BAB I

PENDAHULUAN

I.1. Latar Belakang

Selama ini ujian bimbingan digunakan sebagai sarana evaluasi untuk mengukur pengetahuan, untuk memenuhi syarat untuk kelulusan dan bentuk ujiannya masih dalam bentuk konvensional.

Dengan perkembangan teknologi saat ini khususnya perkembangan informasi dalam bentuk web sangat beraneka ragam bentuk, baik dari web statik maupun web dalam bentuk dinamis.Web adalah sebuah perangkat lunak untuk membantu manusia dengan mudah dalam memberikan informasi dan keamanan data adalah hal yang sangat penting dan perlu adanya upaya keseriusan guna meningkatkan kesadaran keamanan informasi baik dilingkungan pemerintah, instansi dan organisasi.Salah satu teknik mengamankan data yaitu dengan teknik penyandian atau kriptografi. (Arisantoso,dkk 2017).

Kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut dengan melakukan pembangkitan kunci, enkripsi dan dekripsi. Kriptografi bertujuan untuk memberi layanan keamanan (Sholeh, dkk, 2015 : 2).

AES (Advanced Encryption Standard) adalah sebuah *symmetric block cipher* yang dapat melakukan enkripsi dan dekripsi pada data. Algoritma AES dapat menggunakan kunci 128, 192 dan 256 *bit* untuk melakukan enkripsi dan dekripsi terhadap data dengan ukuran blok 128 *bit* (Voni Yuniati,dkk ;2015:24).

Beberapa kelebihan dari AES (Advanced Encryption Standard) Dilihat dari segi jenis kunci yang simetri maka kecepatan operasi (komputasi) lebih tinggi bila dibandingkan dengan algoritma asimetrik sehingga dapat digunakan pada sistem realtime seperti GSM. (Asriyanik;2017:556).

Selama ini soal ujian yang di buat oleh pembimbing di berikan secara manual kepada bagian admin dalam bentuk file sehingga sering terjadi kebocoran soal, dari permasalahan tersebut peneliti termotivasi dan mencoba memberikan pemecahan masalah tentang kebocoran soal yang dihadapi dengan kecurangan pada saat ujian maka peneliti merancang dan membangun aplikasi agar dapat mengamankan data dan menjaga kerahasiaan data soal ujian. Oleh karena itu, maka dalam penyusunan skripsi ini peneliti mengambil judul "**Implementasi Metode Aes Dalam Pengamanan Data Soal Ujian Bimbingan Belajar Berbasis Web**". Dan teknik yang dapat digunakan adalah dengan menerapkan suatu metode kriptografi pada soal ujian.Dengan tersandikannya isi data ujian, maka seseorang tidak dapat mengubah isi dari soal ujian tersebut.

Adapun hasil dari penelitian ini adalah mempermudah dalam penentuan soal ujian serta mengefisienkan waktu dalam penentuan soal ujian menjadi lebih aman dan akurat serta terjaga, terutama pada era berkembangnya teknologi penulis berharap penelitian ini sangat bermanfat dan digunakan dengan sebaik mungkin untuk penelitian selanjutnya.

I.2. Ruang Lingkup Permasalahan

Ruang lingkup permasalahan yang terdapat pada penelitian ini berdasarkan latar belakang adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Identifikasi masalah dari penulisan untuk penelitian ini adalah :

1. Pelaksanaan pengiriman soal ujian bimbingan masih sistem manual.
2. Penyimpanan data peserta ujian bimbingan belum menggunakan aplikasi tersimpan pada sistem database.
3. Keamanan data ujian bimbingan tidak terjamin karena masih tersimpan didalam lemari.

I.2.2. Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian ini yaitu :

1. Bagaimana merancang aplikasi mengamankan pengiriman Soal ujian?
2. Bagaimana mengimplementasi keamanan data dengan metode AES?
3. Bagaimana merancang database pengamanan Data Soal ujian?

I.2.3. Batasan Masalah

Agar pembahasan masalah tidak kemana-mana maka penulis membatasi masalah sebagai berikut :

1. Aplikasi yang di bangun hanya membahas keamanan soal ujian
2. Keamanan data soal ujian menggunakan metode AES.

3. Pemrograman berbasis *web* dan *database* menggunakan MySQL.
4. Bahasa pemograman yang dipakai dalam perancangan aplikasi ini menggunakan bahasa pemograman php.
5. Format data gambar yang dipakai dalam file soal berformat Pdf dan berukuran 2 MB dan format gambar JPEG yang digunakan hanya berukuran 2 MB juga untuk pembuatan profil yang berisikan gambar.

I.3. Tujuan dan Manfaat

Adapun beberapa tahap yang dilakukan dalam membuat tujuan dan manfaat adalah :

I.3.1. Tujuan

Tujuan dari penelitian ini yaitu :

1. Membangun sebuah aplikasi yang dapat mengamankan data soal ujian bimbingan.
2. Menerapkan metode Algoritma AES untuk pengamanan dan menjaga kerahasiaan data.
3. Menyajikan solusi keamanan data soal ujian.

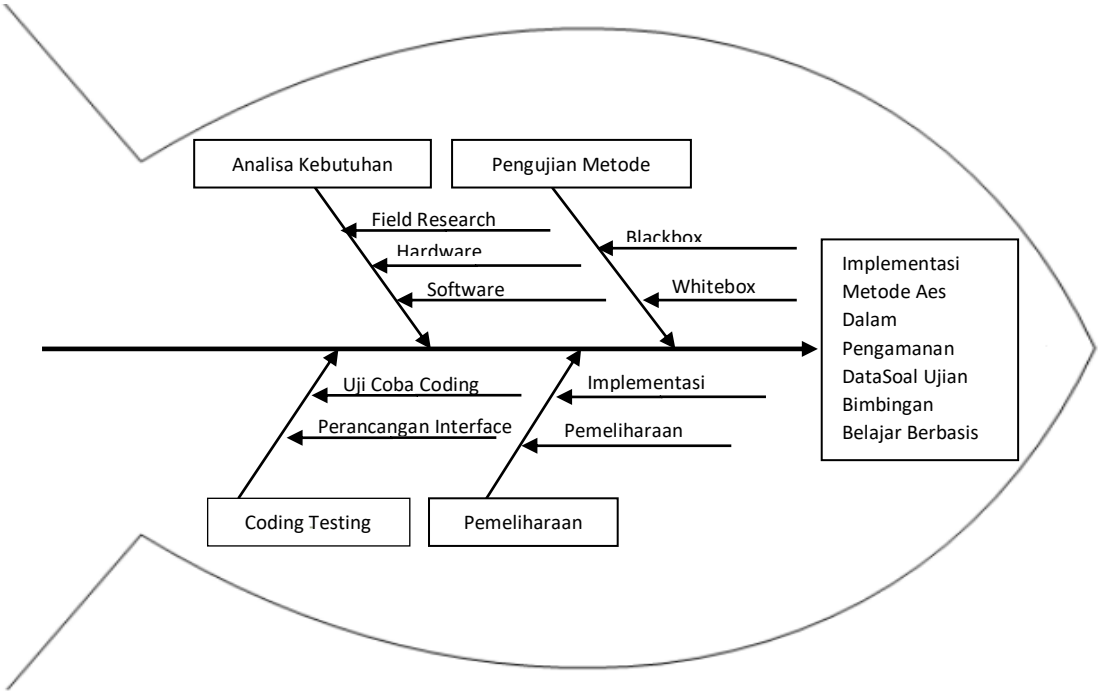
I.3.2. Manfaat

Manfaat penelitian ini yaitu :

1. Memudahkan pengerjaan dalam membuat laporan data soal ujian bimbingan.
2. Memudahkan *user* dalam melindungi data menjadi lebih aman dari pencurian.
3. Membuat *user* mengerti dalam penggunaan sistem aplikasi.

I.4. Metode Penelitian

Merupakan cara pengumpulan data dengan mempelajari literatur, paket modul dan panduan, buku-buku pedoman, buku-buku perpustakaan dan segala kepustakaan lainnya yang dianggap perlu dan mendukung. Peneliti menggunakan *Fishbone* untuk menggambarkan alur kerja yang peneliti lakukan untuk menyelesaikan penelitian ini.



Gambar III.1. Diagram *Fishbone* Proses Perancangan Sistem

Dalam pengembangannya metode kerangka *fishbone*memiliki beberapa tahapan yaitu : *requirement* (analisis kebutuhan), *design* sistem (*system design*), *coding*, pengujian program, pemeliharaan sistem:

1. Target/Tujuan Penelitian

Target penelitian ini yaitu merancang dan membangun sistem keamanan data menggunakan metode aes pada soal ujian bimbingan.

2. Analisis Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan pengumpulan data-data teori yang terkait dengan data soal ujian bimbingan.

3. Pengujian Metode

Tujuan utama tahap pengujian metode untuk mengetahui syarat kemampuan yang harus dipenuhi oleh sistem agar keinginan pemakai sistem dapat terwujud. Tahap analisis ini terbagi menjadi dua, yaitu analisis kebutuhan sistem fungsional dan analisis kebutuhan sistem nonfungsional yang dapat dilihat pada Tabel I.1 dan Tabel I.2 dibawah ini:

Tabel I.1. Kebutuhan Sistem Fungsional

No	Kebutuhan	Rincian Kebutuhan
1.	Fungsi Sistem	– Sistem Keamanan DataDalam mengamankan data soal ujian bimbingan – Sebagai *interface* penyampaian informasi
2.	Perangkat Lunak	– *Notepad++. Xampp*
3.	Pelaksana Sistem	– *User*
4.	Pengolah Sistem	– *Programmer*

Tabel I.2. Kebutuhan Sistem Nonfungsional

No	Kebutuhan	Rincian Kebutuhan
1.	Sistem Operasi	– Minimal Windows 7
2.	Prosesor	– Minimal Intel
3.	RAM	– Minimal 2GB
4.	Hardisk	– Minimal 120GB
5.	Monitor/LCD	– Minimal Resolusi 1024x768

4. Coding Sistem

Coding merupakan penerjemahan desain dalam bahasa yang bisa dikenali oleh komputer. Dilakukan oleh programmer yang akan menterjemahkan transaksi yang diminta oleh *user*. Tahapan inilah yang merupakan tahapan secara nyata dalam mengerjakan suatu sistem. Dalam artian penggunaan komputer akan

dimaksimalkan dalam tahapan ini. Setelah pengkodean selesai maka akandilakukan testing terhadap sistem yang telah dibuat tadi. Tujuan testing adalah menemukan kesalahan-kesalahan terhadap *system* tersebut dan kemudian bisa diperbaiki.

5. Pengujian Program

Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem.Pengujian yang dilakukan yaitu pengujian perangkat lunak yang tes fungsionalitas dari aplikasi yang bertentangan dengan struktur internal atau kerja. Pengetahuan khusus dari kode aplikasi/struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan, pengujian tersebut untuk masing-masing blok peralatan yang dirancang.

6. Pemeliharaan Sistem

Perangkat lunak yang susah disampaikan kepada pelanggan pasti akan mengalami perubahan. Perubahan tersebut bisa karena mengalami kesalahan karena perangkat lunak harus menyesuaikan dengan lingkungan (periperal atau sistem operasi), atau karena pelanggan membutuhkan perkembangan fungsional.

I.5. Kontribusi Penelitian

Penelitian ini diharapkan dapat memberikan manfaat dari sisi keilmuan, adapun manfaat tersebut, yaitu:

1. Menambah pengetahuan dalam melakukan pengamanan data menggunakan Algoritma AES.

2. Enkripsi Algoritma AES sebagai bahan referensi bagi peneliti lain yang ingin mengembangkannya dalam proses pengamanan data pesan di jaringan blouetooth.
3. Perangkat lunak enkripsi Algoritma AES untuk mempermudah dalam mengamankan data yang berjenis teks di dalam jaringan bloetooth.

I.6. Sistematika

Dalam penelitian ini pembahasan terbagi dalam lima bab yang secara singkat akan diuraikan sebagai berikut:

BAB I : PENDAHULUAN

Dalam bab ini akan dibahas mengenai latar belakang penulisan skripsi, batasan masalah, tujuan dan manfaat, metode penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Dalam bab ini akan dibahas mengenai berbagai teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN PERANCANGAN

Dalam bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan skripsi.

BAB IV : HASIL DAN UJI COBA

Dalam bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan, serta perangkat yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini menguraikan tentang kesimpulan dari hasil penelitian yang didapat dan juga saran yang dapat digunakan untuk pengembangan sistem ini kearah yang lebih baik lagi di masa yang akan datang.