandikan data sehingga sulit untuk di deteksi oleh pihak yang tidak berhak. Untuk keperluan tersebut, maka di perlukan teknik kriptografi dengan metode enkripsi dan dekripsi.

Kriptografi adalah ilmu untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau plainteks menjadi cipherteks (pesan tersandi). Sedangkan dekripsi adalah proses penyandian kembali cipherteks menjadi plainteks.

Algoritma yang akan digunakan untuk mengamankan data pada penelitian ini adalah AES dan Railfence. AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik. Sedangkan algoritma Railfence adalah salah satu bentuk *cipher* transposisi yang sederhana yang diinspirasi dari model *Polybiussquare* (Retnani ; 2017).

Kekuatan AES terletak pada karakteristik sifat dari medan GF(28) dimana untuk setiap bilangan prima selalu terdapat sebuah medan tunggal terbatas yang unik sehingga seluruh representasi dari GF(28) bersifat isomorphic dan pemilihan polinomial biner berderajat 8 m(x) bersifat irreducible yakni tidak dapat dibagi oleh bilangan lain pada medan selain 1 dan dirinya sendiri, relatif prima terhadap medan.Kekuatan ini didasari oleh operasi matematis yang kompleks dan membutuhkan sumber daya yang tidak sedikit untuk melakukan komputasi. Karena didasarkan pada persamaan matematis, AES dapat dengan mudah dibuktikan keamanannya (Joan Daemen, Rijmen Vincent. AES Proposal: Rijndael. Document

version 2-Date ; 2018). Sedangkan Algoritma RailFence memiliki keunggulan dibanding algoritma lainnya karena dalam tahap proses penulisan plaintext menjadi ciphertext dapat dilakukan pada baris mana saja sehingga menambah kerumitan proses enkripsi dan dekripsi. (Singh dkk. 2012).

Berdasarkan latar belakang tersebut pada penelitian ini akan di buat sebuah aplikasi untuk mengamankan file rahasia dalam bentuk musik menggunakan algoritma AES sehingga aman dari tindak pencurian informasi dari musik rahasia tersebut. Maka pada penelitian ini akan di tarik judul penelitian **"Penerapan Algoritma AES Pada Keamanan *File* Musik Dengan Generator Kunci Menggunakan Algoritma Railfence"**.

I.2. Ruang Lingkup Permasalahan

I.2.1.Identifikasi Masalah

Adapun hal-hal yang menjadi identifikasi masalah aplikasi ini adalah :

1. Berkas rahasia yang disimpan dalam bentuk musik sewaktu-waktu dapat diketahui isinya oleh pihak yang tidak di inginkan.
2. Dibutuhkan sebuah media yang dapat digunakan untuk mengamankan *file* musik sehingga isi dari *file* musik tersebut tidak dapat diketahui oleh orang lain.

I.2.2. Perumusan Masalah

Berikut perumusan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini, antara lain :

1. Bagaimana merancang dan membuat sebuah aplikasi berbasis *dekstop* untuk mengamankan *file musik* menggunakan algoritma AES ?
2. Bagaimana penerapan algoritma Railfence untuk menghasilkan kunci acak untuk digunakan dalam proses enkripsi dan dekripsi *file musik* ?

I.2.3. Batasan Masalah

Dalam penulisan skripsi ini dibatasi permasalahannya sebagai berikut :

1. Aplikasi ini dibangun menggunakan bahasa pemrograman VB.NET pada perangkat lunak Visual Studio.
2. Aplikasi ini bertujuan untuk digunakan dalam mengamankan *file* musik dengan ekstensi .mp3, .wav, .wma, .pcm, .flac.
3. Batas maksimal kapasitas musik adalah berukuran 500 MB (Lima ratus *Megabyte*).
4. Aplikasi ini dirancang untuk digunakan pada perangkat *desktop* seperti komputer dan laptop.
5. Algoritma yang digunakan untuk mengamankan *file* musik adalah algoritma AES.
6. Pada aplikasi yang akan dirancang juga akan diterapkan algoritma Railfence yang berguna dalam melakukan pengacakan kunci yang akan digunakan untuk mengamankan dan mengembalikan *file* musik.
7. Kunci yang akan digunakan untuk proses enkripsi dan dekripsi adalah seluruh karakter berdasarkan tabel ASCII.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

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

1. Membangun aplikasi yang dapat mengamankan *file musik* yang bersifat rahasia.
2. Menerapkan algoritma AES untuk mengamankan *file musik* yang bersifat rahasia sehingga tidak dapat diketahui isinya oleh pihak lain.

I.3.2. Manfaat

Adapun manfaat yang dapat diambil dalam penulisan skripsi ini adalah:

1. Dapat digunakan untuk mengamankan sebuah *file musik* yang bersifat rahasia agar tidak dapat diketahui oleh pihak lain yang tidak diinginkan.
2. Sebagai media yang dapat digunakan pengguna untuk mengamankan *file musik* agar pengguna dapat bertukar *file musik* yang bersifat aman secara rahasia.

I.4. Metodologi Penelitian

Untuk dapat mengimplementasikan sistem di atas, maka secara garis besar digunakan beberapa metode sebagai berikut:

I.4.1. Metode Pengumpulan Data

Sistem yang dirancang tentunya memerlukan pengumpulan data, dalam proses pengumpuan data terdapat beberapa cara, berikut diantaranya :

a. Survei Lapangan

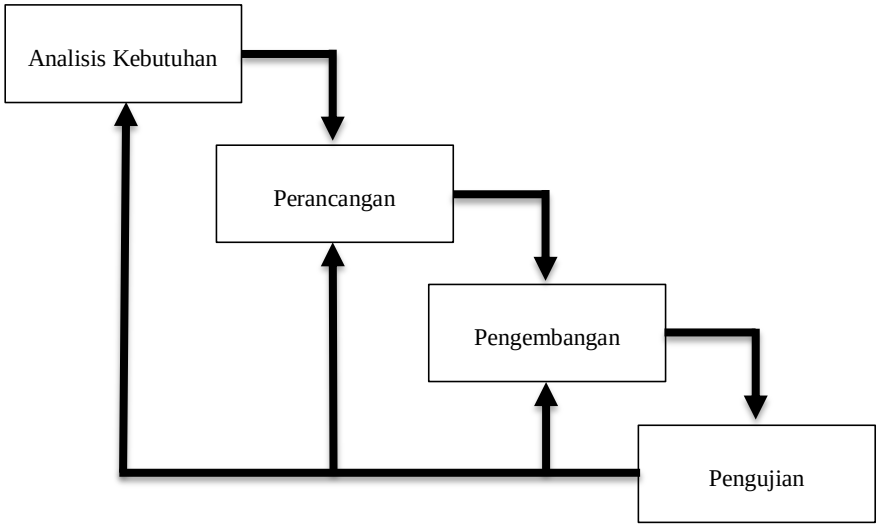
Survei lapangan merupakan langkah awal yang bertujuan untuk memperoleh data yang di butuhkan dalam tahap analisis. Pada tahap ini memberikan pertanyaan mengenai bagaimana bentuk pesan rahasia yang biasanya di kirimkan atau di terima.

b. Studi Pustaka

Studi pustaka merupakan kegiatan mengumpulkan data-data berupa teori pendukung dari sistem yang di buat dengan maksud untuk memaparkan tentang teori-teori yang di kaitkan dalam penelitian ini. Sumber-sumber yang di dapat berupa literatur, *ebook*, dan lainnya yang relevan dengan penelitian.

I.4.2. Metode Perancangan Sistem

Dalam merancang sistem dilakukan tahap prosedur perancangan, langkah-langkah yang diperlukan untuk mencapai tujuan perancangan dapat dilihat pada *model diagram waterfall* gambar I.1. Sesuai dengan namanya *waterfall* (air terjun) maka tahapan dalam model ini disusun bertingkat, setiap tahap dalam model ini dilakukan beurutan, satu sebelum yang lainnya (sesuai dengan tanda panah). Selain itu dari satu tahap kita dapat kembali ketahap sebelumnya jika terdapat kekurangan dalam satu tahap tersebut.



Gambar I.1. Diagram *Waterfall* Perancangan Sistem

Lebih rinci lagi langkah-langkah perancangan sistem dapat dijelaskan sebagai berikut:

I.4.2.1. Tahap Analisis

a. Analisis Kebutuhan

Seluruh kebutuhan *software* harus bisa didapatkan dalam fase ini, termasuk didalamnya kegunaan *software* yang diharapkan pengguna dan batasan *software*. Informasi ini biasanya dapat diperoleh melalui pengamatan. Informasi tersebut dianalisis untuk mendapatkan dokuementasi kebutuhan pengguna untuk digunakan pada tahap selanjutnya.

Dalam membuat penelitian ini, spesifikasi minimum dari perangkat keras (*Hardware)* dan perangkat lunak (*Software)* yang digunakan adalah sebagai berikut :

1) Perangkat Keras *(Hardware)*

Perangkat keras yang digunakan antara lain :

a. Laptop

b. RAM 2 GB

2) Perangkat lunak *(Software)*

Software yang digunakan untuk membuat skripsi ini antara lain :

a. Sistem Operasi *Windows* 10

b. Microsoft Visual Studio

I.4.2.2. Tahap Perancangan

Pada tahap ini akan di lakukan perancangan dari aplikasi yang akan dibuat meliputi : model sistem, perancangan arsitektural, perancangan antarmuka, dan perancangan prosedur.

I.4.2.3. Tahap Pengembangan

Pada tahap ini perangkat lunak Visual Studio di gunakan untuk membuat aplikasi berdasarkan rancangan yang telah di buat untuk menghasilkan aplikasi penerapan algoritma AES pada keamanan *file musik* dengan generator kunci menggunakan algoritma Railfence.

I.4.2.4. Tahap Pengujian

a. Pengujian Sistem

Pengujian adalah elemen kritis dari jaminan kualitas dan merepresentasikan spesifikasi, desain dan pengkodean. Dalam melakukan uji coba ada dua masalah

penting yang akan di bahas, yaitu teknik uji coba perangkat lunak dan strategi uji coba perangkat lunak.

b. Verifikasi dan Validasi Sistem

Verifikasi dan validasi sistem bertujuan untuk menguji kelayakan dan rasional sistem oleh praktisi yang berhubungan dengan penelitian. Langkah ini di lakukan dengan menggunakan format uji sistem.

c. Revisi dan Review Sistem

Setelah verifikasi dan validasi, maka akan di lakukan revisi dan review yang di maksudkan agar sistem sudah memiliki kelayakan dan fungsionalitas yang baik untuk menjadi sebuah aplikasi kemanan *file musik* yang sesuai dengan rancangan. Tahap ini akan melihat kembali aplikasi yang di hasilkan di lihat dari kelayakan yang di hasilkan, serta kekurangan, kelebihan, kendala dan rekomendasi.

d. Implementasi Sistem

Uji coba akan di lakukan pada beberapa pengguna perangkat *desktop* untuk melihat kelayakan aplikasi ini untuk selanjutnya di gunakan secara umum. Pada tahap ini pengguna akan di berikan kuesioner untuk penilaian terhadap aplikasi.

e. Analisis hasil

Hasil dari tahap implementasi sistem akan di analisis dan kemudian akan di lakukan pemeliharaan. Pemeliharaan sistem dapat meliputi aktivitas-aktivitas berikut:

1) Koreksi kesalahan
2) Adaptasi
3) Peningkatan

4) Perekayasaan kembali

I.5. Kontribusi Penelitian

Adapun kontribusi yang di berikan pada penelitian yang di laksanakan adalah berupa :

Pada penelitian sebelumnya, Nurliana (2015) melakukan penelitian "Aplikasi Keamanan File Algoritma Blowfish pada Universitas Lancang Kuning". Penelitian tersebut menghasilkan aplikasi untuk mengamankan *file* dokumen menggunakan algoritma blowfish. Hal inilah yang seringkali di takutkan oleh pihak – pihak yang saling ingin bertukar informasi.. Penelitian ini menggunakan algoritma blowfish sebagai algoritma kriptografi. Penelitian ini melakukan analisa kinerja algoritma blowfish pada simulasi data terbatas yaitu pada lalu lintas data di website. Penelitian ini menggunakan metode End Of File (EOF) untuk enkripsi citra dengan cara menyisipkan/menyembunyikan kunci yang digunakan untuk proses enkripsi dan deskripsi pada citra hasil enkripsi setelah dikirimkan. Penelitian ini menggabungkan dua metode yaitu steganografi DCS dan blowfish untuk strategi pengamanan ganda konten digital. Penelitian ini menggunakan algoritma blowfish untuk pengamanan suara. Dari penelitian ini keamanan data suara tergantung dari panjang kunci, dimana panjang kunci yang fleksibel dengan menggunakan algoritma blowdfish yaitu pada satu sampai enam belas karakter. Dari penelitian inilah dapat menghasilkan sebuah aplikasi yang bisa digunakan untuk mengamankan file *dokumen* dengan aman dan rahasia tanpa harus takut tertukar informasi. (Nurliana, Aplikasi Keamanan File Algoritma Blowfish ; 2015)

Pada kali ini saya akan melakukan penelitian “Penerapan Algoritma AES pada Keamanan File Musik dengan generator kunci menggunakan Algoritma Railfence”. Untuk menjaga hasil rekaman yang di dapat dari kegiatan yang bersifat rahasia di perlukan sistem pengamanan *file musik* hasil rekaman tersebut. Penelitian ini menggunakan 2 algoritma yaitu algoritma AES dan juga algoritma RailFence untuk pengamanan file musik. Dimana dengan menggunakan algoritma AES yang didasarkan pada persamaan matematis, AES dapat dengan mudah dibuktikan keamanannya sedangkan Sedangkan Algoritma RailFence memiliki keunggulan dibanding algoritma lainnya karena dalam tahap proses penulisan plaintext menjadi ciphertext dapat dilakukan pada baris mana saja sehingga menambah kerumitan proses enkripsi dan dekripsi. Dari penelitian tersebut akan di hasilkan sebuah aplikasi berbasis desktop untuk mengamankan *file musik* yang bersifat rahasia menggunakan algoritma AES. Algoritma railfence di gunakan untuk menghasilkan kunci yang lebih acak dalam untuk di gunakan pada proses enkripsi dan dekripsi.

I.6. Sistematika Penulisan

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

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metodologi penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan aplikasi yang dirancang serta kelebihan dan kekurangan aplikasi yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk pembuatan aplikasi penerapan algoritma AES pada keamanan *file* musik dengan generator kunci menngunakan algoritma Railfence.