BAB I PENDAHULUAN

Dalam perkembangan teknologi yang begitu cepat, komunikasi manusia sudah mengalami berbagai perubahan. Dalam bertukar informasi saat ini sudah tidak dibatasi oleh jarak, sekarang dalam komunikasi manusia dalam melakukan pertukaran pesan, telepon, maupun melalui internet. Saat ini internet merupakan teknologi yang paling sering digunakan dalam komunikasi antar manusia. Melalui internet manusia dalam mengirim email, pesan, gambar, video, audio dan lainnya.

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Kelompok (organisasi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap kegiatannya. Dari hal penggunaan komputerisasi tersebut, maka dibuatlah sebuah keamanan bagi seluruh aset-asetnya, terutama informasi-informasi dan data-data penting demi menjaga kerahasiaan informasi data tersebut. Dari keamanan data tersebut menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar dapat mengamankan data dari berbagai ancaman yang mungkin timbul. Ini merupakan latar belakang berkembangnya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi[6].

Komunikasi merupakan salah satu kebutuhan vital bagi manusia untuk bertahan hidup. Telah banyak inovasi dan terobosan untuk menciptakan layanan komunikasi yang bisa diandalkan. Salah satu contoh terobosan dan inovasi yang telah tercipta adalah aplikasi chatting. Aplikasi chatting saat ini menjadi media komunikasi alternatif yang digemari oleh banyak orang. Seiring dengan perkembangannya, aplikasi chatting dituntut untuk mampu mendistribusikan pesan instan dalam waktu yang sangat singkat. Aplikasi chatting juga memerlukan sistem keamanan yang baik untuk mengamankan pesan instan bersifat rahasia dan eksklusif. Masalah penyadapan pesan instan pada aplikasi yang berjalan di jaringan Internet juga menjadi isu krusial yang harus ditemukan solusinya[4].

Tuntutan perkembangan informasi yang begitu cepat dan mudah akhirnya membawa kehidupan manusia ke zaman yang lebih maju dan modern, dikarenakan kebutuhan informasi yang semakin tinggi. Untuk memenuhi kebutuhan informasi akhirnya mendorong pemikiran manusia untuk mengembangkan teknologi sehingga memberikan kemudahan dalam kehidupan manusia. Salah satu perkembangan di bidang telekomunikasi yang berkembang pesat adalah telepon seluler. Mulai dari ponsel yang hanya bisa menerima telepon dan pesan singkat hingga smartphone yang memiliki berbagai fungsi seperti multimedia, video streaming, transfer data. Berbagai operating system mobile bermunculan, salah satunya yang cukup dikenal yaitu Android[12].

Pada penelitian kali ini dirancang sebuah aplikasi pesan instan yang melakukan enkripsi pesan yang akan dikirim dengan kunci yang ditentukan pengirim. Aplikasi ini mengirimkan pesan yang terenkripsi sehingga pesan ini aman saat melalui jaringan internet sehingga mencegah terjadinya pembajakan pesan yang terkirim. Aplikasi chatting ini menggunakan enkripsi Algoritma AES. Algoritma AES digunakan untuk enkripsi pesan yang akan dikirim dan dekripsi pesan yang diterima agar dapat dibaca oleh pengguna.

A. Rumusan Masalah

Berdasarkan uraian diatas, maka dirumuskan masalah dari penelitian ini adalah bagaimana merancang aplikasi chatting dengan mengimplementasi algoritma AES untuk keamanan pesan

B. Tujuan

Merancang dan membangun aplikasi chatting dengan mengimplementasikan algoritma AES untuk keamanan pesan. Melakukan analisis terhadap pesan yang di enkripsi dan dekripsi untuk memastikan pesan yang diterima aman dan dapat didekripsi.

C. Batasan Masalah

Dalam penelitian ini penulisan membuat batasan masalah sehingga tidak menyimpang dari masalah yang telah dirumuskan, yaitu:

1. Aplikasi ini berbasis Android yang dirancang menggunakan bahasa kotlin dengan android studio sebagai IDE.
2. Mengirimkan pesan dari seorang pengguna ke seorang pengguna.
3. Database menggunakan Firebase realtime database.
4. Pesan yang dikirim hanya berupa teks.
5. Kunci yang digunakan merupakan kunci yang telah disepakati bersama oleh pengirim dan penerima secara langsung.
6. Kunci hanya terbatas pada 16 karakter