

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: “cryptós” artinya “secret” (rahasia), sedangkan “gráphein” artinya “writing” (tulisan). Jadi, kriptografi berarti *secret writing* (tulisan rahasia) (Munir, 2006)

Android adalah sebuah sistem operasi untuk perangkat mobile berbasis Linux yang mencakup sistem operasi, *middleware* dan aplikasi. Android menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka (Safaat, 2012).

Short Message Service (SMS) adalah suatu fasilitas untuk mengirim dan menerima suatu pesan singkat berupa teks melalui perangkat nirkabel, yaitu perangkat komunikasi telepon selular, dalam hal ini perangkat nirkabel yang digunakan adalah telepon selular. Salah satu kelebihan dari SMS adalah biaya yang murah. *Short Message Service* disingkat dengan SMS, merupakan cara berkomunikasi melalui sebuah ponsel atau perangkat lainnya untuk mengirim atau menerima pesan-pesan pendek. Layanan SMS menggunakan kanal atau jalur teks dalam proses penyampaiannya. Sehingga meskipun sang penerima SMS sedang melakukan kegiatan pembicaraan dengan telepon genggamnya, SMS yang masuk tetap dapat diterima. (Sadeli, 2015)

Dengan tersimpannya isi pesan di SMS tanpa pengamanan, seseorang dapat melihat atau membaca isi pesan. Jika isi pesan tersebut dapat dibaca oleh orang lain, maka pesan yang dikirim tidaklah aman karena isi pesan yang seharusnya bersifat rahasia menjadi dapat di lihat dan di baca oleh orang lain

Berdasarkan latar belakang di atas maka diperlukan suatu algoritma kriptografi untuk merahasiakan isi pesan dengan cara mengenkripsikan isi pesan sebelum di kirim ke penerima pesan melalui aplikasi SMS berbasis

android. Bila SMS yang dikirim telah dienkripsi sebelum dikirim maka tidak ada yang bisa membaca isi pesan kecuali penerima pesan yang memiliki aplikasi yang sama. Pada tahap ini penulis akan mengimplementasikan algoritma kriptografi *Improved Caesar Cipher* untuk proses enkripsi dan dekripsi pesan *text*, karena pada metode *Improved Caesar Cipher* SMS akan lebih terjaga .

1.2 Perumusan Masalah

Masalah yang akan diselesaikan dalam penelitian ini adalah bagaimana membuat pesan *text* yang dikirim dapat dibaca oleh penerima pesan yang memiliki aplikasi yang sama

1.3 Batasan Masalah

Mengingat adanya berbagai keterbatasan dan untuk menghindari kompleksitas yang mungkin timbul selama penelitian berlangsung, diberikan batasan-batasan dalam penelitian ini, yakni:

1. Pengirim dan penerima pesan harus menggunakan aplikasi yang sama untuk membaca isi pesan.
2. Android yang digunakan minimal versi *Ice Cream Sandwich*.
3. Jenis karakter yang digunakan 93 karakter.

1.4 Tujuan dan Manfaat Penelitian

Tujuan dan manfaat yang ingin dicapai dalam melakukan penelitian ini dapat dilihat sebagai berikut :

1.4.1 Tujuan Penelitian

Tujuan penulis ialah membuat aplikasi yang dapat mengenkripsi dan mendenkripsi isi pesan dengan metode algoritma *Improved Caesar Cipher* di *smartphone*.

1.4.2 Manfaat Penelitian

Manfaatnya yaitu agar isi pesan yang dikirim tidak dapat dibaca oleh orang lain dan menjaga privasi pemilik *smarthphone*.

1.5 Metodologi Penelitian

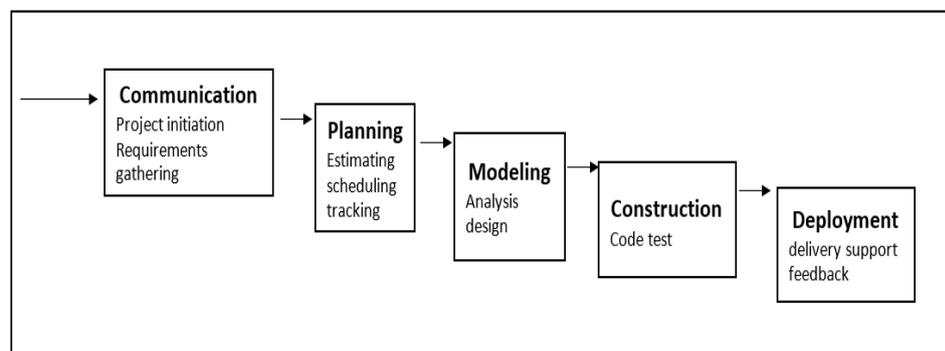
Metodologi penelitian yang digunakan dapat dilihat sebagai berikut:

1.5.1 Jenis Penelitian

Jenis penelitian yang digunakan pada penelitian ini adalah penelitian terapan dimana penelitian ini memberikan solusi atas permasalahan tertentu secara praktis.

1.5.2 Metode Pengembangan Sistem

Metode yang digunakan dalam pengembangan sistem ini menggunakan model air terjun (*waterfall*). Model ini di ilustrasikan pada gambar 1.1



Gambar 1.1 Model Waterfall (Pressman, 2012)

Berikut penjelasan mengenai tahap-tahap tersebut menurut Pressman (Pressman, 2012).

a. *Communication*

Langkah ini merupakan analisis terhadap kebutuhan *software*, Seperti menganalisis kebutuhan sistem yang akan digunakan dalam pembuatan aplikasi SMS berbasis android seperti ,menu-menu apa saja yang ada dalam aplikasi SMS berbasis android ini.

b. Planning

Proses *planning* merupakan lanjutan dari proses *communication (analysis requirement)*. Tahapan ini menghasilkan dokumen *user requirement* atau bisa dikatakan sebagai data yang berhubungan dengan keinginan *user*. Pada tahap ini peneliti akan melakukan pembuatan jadwal pelaksanaan atau jadwal dalam membuat aplikasi SMS berbasis android. penelitian dilakukan selama 6 bulan

c. Modeling

Proses *modeling* ini akan menerjemahkan syarat kebutuhan ke- sebuah perancangan *software* yang dapat diperkirakan sebelum di buat *coding*. Pada tahap *modeling* akan melakukan desain dalam pembuatan program seperti, struktur data, alur program seperti *flowchart*, dan pembuatan *interface* yang akan digunakan dalam aplikasi SMS berbasis android. *Tools* yang digunakan untuk mendesain Aplikasi SMS ini menggunakan UML(*Unified Modeling Language*), yang terdiri dari *use-case diagram*, *class diagram*, *Activity Diagram*

d. Construction

Construction merupakan proses membuat aplikasi. *Coding* atau pengkodean merupakan penerjemah desain bahasa yang bisa dikenali oleh komputer. Tahap ini dilakukan dengan pembuatan program dengan menggunakan *editor eclipse*, ADT (*Android Development Tools*), dan membuat *interface* aplikasi SMS berbasis android.

Setelah selesai membangun aplikasi, maka akan diuji terlebih dahulu apakah fungsi-fungsi di aplikasi tersebut sudah berjalan sesuai dengan yang diharapkan atau tidak. Pengujian yang dilakukan adalah pengujian *blackbox testing*, dan *white box testing*. Pengujian *black box* berfokus pada persyaratan fungsional perangkat lunak. Sedangkan pengujian *white box* menggunakan struktur kontrol desain prosedural untuk memperoleh *test case*. Setelah pengujian, perbaikan akan dilakukan jika diperlukan dan atau ditemukannya *error*.

e. Deployment

Tahapan ini bisa dikatakan final dalam pembuatan sebuah *software* atau sistem. Setelah melakukan analisis, desain dan pengkodean maka sistem yang sudah jadi akan digunakan oleh *user*. Pemilihan metode *waterfall* dalam pengembangan sistem ini dikarenakan metode ini cocok yang di dasari oleh berbagai pertimbangan, salah satunya karena metode ini sering dibahas dan digunakan dalam berbagai penelitian dapat dijadikan referensi.

1.6 Sistematika Penulisan

Sistematika penulisan dilakukan secara sistematis menggunakan beberapa bab, gambaran umum mengenai isi laporan penelitian secara keseluruhan akan diuraikan secara singkat dengan sistematika sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini berisikan latar belakang masalah yang dibahas dalam penelitian yaitu, perumusan masalah, tujuan, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini berisikan teori teori dasar yang digunakan sebagai landasan dan referensi dalam penelitian. Teori tersebut mencakup mengenai teori Android, Android SDK, Eclipse, SMS, Kriptografi, *Caesar Cipher*, ROT13 dan *Improved Caesar Cipher*.

BAB 3 ANALISIS PERANCANGAN SISTEM

Bab ini berisikan analisis kebutuhan sistem, pemodelan UML, desain arsitektur sistem dan desain antarmuka.

BAB 4 IMPLEMENTASI PENGUJIAN SISTEM

Bab ini berisikan pembahasan dari proses pembuatan sistem seperti hasil penerapan desain dalam sistem dan juga pengujian fungsionalitas sistem.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan yang dapat diambil dari penelitian yang dilakukan serta saran saran yang berguna untuk penelitian berikutnya.