BAB I
PENDAHULUAN

1.1 Latar Belakang

Kerahasiaan dan keamanan data adalah hal yang sangat penting dalam komunikasi, baik dengan tujuan keamanan bersama maupun untuk privasi individu tak terkecuali ponsel androidpun sangat berkembang pesat, banyak fitur – fitur aplikasi yang disediakan salah satunya yaitu SMS (*Short Message Service)* yang sampai saat ini masih banyak digunakan untuk berbagi pesan singkat kepada rekan kerja dan keluarga untuk saling bertukar informasi tetapi seiring berkembangnya waktu proses keamanan dalam melakukan pengiriman data pun semakin rawan. Fitur layanan SMS saat ini belum memiliki standar keamanan yang baik. Hal-hal tersebut menyebabkan kurang terjaminnya kerahasiaan pesan pengirim.

Pesan yang dikirim mengunakan aplikasi SMS masih berupa teks terbuka belum terproteksi dengan kata lain pesan teks yang dikirimkan tidak langsung diterima oleh penerima tetapi pesan tersebut harus melewati *Short Message Service Center* (SMSC). SMSC berfungsi untuk mencatat komunikasi yang terjadi antara pengirim dan penerima SMS, semuanya tersimpan pada SMSC, hal ini menyebabkan seorang operator dapat memperoleh informasi atau membaca SMS didalam SMSC. Dari beberapa kasus yang terjadi dimana pihak berwenang seperti kepolisian, kejaksaan, atau KPK dapat meminta transkrip SMS ke operator untuk dijadikan bahan penyelidikan dipersidangan. Hal ini menunjukan bahwa pesan SMS yang dikirimkan tersebut belum terproteksi sehingga pesan–pesan yang dikirimkan dapat dibaca oleh pihak lain, Sehingga pihak lain tersebut dapat dengan mudah dan bebas untuk membuka data penting kita. Oleh karena hal itu dibutuhkan keamanan tambahan untuk mengamankan pesan–pesan penting yang akan dikirim melalui SMS agar data dalam handphone dapat aman dan kerahasiaan data akan tetap terjamin. Karena beberapa hal di atas, dibutuhkan sebuah teknik untuk menjaga kerahasiaan tersebut. Teknik tersebut adalah kriptografi, Kriptografi adalah ilmu untuk menjaga kerahasiaan informasi dari aspek –aspek, yang dapat

mengancam keamanan suatu informasi dengan metode dan teknik matematika tertentu. Dengan isi informasi yang asli (*plaintext*) diubah menjadi informasi acak (*cipherteks*) terlebih dahulu, yang sama sekali tidak memiliki makna.

Berdasar uraian di atas, penulis mencoba mengimplementasikan algoritma didalam satu aplikasi perangkat lunak oleh karena itu penulis mengambil judul "Aplikasi Pengamanan Pesan SMS Menggunakan Algoritma Kriptografi RC6 Berbasis *Android*".

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah sebagai berikut:

1. Bagaimana pesan yang dikirim melaui media SMS dapat terkirim dengan aman.
2. Bagaimana mengimplementasikan algoritma RC6 pada aplikasi pengamanan pesan SMS.

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini sebagai berikut:

1. Perangkat lunak yang dibangun merupakan perangkat lunak yang diterapkan pada telepon selular yang bersistem operasi *android*.
2. Dua belah pihak pengguna harus sama – sama menggunakan aplikasi ini.
3. Enkripsi yang dilakukan adalah enkripsi data SMS.
4. Batasan karakter dalam aplikasi ini yaitu 160 karakter.
5. Aplikasi hanya dapat mengirim dan menampilkan pesan.
6. Dalam proses pengiriman pesan mengunakan jaringan *provider* SIM *Card* pada perangkat *android*, dan bagi perangkat *android* dengan fitur dual SIM *Card*, maka aplikasi akan mendeteksi pengunaan SIM *Card* pada *slot* SIM 1 (slot utama).

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk membangun aplikasi pengamanan pengiriman pesan dengan teknik kriptografi menggunakan algoritma RC6 yang

mampu bekerja pada perangkat *android*, sebagai aplikasi pihak ketiga yang mampu melakukan enkripsi dan dekripsi data teks pesan sebelum dan sesudah di kirimkan.

1.5 Manfaat Penelitian

Manfaat penelitian ini secara umum yaitu:

1. Aplikasi yang dibangun mampu bekerja pada perangkat *android*, sebagai aplikasi pihak ketiga yang mampu melakukan enkripsi dan dekripsi pesan teks.
2. Menjaga kerahasiaan pesan agar tetap aman sehingga tidak dapat dengan mudah dan bebas membuka data penting dari tangan atau pihak yang tidak bertanggungjawab.

Adapun manfaat peneltian secara khusus diantaranya adalah:

1. Dapat memahami bagaimana teknik pengamanan pengiriman pesan melalui jaringan SMS.
2. Perancangan *prototyping* untuk mempermudah implementasi teknik kriptografi pengamanan pesan dengan algorima RC6.
3. Mengurangi resiko penyalahgunaan hak akses membuka, membaca isi pesan bahkan menyisipkan isi pesan tersebut dari pihak-pihak yang tidak bertanggung jawab.