

BAB I

PENDAHULUAN

I.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. Perangkat keras yang cukup banyak digunakan pada saat ini adalah *smartphone* android. Banyak merek dan jenis *smartphone* android beredar di pasaran.

Layanan pesan singkat menggunakan aplikasi SMS pada ponsel masih banyak digunakan, namun bukan jalur yang aman untuk pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi, selain itu proses pengiriman SMS tidak sampai ke penerima secara langsung, akan tetapi pengiriman SMS harus melewati *Short Message Service Center (SMSC)* yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima.

Dengan tersimpannya 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 kepolisian, kejaksaan atau KPK, dimana pihak penyelidik tersebut meminta transkrip 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 yang disebut *plaintext* menjadi sebuah sandi atau kode yang tidak terbaca yang disebut *chipertext* dan tidak dapat dimengerti, untuk mengembalikan pesan ke bentuk 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.

Berdasarkan latar belakang yang telah dijabarkan di atas, maka dalam penelitian ini penulis memilih judul “**Perancangan Aplikasi Keamanan Pesan SMS Menggunakan Algoritma Kriptografi RC6 Berbasis Android**”.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikas Masalah

Adapun identifikasi masalah yang ada yaitu sebagai berikut :

1. Pengiriman teks SMS ke penerima yaitu dalam bentuk byte plain sehingga mudah untuk disadap oleh orang yang tidak bertanggung jawab.
2. Mengenkripsi isi pesan SMS dengan menggunakan metode kriptografi agar pesan tersebut sulit untuk dibaca.
3. Kerahasiaan merupakan faktor penting untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi tersebut.

I.2.2. Rumusan Masalah

Berikut ini beberapa rumusan masalah dalam penelitian ini yang akan dicari penyelesaiannya, antara lain :

1. Bagaimana cara merancang sebuah aplikasi SMS dengan pengamanan teks menggunakan algoritma RC6
2. Bagaimana membuat sebuah penyandian SMS dengan menggunakan metode RC6 untuk mengamankan sebuah SMS dari orang-orang yang tidak berhak.

I.2.3. Batasan Masalah

Batasan yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Implementasi program pada smartphone android.
2. Aplikasi akan dikembangkan untuk android dengan versi minimal android (froyo) dengan level API 8.
3. Aplikasi dibangun dengan target android versi 4.1 (jelly bean) dengan level API 18.
4. Proses enkripsi dan dekripsi pesan hanya digunakan untuk data text berupa huruf, angka dan symbol.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk membuat aplikasi pengamanan teks SMS menggunakan RC6.
2. Memahami dan mengetahui bagaimana cara sebuah aplikasi implementasi algoritma RC6 untuk enkripsi dan dekripsi data pada *smartphone* android.
3. Menghasilkan sebuah aplikasi yang bisa bermanfaat untuk mengamankan data SMS pada *smartphone* android.

I.3.2. Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Membuat sebuah program aplikasi untuk mengamankan data dalam aplikasi android.
2. Membuat pengguna SMS pada android mejadi lebih aman, nyaman dan mudah dalam penggunaan SMS.
3. Membantu pemahaman tentang kriptografi terutama mengenai algoritma RC6.

I.4. Metode Pengumpulan Data

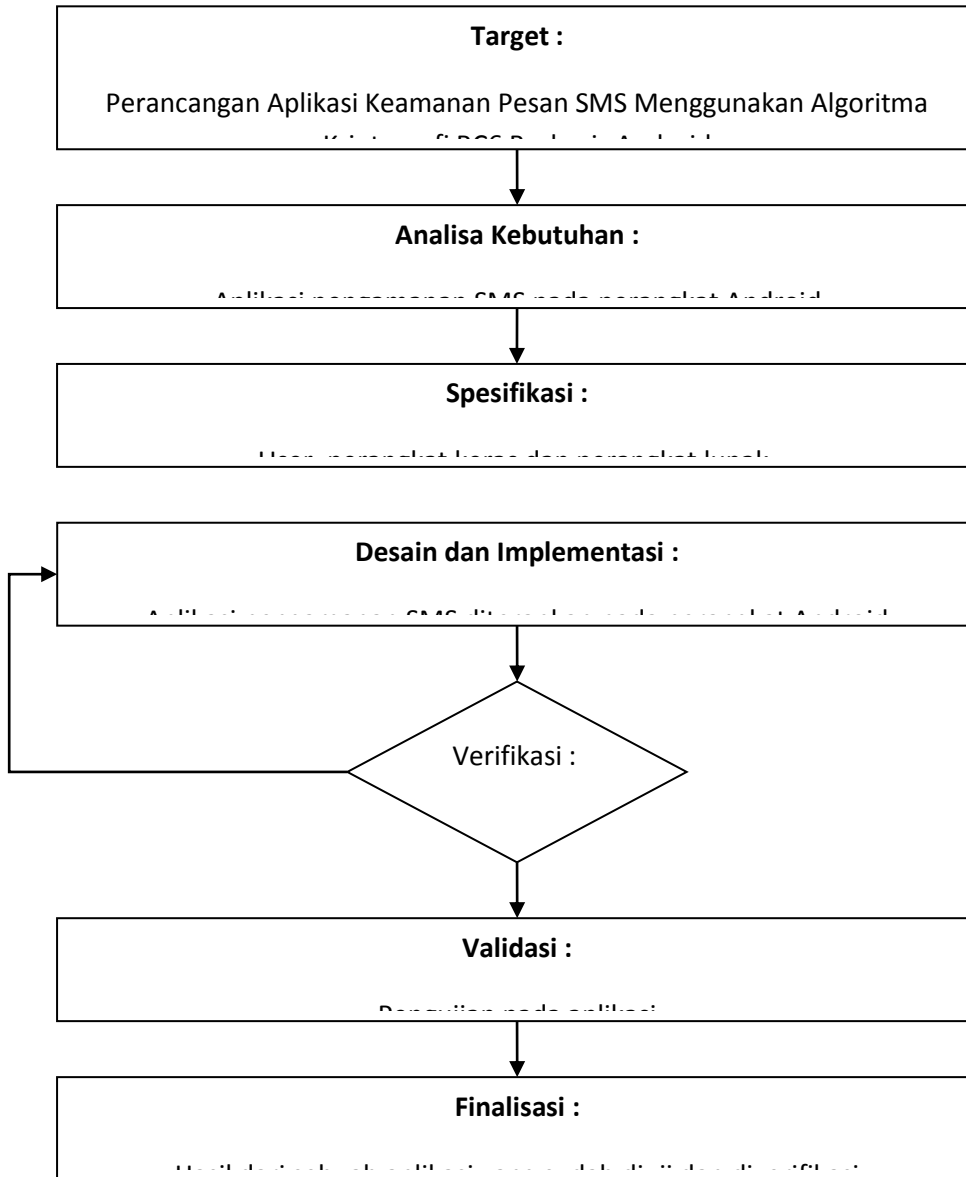
Adapun langkah-langkah yang akan ditempuh dalam proses penelitian selama penulisan skripsi ini adalah sebagai berikut :

A. Metode Pengumpulan Data, yaitu :

- a. Studi Literature, penulisan ini dimulai dengan studi keperustakaan, yaitu dengan mengumpulkan bahan-bahan referensi baik dari buku, artikel jurnal, makalah, situs internet, konsep matematis yang mendasarinya dan bahasa pemograman untuk pembuatan aplikasinya, juga beberapa referensi lainnya untuk pencapaian tujuan skripsi yang dibuat.
- b. Metode wawancara melakukan wawancara kepada pihak yang tarkait mengenai perancangan aplikasi yang berjalan dan diinginkan sehingga nantinya aplikasi ini dapat dimanfaatkan dan digunakan.
- c. Metode observasi, melakukan pengamatan langsung bagaimana menggunakan SMS serta Keamanannya untuk mengetahui langkah-langkah yang perlu diambil dalam perancangan aplikasi ini.

B. Metode Perancangan, yaitu :

a. Prosedur Perancangan, berisi tata cara dan langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan.



Gambar I.1. Flowchart Prosedur Perancangan

b. Analisa Kebutuhan, berisi tentang hal-hal yang harus ada pada hasil perancangan agar mampu menyelesaikan masalah yang ada sesuai tujuan.

- c. Spesifikasi dan Desain, Berdasarkan spesifikasi dalam perancangan aplikasi pengamanan SMS pada Perangkat *smartphone* menggunakan *eclipse* dan *sdk* dengan bahasa pemrograman Java untuk merancang aplikasi SMS ini.
- d. Implementasi dan Verifikasi, dalam perancangan aplikasi kompresi SMS pada perangkat *smartphone*, diimplementasikan menggunakan *eclipse* dan *sdk* sebagai tempat penulisan coding program tersebut.
- e. Validasi, berisi langkah-langkah yang dilakukan saat pengujian terhadap aplikasi untuk mengetahui sejauh manakah kesuksesan program yang telah dirancang.
- f. Finalisasi, mendapatkan hasil akhir aplikasi yang telah diuji dan diverifikasi.

I.5. Keaslian Penelitian

Keaslian penelitian ini berdasarkan pada beberapa penelitian terdahulu yang mempunyai karakteristik yang relatif sama dalam hal tema kajian, meskipun berbeda dalam hal kriteria subjek, jumlah, platform yang digunakan dan posisi variabel penelitian atau metode analisis yang sudah digunakan. Penelitian yang akan dilakukan mengenai pengamanan SMS pada *smartphone* berbasis android.

Adapun penelitian yang terkait dengan penelitian ini adalah :

Tabel I.1. Keaslian Penelitian

No	Penelitian	Judul Penelitian	Hasil Penelitian
1	Yuli Uswiratri, 2011	Implementasi Algoritma RC6 untuk Enkripsi Citra pada MMS dengan Menggunakan J2ME	Aplikasi Enkripsi pada MMS Berbasis J2ME / Symbian
2	Hartanius Gea, 2015	Perancangan Aplikasi Pengamanan SMS Pada Mobile Device Dengan Metode RC6	Perancangan Aplikasi Pengamanan SMS Pada Mobile Device Dengan Metode RC6
3	Hendra, 2013	Aplikasi Pengaman Pertukaran SMS Pada Perangkat Android	Aplikasi Pengaman Pertukaran SMS Berbasis Symbian
4	M. Amin, 2016	Perancangan Aplikasi Keamanan Pesan SMS Menggunakan Algoritma Kriptografi RC6 Berbasis Android	Perancangan Aplikasi Keamanan Pesan SMS Menggunakan Algoritma Kriptografi RC6 Berbasis Android

I.6. Sistematika Penulisan

Langkah dan tahapan yang ditempuh dalam menyelesaikan penulisan ini adalah :

BAB I PENDAHULUAN

Dalam BAB ini di bahas mengenai Latar Belakang, Identifikasi Masalah, Batasan Masalah, Tujuan dan Manfaat Penelitian, Metodologi yang digunakan serta Sistematika Penulisan ini sendiri.

BAB II TIJAUAN PUSTAKA

Pada BAB ini dijelaskan teori-teori yang berkaitan dengan pembuatan, desain dan tampilan rancangan aplikasi enkripsi folder, serta teori-teori yang mendukung analisa penelitian.

BAB III ANALISIS DAN DESAIN SISTEM

Berisi tentang analisa dan perancangan aplikasi, yang meliputi analisa masalah, perancangan *interface*, perangkat yang digunakan, algoritma serta ketentuan pengguna.

BAB IV HASIL DAN PEMBAHASAN

Pada BAB ini berisikan tentang tampilan hasil, pembahasan, kelebihan dan kekurangan dari sistem yang dirancang.

BAB V KESIMPULAN DAN SARAN

BAB ini merupakan penutup dari penulis laporan Skripsi ini yang berisikan kesimpulan atas hasil analisa dan perancangan serta berisikan saran-saran.