BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dan telekomunikasi saat ini berkembang sangat pesat dan memberikan banyak pengaruh bagi kehidupan manusia. Hal yang paling jelas yang dialami saat ini adalah perkembangan jaringan *internet* yang sangat membantu manusia melakukan banyak kegiatan seperti bertukar data dan informasi dengan orang lain melalui *internet*. Namun seiring dengan meluasnya penggunaan jaringan *internet*, pengiriman informasi pun semakin rentan terhadap penyadapan yang dapat mengubah integritas data. Tulisan adalah salah satu media komunikasi yang sering digunakan untuk menyampaikan pesan kepada manusia. Pada kepentingan atau tujuan tertentu seseorang ingin mengirim pesan yang isi pesannya tidak ingin diketahui oleh orang lain selain si penerima pesan yang dituju karena isi pesan tersebut bersifat sangat rahasia atau pribadi. Tentu kejahatan dalam dunia maya merupakan hal yang sangat merugikan baik bagi pengguna *internet* maupun penyedia jasa *internet*. Namun kenyataannya banyak kasus pencurian data atau penyadapan data yang sangat rahasia bisa dibobol oleh pihak yang tidak bertanggung jawab yang biasa dikenal sebagai *cybercrime*. Untuk mengamankan data penting yang berupa informasi tersebut dibutuhkan suatu kriptografi.

Salah satu sarana dari *internet* yang digunakan untuk membaca dan mengirim pesan yaitu *email*. Mayoritas masyarakat menggunakan *internet* untuk membaca dan mengirim *email*. *Email* mengubah mekanisme komunikasi sehingga orang-orang dapat berkomunikasi jarak jauh dalam waktu yang relatif singkat. Pada perkembangannya *email* tidak hanya digunakan untuk mengirim pesan tulisan saja akan tetapi data-data elektronik tertentu juga dapat di kirim melalui sarana tersebut.

Jika pesan atau data yang dikirim dengan mengunakan sarana *email* dikirim melewati jaringan *public* maka tingkat keamanannya sangat beresiko. Teknik-teknik pencurian informasi dari sebuah *email* ini semakin canggih dari hari ke hari. Salah satunya adalah serangan *Man-In-The Middle*. Cara untuk memberikan keamanan data yaitu dengan menggunakan kriptografi, walaupun *attacker* atau

Man-In-The Middle berhasil mendapatkan data yang kita kirim namun tidak bisa mendapatkan informasi yang akurat karena teks yang didapat sudah ter-enkripsi sebelumnya. Sedangkan *Chipertext* yang didapat hanya bisa dibuka oleh pihak yang memiliki kunci *private* (Kunci untuk dekripsi).

Berbagai permasalahan tersebut dapat diatasi dengan proses enkripsi. Salah satu enkripsi yang cukup dikenal adalah dengan metode enkripsi AES (*Advanced Encryption Standar*). Metode enkripsi AES ini akan memberikan *private key* yang digunakan dalam proses enkripsi dan dekripsi. Pada penelitian ini ,algoritma AES akan implementasikan pada salah satu sarana komunikasi yaitu *email* . Sehingga diharapkan implementasi algoritma AES ini bisa menjadi salah satu cara pengamanan pengiriman data.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah yang akan dipecahkan/diselesaikan pada penelitian ini. Adapun pokok permasalahan dalam penelitian ini adalah :

1. Bagaimana enkripsi dan dekripsi pada teks?
2. Bagaimana encode dan decode base 64 *chipertext* hasil enkripsi AES?
3. Unjuk kerja sistem enkripsi data ?

1.3 Batasan Masalah

Agar masalah yang diteliti tidak menyimpang maka diperlukan suatu batasan masalah. Adapun batasan masalah pada penelitian ini adalah sebagai berikut :

1. Desain implementasi ini menggunakan algoritma kriptografi AES dalam proses enkripsi dan dekripsi dan base 64 pada pesan teks.
2. Inputan pada implementasi berupa teks dan maksimal pada pengujian yaitu 1 halaman.
3. Pembuatan program pendukung implementasi kriptografi AES menggunakan bahasa pemrograman PHP,HTML, CSS, dan Javascript

4. Pesan/data dapat dienkripsi/didekripsi jika *user* sama-sama menggunakan aplikasi ini.
5. Desain enkripsi data ini dengan membuat aplikasi berbasis *web* dan pengujiannya dengan dihubungkan ke imap(*internet message access protocol*) dan smtp(*simple mail transfer protocol*) gmail sebagai penunjangnya.

1.4 Maksud dan tujuan penelitian

Adapun maksud dan tujuan yang ingin dicapai dari penelitian ini adalah :

1. Adanya implementasi dan hasil analisa yang mampu ditunjukkan sebagai bukti bahwa algoritma kriptografi AES dan base64 mampu digunakan sebagai aplikasi yang bisa merahasiakan pesan *email* dan dokumen yang sulit dipecahkan dengan perhitungan tanpa bantuan komputer.
2. Menghasilkan sebuah aplikasi berbasis *web* yang berfungsi untuk mengenkripsi dan dekripsi pesan *email* serta dokumen dengan algoritma kriptografi AES dan base64 berbasis *web*.
3. Sebagai bahan penelitian yang dapat dikembangkan dan diperbaiki pada penelitian berikutnya.

1.5 Manfaat Penelitian

Manfaat yang akan didapat dari penelitian ini adalah sebagai berikut :

1. Dapat memberikan perlindungan terhadap informasi pesan maupun dekumen agar tidak mudah untuk diakses oleh pihak-pihak yang tidak bertanggung jawab.
2. Dapat digunakan sebagai bahan kajian untuk mengembangkan teknologi informasi terutama faktor yang berhubungan dengan keamanan.