BAB I

PENDAHULUAN

I.1. Latar Belakang

Di era globalisasi saat ini, mendapatkan informasi sangatlah mudah. Setiap orang dengan mudah mendapatkan data ataupun berita yang diinginkan. Hal ini didukung dengan teknologi informasi dan komunikasi yang terus berkembang pesat dari tahun ke tahun. Akan tetapi kemudahan mendapatkan informasi juga memberikan ancaman. Beberapa ancaman yang diberikan adalah masalah tentang keamanan, kerahasiaan, dan keotentikan data. Oleh karena itu diperlukan suatu sistem pengamanan data yang bertujuan untuk meningkatkan keamanan data, melindungi suatu data atau pesan agar tidak dibaca oleh pihak yang tidak berwenang, dan mencegah pihak yang tidak berwenang untuk menyisipkan, menghapus, ataupun merubah data.

Aplikasi pengiriman *email* saat ini tidak memiliki fitur untuk mengamankan data didalamnya, sehingga siapa saja dapat mengetahui isi dari *email* tersebut. Untuk itu dibutuhkan sebuah aplikasi dengan sebuah metode yang dapat melakukan pengamanan data *email*.

Salah satu ilmu pengamanan data yang terkenal adalah kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna.

Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau plainteks menjadi cipherteks (teks

tersandi). Sedangkan dekripsi adalah proses penyandian kembali cipherteks menjadi plainteks.

Salah satu metode enkripsi yang terkenal adalah metode RC4. RC4 pertama kali dibuat oleh Ron Rivest di Laboraturium RSA pada tahun 1987. RC4 (Rivest Cipher 4) adalah sebuah synchrone stream cipher, yaitu cipher yang memiliki kunci simetris dan mengenkripsi plainteks secara digit per digit atau byte per byte dengan cara mengkombinasikan dengan operasi biner (biasanya XOR) dengan sebuah angka semi acak.

Dengan menggunakan algoritma RC4 pengirim dan penerima *email* dapat mengirimkan data *email* yang telah diamankan, sehingga informasi dari data *email* itu hanya dapat diketahui oleh pengirim dan penerima *email*.

Berdasarkan latar belakang diatas, maka pada skripsi ini akan dirancang "**Implementasi Algoritma RC4 Dalam Pengamanan Data Email Berbasis Android**".

I.2. Ruang Lingkup Permasalahan

I.2.1.Identifikasi Masalah

Adapun hal-hal yang menjadi identifikasi masalah aplikasi ini adalah :

1. Pesan teks yang dikirimkan melalui *email* tidak cukup aman karena dapat dibaca oleh pihak yang tidak diinginkan.
2. Dibutuhkan sebuah metode yang aman untuk dapat mengirimkan pesan melalui *email* sehingga isi pesan tersebut hanya dapat dipahami antara pengirim dan penerima.

I.2.2. Perumusan Masalah

Berikut penulisan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini, antara lain :

1. Bagaimana merancang dan membuat sebuah aplikasi pengamanan data *email* menggunakan algoritma RC4 pada perangkat *mobile* berbasis android ?
2. Bagaimana penggunaan bahasa pemrograman dalam membangun aplikasi pada perangkat *mobile* berbasis android ?
3. Bagaimana penggunaan algoritma RC4 dalam pengamanan data *email* ?

I.2.3. Batasan Masalah

Dalam penulisan skripsi ini dibatasi permasalahannya sebagaiberikut :

1. Aplikasi pada perangkat *mobile* menggunakan bahasa pemrograman JAVA.
2. Aplikasi ini dibuat sebagai pengaman data teks yang akan dikirimkan melalui *email*.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut :

1. Menghasilkan aplikasi enkripsi dan dekripsi untuk melakukan pengamanan data teks pada pengiriman *email*.
2. Melakukan analisa dari hasil pengujian aplikasi.

I.3.2. Manfaat

Adapun manfaat yang dapat diambil dalam penulisan skripsi ini adalah:

1. Sebagai bentuk realisasi teori-teori yang diterima menjadi sebuah aplikasi.
2. Dapat digunakan untuk melakukan enkrip pada pesan teks yang akan dikirim melalui *email* dan dapat di dekrip oleh penerima, sehingga keamanan informasi yang ada pada *email* hanya diketahui antara pengirim dan penerima.
3. Sebagai referensi bagi pembaca yang ingin membuat aplikasi kriptografi.

I.4. Metodologi Penelitian

Untuk dapat mengimplementasikan sistem di atas, maka secara garis besar digunakan beberapa metode sebagai berikut:

I.4.1. Metode Pengumpulan Data

Sistem yang dirancang tentunya memerlukan pengumpulan data, dalam proses pengumpulan data terdapat beberapa cara, berikut diantaranya :

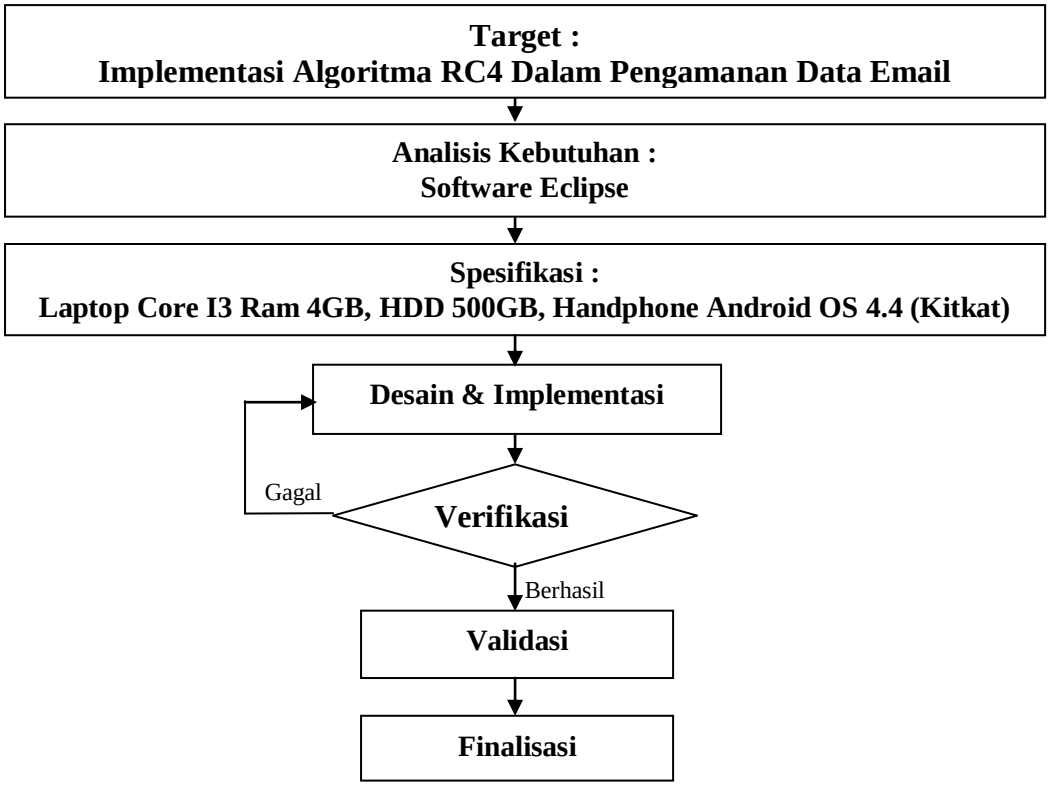
a. Studi Literatur, dengan cara mempelajari buku-buku acuan dan literatur yang berhubungan dengan materi dalam penulisan skripsi.
b. Pengamatan, yaitu pengumpulan data dan informasi yang dilakukan dengan cara menganalisa aplikasi kriptografi yang sudah ada.
c. Wawancara, yaitu pengumpulan data dengan cara melakukan tanya jawab dengan orang yang memahami metode perhitungan kriptografi.
d. Searching, yaitu penulis mencari data-data yang mendukung penulisan skripsi melalui internet.

I.4.2. Metode Perancangan Sistem

Dalam merancang sistem agar mencapai hasil yang diharapkan dilakukan tahap-tahap sebagai berikut :

1. Prosedur Perancangan

Langkah – langkah yang diperlukan untuk mencapai tujuan perancangan dapat dilihat pada gambar I.1. di bawah ini :



Gambar I.1.Prosedur Perancangan

2. Analisis Kebutuhan

Setelah melalui tahap prosedur perancangan, maka tahap selanjutnya adalah analisa kebutuhan yaitu hal-hal yang diperlukan untuk perancangan sistem

berupa perangkat lunak dan perangkat keras yang dibutuhkan untuk membangun aplikasi.

3. Spesifikasi

Dalam membuat skripsi ini, spesifikasi dari perangkat keras (*Hardware*) dan perangkat lunak (*Software*) yang digunakan adalah :

a. Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan antara lain :

1. Laptop:*Core i3 Processor*
2. *Hard disk* : 500 GB
3. RAM 4 GB

b. Perangkat lunak (*Software*)

Software yang digunakan untuk membuat skripsi ini antara lain :

1. Sistem operasi Windows *7*
2. Adobe Dreamweaver CS6
3. Xampp
4. Eclipse Juno

4. Desain dan Implementasi

Pada tahap ini dirancang sebuah desain dari aplikasi pengamanan data *email* menggunakan algoritma RC4. Bagaimana desain yang akan digunakan pada antarmuka perangkat *mobile*. Setelah dilakukan perancangan desain aplikasi selanjutnya melakukan implementasi terhadap desain yang telah dirancang kedalam bahasa pemrograman JAVA.

5. Verifikasi

Verifikasi dilakukan untuk memeriksa ulang apakah aplikasi telah dibuat sesuai dengan apa yang direncanakan dalam perancangan yang akan digunakan dalam pembuatan aplikasi ini. Apakah desain yang dirancang dapat diimplementasikan kedalam bahasa pemrograman.

6. Validasi

Pada tahap ini dilakukan pengujian aplikasi pengamanan data *email* menggunakan algoritma RC4 secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan aplikasi. Pengujian fungsional dilakukan untuk mengetahui bahwa aplikasi pengamanan data *email* menggunakan algoritma RC4 telah berjalan dengan sesuai dengan perancangan. Pengujian ketahanan merupakan kemampuan aplikasi untuk berjalan dengan baik pada spesifikasi minimum komputer sesuai dengan yang telah dicantumkan.

I.4.3. Keaslian Penelitian

Terdapat beberapa penelitian sebelumnya yang berhubungan dengan penelitian yang akan penulis lakukan, yaitu :

Tabel 1. Tabel Perbandingan Penelitian

No.	Peneliti	Judul	Hasil	Perbedaan Dengan Aplikasi Yang Dirancang
1.	Winda Erika, et al., 2012.	Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)	Aplikasi pengmanan data email dengan algoritma RSA.	Algoritma yang digunakan adalah algoritma RSA.
2.	Wibowo dan Suprayogi, 2014.	Aplikasi Enkripsi Email Dengan Menggunakan Metode Blowfish Berbasis J2SE	Aplikasi pengmanan data email dengan algoritma blowfish.	Algoritma yang digunakan adalah algoritma blowfish.

I.4.4. Pengujian/Uji Coba Sistem yang Dirancang

Dilakukan untuk mengetahui apakah pekerjaan pemrograman dalam pembuatan aplikasi telah dilakukan secara benar sehingga menghasilkan fungsi-fungsi yang dikehendaki. Pengujian juga dimaksudkan untuk mengetahui keterbatasan dan kelemahan program aplikasi yang dibuat untuk sebisa mungkin dilakukan penyempurnaan.

I.5. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam penulisan skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metodologi penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan aplikasi yang dirancang serta kelebihan dan kekurangan aplikasi yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk implementasi algoritma RC4 dalam pengamanan data email berbasis android.