

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. Aplikasi *Chatting* adalah salah satu media komunikasi yang sering digunakan untuk menyampaikan pesan. 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 *teknologi* yang digunakan dalam mengirim pesan yaitu aplikasi *chatting*, mayoritas pengguna *internet* berkomunikasi menggunakan *chatting* yang memungkinkan pengguna saling terhubung untuk melakukan komunikasi di tempat yang berbeda dengan relatif waktu yang singkat. Pada perkembangannya aplikasi *chatting* tidak hanya digunakan untuk mengirim pesan berupa teks tapi dapat berupa gambar, pesan suara dan lainnya .

Berbagai permasalahan tersebut dapat diatasi dengan proses enkripsi, yang cukup dikenal adalah dengan metode enkripsi *AES (Advanced Encryption Standar)* dan *base 64*. metode enkripsi ini akan memberikan *private key*. yang digunakan dalam proses enkripsi dan deskripsi, pada penelitian ini algoritma *AES-CBC* akan di implementasikan pada salah satu teknik berkomunikasi yaitu

chatting. sehingga diharapkan implementasi algoritma *AES-CBC* ini bisa menjadi salah satu cara mengamankan pesan dalam *chatting*.

1.2 Perumusan Masalah.

Adapun perumusan masalah dalam penelitian ini diantaranya adalah sebagai berikut:

1. Bagaimana rancangan antar muka pada aplikasi *chatting*?
2. Bagaimana Cara enkripsi dan dekripsi pada aplikasi *chat realtime*?
3. Bagaimana unjuk kerja enkripsi dan dekripsi data pesan?

1.3 Tujuan Penelitian.

Adapun perumusan masalah dalam penelitian ini diantaranya adalah sebagai berikut:

1. Membuat rancangan antar muka yang akan di gunakan untuk mengirim pesan dan membaca pesan.
2. Mengimplementasikan metode *kriptografi* yang dikembangkan ke dalam aplikasi *chatting*.
3. Mengetahui hasil dari dari unjuk kerja pada proses enkripsi dan deskripsi pesan.

1.4 Manfaat Penelitian.

Manfaat dari penelitian ini adalah kemudahan dan keamanan bagi para pengguna aplikasi *chat* dari orang-orang yang tidak bertanggung jawab yang ingin mengetahui isi pesan dalam chat tersebut.