BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi yang ada pada saat ini mampu menciptakan berbagai macam perangkat keras yang dapat digunakan untuk mengirim atau menerima informasi dengan cepat dan mudah.Penggunaan *handphone* sebagai *device* akses informasi telah berkembang pesat pada era ini.Terlebih lagi, banyak aplikasi *mobile* yang diciptakan, membuat informasi-informasi yang dibutuhkan mudah untuk didapat. Para *operating system* pada *handphone* pun telah berhasil membuat *device* komunikasi tersebut menjadi sebuah *smartphone* dengan fungsionalitas lebih baik. Salah satu perangkat keras yang cukup banyak digunakan pada saat ini adalah smartphone android.Banyak merk dan jenis smartphone android beredar di pasaran.

Banyak fitur-fitur aplikasi yang disediakan oleh Android sebagai system operasi pemutar video,*push mail*,mengakses layanan internet dan sebagainya. Akan tetapi fitur-fitur yang digunakan seperti ponsel biasa lainya yaitu seperti *Short Message Service* (SMS), *call*, dan *Multimedia Message Service* (MMS) masih dapat digunakan pada perangkat android tersebut. Dari sekian banyak fitur yang dimiliki Android,salah satunya yang masih banyak digunakan yaitu SMS, bahwa pengguna dapat mengirim dan menerima pesan singkat kepada pengguna ponsel lainya.

Layanan SMS yang menggunakan aplikasi SMS bahwa ponsel masih banyak digunakan oleh setiap orang, dan merupakan bukan jalur yang aman dalam pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi selain itu pengiriman SMS yang dilakukan tidak sampai kepenerima secara langsung, akan tetapi pengiriman SMS harus melewati *Short Message Service Center* (SMSC) yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima.

Dengan tersimpanya SMS pada SMSC,maka seorang operator dapat memperoleh informasi atau membaca SMS di dalam SMSC tersebut, hal ini dapat dibuktikan dari beberapa kasus yang ditangani pihak kepolisian, kejaksaan atau KPK,dimana pihak-pihak tersebut meminta transkip SMS ke operator untuk dijadikan bahan penyelidikan di persidangan.

Dengan demikian dibutuhkan suatu metode dan aplikasi yang dapat mempertimbangkan solusi *encrypted end to end* dengan melakukan enkripsi terhadap pesan SMS. Enkripsi adalah proses mengubah suatu pesan asli yamg disebut plaintext menjadi sebuah sandi atau kode yang tidak terbaca yang disebut chipertext dan tidak dapat dimengerti, untuk mengembalikan pesan kebentuk asli seperti semula diperlukan proses yang disebut dekripsi. Enkripsi dimaksudkan untuk melindungi dan menyamarkan informasi agar tidak terlihat oleh pihak atau orang yang bukan seharusnya.

Dunia kriptografi saat ini semakin mudah dengan adanya aplikasi kriptografi dimana pengguna tidak lagi membutuhkan waktu yang lama,rumit dan berpotensi dan menimbulkan kesalahan. Dengan menggunakan algoritma yang

ada pengguna dapat dengan mudah meng-enkripsi sebuah teks hanya dengan sekali klik.Sayangnya jumlah aplikasi kriptografi yang ada saat ini sangat minim, terutama di sistem operasi android.

Oleh karena itu, penulis mencoba merancang sebuah aplikasi kriptografi untuk telepon seluler berbasis Android dengan algoritma enkripsi yang kuat. Aplikasi ini sangat berguna untuk mempermudah penyandian suatu informasi tanpa harus membutuhkan waktu yang lama, rumit dan memahami algoritma ataupun cara kerjanya. Salah satu metode enkripsi yang umum digunakan yaitu menggunakan algoritma enkripsi dan kunci yang dapat diubah-ubah sesuai kesepakatan untuk meningkatkan keamanan. Teknik ini disebut sebagai algoritma kunci simetris (*symetric key*) yaitu suatu enkripsi dengan menggunakan kunci yang sama untuk melakukan proses enkripsi dan dekripsi. Contoh algoritma kunci simetris yaitu *Rivest Code* 6 (RC6) yang dirancang oleh Ronald L. Rivest, M.J.B.Robshow, R. Sidney dan Y.L. algoritma ini merupakan pengembangan dari algoritma sebelumnya yaitu RC5.

1.2 Rumusan Masalah

Untuk proses analisis dan perancangan sebuah aplikasi membutuhkan ketelitian. Sedangkan, ilmu kriptografi membutuhkan ide dan kreatifitas, bermodalkan algoritma kriptografi yang *logic* serta *software* yang memudahkan perancangan sampai pembuatan aplikasi yaitu eclips maka penulis membuat rumusan masalah:

1. Bagaimana menerapkan algoritma *Rivest Code* 6 (RC6) pada enkripsi SMS berbasis android ?
2. Bagaimana mengevaluasi algoritma kriptografi RC6 yang telah diimplementasi diaplikasi SMS ini?

1.3 Batasan Masalah

Dalam pembuatan skripsi ini ditentukan suatu batasan masalah yang bertujuan untuk memudahkan pengerjaan dan menghindari adanya kegiatan di luar sasaran yang tidak diinginkan. Batasan-batasan tersebut adalah:

1. *Software* yang digunakan untuk membuat aplikasi adalah Eclips.
2. Metode yang digunakan adalah algoritma *Rivest Code* 6 (RC6).
3. Kunci yang dimasukan untuk proses dekripsi yaitu sama dengan kunci yang digunakan pada saat proses enkripsi.
4. Kedua belah pihak harus pengguna harus menggunakan aplikasi ini.
5. Aplikasi ini berjalan pada ponsel dengan menggunakan sistem operasi Android minimal versi 2.2 *(Froyo)*.

1.4 Tujuan Penelitian

Tujuan dari pembuatan skripsi ini adalah :

1. Menerapkan algoritma RC6 untuk aplikasi enkripsi atau dekripsi pesan sebagai upaya mengamankan suatu informasi pada layanan pesan singkat (SMS) .

2. Untuk memenuhi salah satu syarat kelulusan Strata Satu di Sekolah Tinggi Manajemen Informatika dan Komputer Amikom Yogyakarta jurusan Teknik Informatika.

1.5 Manfaat Penelitian

Manfaat yang didapat dengan adanya aplikasi ini adalah:

1. Membantu mengamankan sebuah pesan yang sifatnya rahasia.
2. Memberikan kemudahan dalam proses pengiriman pesan melalui perangkat *mobile* dengan lebih aman.
3. Menambah pengetahuan tentang keamanan pesan.

1.6 Metodologi Pengumpulan Data

Dalam melakukan penelitian dan pembuatan skripsi ini penulis mengumpulkan data melalui beberapa metode agar data yang terkumpul menjadi informasi yang lengkap, tepat dan terstruktur. Oleh karena itu metode-metode penelitian tersebut adalah sebagai berikut:

1. Metode Studi Literatur

   Metode pengambilan data menggunakan berbagai macam literature yaitu dengan mencari informasi di berbagai *website*yang memiliki konten berkaitan dengan dunia kriptografi modern.

2. Metode kepustakaan

Metode kepustakaan dengan membaca buku-buku literature, dokumen, catatan kuliah dan bacaan lainya sebagai referensi yang berhubungan dengan permasalahan.

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam penelitian ini yaitu :

BAB I : PENDAHULUAN

Pada bab ini berisikan Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Metodologi Pengumpulan Data dan Sistematika Penulisan.

BAB II : LANDASAN TEORI

Landasan Teori ini adalah kumpulan dari studi pustaka penulis yang didalamnya membahas seputar teori-teori yang mendukung dalam pembuatan penelitian ini.

BAB III : ANALISA DAN PERANCANGAN SISTEM

Bab ini membahas tentang analisis terhadap sistem yang akan dibuat seperti kebutuhan apa saja yang diperlukan untuk membuat aplikasi, UML, rancangan *user interface* dan rancangan tentang aplikasi yang akan dibuat.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Dalam bab ini akan dijelaskan secara lengkap tentang tahap-tahap perancangan dan pembuatan program. Tentang cara kerja sistem dan pembahasan, serta melakukan pengujian aplikasi yang akan dibuat.

BAB V : PENUTUP

Pada bab ini akan membahas tentang kesimpulan penelitian dan saran yang dituliskan oleh penulis.