BAB I
PENDAHULUAN

1.1. Latar Belakang

Komputer dapat dengan mudah ditemukan sebagai alat pertukaran informasi atau data. Informasi atau data ada yang bersifat rahasia dan ada yang bersifat terbuka. Dalam pertukaran informasi atau data, berarti akan ada suatu informasi yang berpindah dari satu tempat ke tempat yang lain. Pada proses pertukaran informasi atau data rahasia dimungkinkan akan ada gangguan yang menyebabkan informasi rahasia yang dikirim dapat diketahui orang lain yang tidak seharusnya mengetahuinya. Untuk itu perlu adanya suatu upaya untuk menjaga informasi atau data tersebut dari ancaman keamanan.

Terdapat beberapa aspek dalam keamananan jaringan, yaitu keaslian sumber atau objek (*authentication*), kendali akses terhadap sumber daya (*access control*), kerahasiaan data (*data confidentiality*), keutuhan data (*data integrity*), *non-repudiation* (menghindari penolakan atas penerimaan/pengiriman data yang terkirim) dan ketersediaan layanan (*availability*). Aspek kerahasiaan merupakan upaya untuk menjaga kerahasiaan dari informasi yang bersifat *privat* agar tidak diketahui orang lain yang tidak memiliki hak akses.

Smartphone pun terus berkembang seiring perkembangan kebutuhan manusia yang menginginkan pertukaran informasi yang cepat. Aplikasi yang terpasang di *smartphone* yang sebelumnya hanya berfokus pada kebutuhan komunikasi, kini juga dapat memenuhi kebutuhan hiburan. Karena teknologi *smartphone* terus berkembang, maka aplikasi yang mendukung keamanan datanya pun harus terus dikembangkan, terutama pada komunikasi menggunakan pesan teks.

Untuk menjaga keamanan dan kerahasiaan dalam pertukaran pesan teks perlu adanya sebuah aplikasi yang dapat digunakan untuk menyembunyikan teks tersebut, yaitu dengan teknik kriptografi. Kriptografi telah lama digunakan untuk menjaga keamanan informasi seperti kerahasiaan dan keutuhan data. Dalam kriptografi dikenal istilah enkripsi dan dekripsi, yang merupakan satu pasang cara pada proses pengamanan informasi dengan metode tertentu. Dapat juga

menggunakan gabungan dari beberapa metode, seperti gabungan antara metode Rivest Code 6 (RC6) dan *Advanced Encription Standard* (AES).

Berdasarkan uraian di atas, penulis ingin membuat sebuah penelitian yang berjudul "Aplikasi Pengamanan Pesan Teks Menggunakan RC6 dan AES Berbasis Android". Penulis berharap penelitian ini dapat berguna untuk masyarakat luas dalam hal pengamanan pertukaran pesan teks dengan aplikasi pada *smartphone* berbasis Android.

1.2. Rumusan Masalah

Adapun rumusan masalah yang dapat didefinisikan dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mendesain perangkat lunak aplikasi kriptografi teks.
2. Bagaimana proses enkripsi dan dekripsi teks ke dalam teks aslinya.
3. Bagaimana unjuk kerja enkripsi dan dekripsi teks dengan metode RC6 dan AES pada *smartphone* berbasis Android.

1.3. Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mendesain perangkat lunak aplikasi kriptografi teks.
2. Melakukan enkripsi dan dekripsi teks ke dalam teks aslinya.
3. Menampilkan hasil unjuk kerja enkripsi dan dekripsi teks dengan metode RC6 dan AES pada *smartphone* berbasis Android.

1.4. Manfaat

Manfaat dari penelitian ini adalah terimplementasinya kriptografi dengan metode RC6 dan AES pada sebuah aplikasi berbasis android sehingga pengguna dapat mengamankan pesan melalui enkripsi dan dekripsi suatu pesan teks pada perangkat Android.