BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era digital sekarang ini, masalah keamanan dan kerahasiaan sebuah data merupakan suatu hal yang penting untuk suatu komunitas atau data pribadi yang bersifat privat. Karena ada data yang umumnya hanya ditunjukkan bagi orang-orang tertentu saja, sehingga jika data tersebut dilihat atau dibajak oleh orang pihak lain maka tidak menutup kemungkinan data tersebut akan dirusak atau bahkan disebar luaskan sehingga dapat mengakibatkan kerugian.

Kebijakan kerahasiaan data ini juga diatur dengan Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan diubah oleh Undang Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektrik.

Dalam upaya untuk menjaga keamanan sebuah data terdapat metode pengamanan data yang disebut dengan nama kriptografi. Kriptografi itu sendiri merupakan suatu metode pengamanan data yang bisa dipergunakan untuk menjaga kerahasiaan dan keaslian sebuah data.

Kriptografi merupakan sebuah ilmu yang digunakan untuk mengacak data sedemikian rupa sehingga data tersebut tidak dapat dibaca oleh pihak luar yang tidak berhak atas data tersebut dan data yang telah diacak tersebut harus dapat dikembalikan kebentuk aslinya oleh pihak orang yang bersangkutan. Umumnya data yang akan diacak disebut *Plaintext*, data yang akan diacak dengan kunci enkripsi dalam prosesnya disebut Enkripsi. *Plaintext* yang teracak disebut *Ciphertext*. Kemudian proses untuk mengembalikan *Ciphertext* ke *Plaintext* disebut proses Dekripsi.

Dalam kriptografi dibagi menjadi 2 jenis algoritma yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris untuk proses enkripsi dan dekripsi menggunakan kunci yang sama, dan untuk algoritma asimetris menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya.

Algoritma kriptografi dapat disebut baik apabila memerlukan waktu lama dalam memecahkan sebuah data yang tersandikan. Seiring perkembangan teknologi informasi, teknologi informasi membutuhkan algoritma kriptografi yang sulit untuk dipecahkan.

Oleh karena itu pada penelitian ini dirancanglah suatu sistem keamanan yang difungsikan untuk melindungi data agar data tidak terbaca oleh pihak yang tidak berhak dengan memakai algoritma AES (*Advanced Encryption Standard*) yang difungsikan untuk proses enkripsi data saat data tersebut dikirim untuk mencegah isi data tersebut tidak bisa dipahami oleh penerima yang tidak berhak atas data tersebut.

1.2 Perumusan Masalah

Perumusan masalah dalam penelitian ini yaitu :

1. Bagaimana cara menerapkan Metode AES pada Aplikasi sistem pengamanan Soal Ujian yang dibuat ?
2. Bagaimana penerapan algoritma AES 128-bit pada aplikasi yang dibuat ?
3. Seberapa lama waktu yang diperlukan untuk proses enkripsi dan dekripsi dokumen ?

1.3 Pembatasan Masalah

Pembatasan masalah dalam penelitian ini yaitu :

1. Metode yang digunakan menggunakan algoritma AES 128-bit.
2. Sistem yang dibangun berbasis Web.
3. Data yang akan di enkripsi dan dekripsi berbentuk Dokumen.
4. Perangkat lunak tidak menampilkan tahapan-tahapan konversi bilangan ke dalam bilangan biner.

1.4 Tujuan

Tujuan dari penelitian ini yaitu :

Merancang sebuah perangkat lunak yang dapat digunakan untuk mengamankan sebuah data yang berupa dokumen dengan algoritma AES

(*Advanced Encryption Standard*) 128-bit untuk proses enkripsi dan dekripsi agar data tidak dapat dipahami oleh pihak yang tidak memiliki kunci ataupun tidak berhak menerima data tersebut.

1.5 Manfaat

Dari penelitian ini, manfaat yang didapat seperti berikut :

1. Untuk Penulis

Dapat menambah pengetahuan mengenai algoritma kriptografi yang khususnya pada proses mengenkripsi dan mendekripsi dalam mengamankan sebuah informasi.

2. Untuk Pembaca

Dapat menambah pengetahuan dan wawasan tentang kriptografi khususnya dalam memahami algoritma AES untuk mengamankan sebuah informasi.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab pendahuluan ini penulis mengutarakan latar belakang yang menjadi acuan judul penelitian, perumusan masalah, pembatasan masalah, tujuan, manfaat, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA DAN DASAR TEORI

Dalam bab ini berisi tentang beberapa dasar teori yang akan dijadikan acuan dalam perancangan dan pembuatan sistem, penelitian terdahulu serta kerangka berfikir. Penyelesaian model matematis, pengembangan sistem yang dibuat beserta perancangan pengujian.

BAB III : METODE PENELITIAN

Di dalam bab ini berisi sebuah langkah–langkah yang harus ditempuh penulis untuk memaparkan hal-hal yang berkaitan dengan kebutuhan sistem yang akan dibuat.

BAB IV : HASIL DAN ANALISIS PENELITIAN

Bab ini menyajikan implementasi sistem dan algoritma, yaitu penerapan desain yang telah dibuat di dalam kode program. Bab ini juga terdapat *testing* atau pengujian yang dilakukan terhadap sistem.

BAB V : KESIMPULAN DAN SARAN

Bab ini memuat kesimpulan dan saran yang di buat setelah membahas serta melakukan penelitian tersebut.