BAB I
PENDAHULUAN

1.1 Latar Belakang

Sejalan dengan perkembangan teknologi informasi dan komputer, maka cara masyarakat dalam berkomunikasi juga berubah. Komunikasi dapat dilakukan dengan teknologi seperti layanan pesan singkat.

Di zaman sekarang data dan informasi sebuah instansi merupakan hal yang sangat mahal, jika data dan informasi tersebut dapat di curi oleh kompetitor sebuah instansi akan menjadi hal yang berbahaya bagi keberlangsungan instansi yang datanya di curi. Untuk itu diperlukan sebuah metode untuk mengenkripsi data dan informasi tersebut sebelum dikirim, diperlukan juga sebuah metode untuk mendekripsi data dan informasi yang telah terenkripsi agar penerima data dan informasi bisa melihat *file* tersebut.

Di SD Islam Al Azhar 12 Cikarang setiap kali melakukan pengiriman data dan informasi masih rentan dilihat oleh pihak luar karena *file* yang dikirim tidak terenkripsi menggunakan algoritma AES ataupun algoritma lain. Oleh karena itu *file* yang terkirim bisa dimanfaatkan oleh pihak luar untuk dipakai tidak sebagaimana mestinya. Peneliti menyarankan agar sebelum data dan informasi dikirim *file* harus di enkripsi agar tidak terbaca menggunakan algoritma kriptografi *Advanced Encryption Standard* (AES).

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan *(Cryptography is the art and science of keeping messages secure)* selain itu ada pengertian tentang kriptografi yaitu kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [1]. Sedangkan algoritma asimetrik menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsinya, yaitu kunci umum *(public key)* yang digunakan untuk proses enkripsi suatu perubahan data teks asli *(plain text)* menjadi teks rahasia *(cipher text)* yang sifatnya tidak rahasia dan kunci pribadi *(private key)* yang digunakan untuk proses dekripsi yaitu pengembalian data

teks rahasia *(cipher text)* menjadi teks asli *(plain text)* yang sifatnya rahasia dan masing-masing pihak memiliki kunci pribadi yang berbeda.

Penggunaan kunci pribadi dapat digunakan untuk autentifikasi (pengenalan identitas pengirim) dan non repudiasi (pencegahan penyangkalan pengiriman data) karena dalam proses dekripsi dapat diketahui siapa pihak pengirim dengan melihat kunci pribadi yang dipakai. Ancaman adalah setiap insiden yang dapat berdampak negatif terhadap suatu aset contohnya diakses oleh pihak yang tidak berwenang. Ancaman dapat dikategorikan sebagai keadaan yang membahayakan kerahasiaan, integritas atau ketersediaan aset dan dapat disengaja atau tidak disengaja (Keamanan Sistem Informasi, Dr. Budi Raharjo, S.Kom., M.Kom., MM, 2021) [2].

Kriptografi memiliki banyak teknik dalam mengenkripsi data [3], diantaranya adalah Algoritma Cipher Transposisi, yaitu teknik pengenkripsian pesan dengan cara mengubah urutan huruf-huruf didalam pesan menjadi pesan yang acak dengan cara tertentu agar isi dari pesan tersebut tidak dapat dipahami kecuali oleh orang-orang tertentu.

Malasah yang terjadi saat pengiriman data dan informasi akan dapat dilihat isi dari data dan informasi tersebut jika *file* dari data dan informasinya tidak terenkripsi menggunakan kunci privat.

Perumusan RSA didasarkan pada teorema Euler, sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitan, meskipun proses enkripsi dan dekripsi menggunakan dua kunci yang berbeda hasilnya akan tetap benar. Kunci umum dan kunci pribadi yang digunakan adalah suatu bilangan prima, dan disarankan bilangan prima yang besar. Hal ini digunakan untuk pencegahan usaha pemecahan teks rahasia, karena semakin besar bilangan prima yang digunakan sebagai kunci maka semakin sulit mencari bilangan besar sebagai faktornya.

DES *(Data Encryption Standard)* yang pernah menjadi standar keamanan di Amerika Serikat, tetapi kemudian digantikan oleh AES *(Advanced Encryption Standard)* pada Mei 2005.

Pada tugas akhir ini dibangun sebuah aplikasi untuk pengamanan data dengan menerapkan algoritma AES untuk enkripsi dan dekripsi data. Dari penjelasan latar belakang diatas, maka penulis akan melakukan penelitian dan mengambil tugas akhir dengan judul **"Penerapan Algoritma *Advanced Encryption Standard* (AES) Pada Pengamanan Data".**

1.2 Identifikasi Masalah

Berdasarkan latar belakang diatas penulis dapat mengidentifikasi beberapa masalah sebagai berikut :

1. Mengkaji permasalahan sistem informasi dengan lebih detail kepada sistem keamanan menggunakan algoritma AES kriptografi;
2. Algoritma AES kriptografi akan dianalisa melalui serangan lubang keamanan pada enkripsi data;
3. Penggunaan *public key* dan *secret key* dalam proses enkripsi dan dekripsi data yang dilanjutkan dengan sistem verifikasi data.

1.3 Rumusan Masalah

Rumusan permasalahan yang akan dikaji dalam penelitian ini yaitu :

1. Bagaimana membangun aplikasi untuk pengamanan data dalam menjaga keamanan informasi dengan lebih detail menggunakan algoritma AES;
2. Bagaimana menerapkan Algoritma AES (*Advanced Encryption Standard)* pada aplikasi pengamanan data agar serangan lubang keamanan dapat dihindari menggunakan algoritma AES;
3. Bagaimana penerapan *public key* dan *secret key* dalam proses enkripsi dan dekripsi data yang dilanjutkan dengan sistem verifikasi data menggunakan kunci yang telah dibangkitkan.

1.4 Tujuan Penelitian

Berdasarkan identifikasi masalah diatas, adapun tujuan dari penelitian ini adalah :

1. Penerapan penggunaan algoritma AES kriptografi untuk keamanan data dengan enkripsi-dekripsi;
2. Memberi kemudahan pada user agar efisien dalam mengirim data dan informasi agar tidak di retas;
3. Pengiriman data aman karena data dan informasi sebelumnya telah di enkripsi.

1.5 Manfaat Penelitian

Adapun manfaat yang di dapat dari penelitian ini adalah sebagai berikut :

1. Dapat mempermudah dalam proses mengamankan data;
2. Hasil penelitian dapat dijadikan sebagai bahan bacaan dan referensi di perpustakaan Universitas Bhayangkara Jakarta Raya.

1.6 Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

1. Membangun Aplikasi sistem keamanan;
2. Aplikasi yang dibangun hanya menangani proses enkripsi-dekripsi data berupa teks kalimat, paragraph dan/atau file.

1.7 Sistematika Tugas Akhir

Sistematika penulisan penelitian tugas akhir ini diharapkan dapat mempermudah dan memahami materi yang ada pada penelitian ini. Berikut susunan dari setiap BAB yang ada didalam tugas akhir ini :

Bab I Pendahuluan

Bab ini menjelaskan tentang latar belakang masalah, identifikasi masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika tugas akhir yang dibuat sehingga tidak terjadi kegiatan menyimpang dari ketentuan yang telah ditetapkan untuk pembuatan sistem keamanan.

Bab II Tinjauan Pustaka

Bab ini berisikan bahasan yang memaparkan teori-teori pustaka pendukung yang dalam penelitiannya memiliki keterkaitan dengan pemecahan masalah dalam pembuatan sistem keamanan serta teori-teori dari penelitian sebelumnya.

Bab III Metodologi Penelitian

Bab ini menjelaskan obyek penelitian, kerangka penelitian, analisis sistem berjalan, analisis usulan sistem, analisis kebutuhan sistem yang diperlukan untuk mendukung pembuatan sistem keamanan.

Bab IV Perancangan Sistem Dan Implementasi

Bab ini menjelaskan tahapan-tahapan yang diperlukan pada penelitian secara garis besar yaitu perancangan sistem keamanan, metode yang digunakan, pengujiuan, dan implementasi fungsi pada sistem keamanan.

Bab V Penutup

Bab ini merupakan bagian penutup yang berisikan kesimpulan dan saran dari hasil penelitian yang telah dilakukan untuk pengembangan sistem lebih lanjut apabila ada pengembangan oleh peneliti lain.