

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan dan perkembangan teknologi informasi pada saat ini berpengaruh pada hampir semua aspek kehidupan manusia, terutama dalam hal berkomunikasi. Komunikasi yang dilakukan banyak sekali mengandung informasi yang bersifat rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi, banyak berbagai hal yang telah dilakukan untuk mendapatkan jaminan keamanan pada informasi yang sifatnya rahasia. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi kode yang tidak dimengerti sehingga apabila disadap maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya.

Ilmu kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data. ilmu kriptografi tidak hanya bisa digunakan di komputer, tapi juga bisa digunakan di beberapa perangkat dan sistem operasi, seperti blackberry, android, Iphone, dan masih banyak lagi. Dari beberapa sistem operasi yang telah di sebutkan, android adalah sistem operasi berbasis kernel linux yang sekarang telah dikembangkan oleh google dan merupakan salah satu sistem operasi yang paling banyak digunakan, dan setiap telepon seluler khususnya android pastilah didalamnya terdapat layanan chat, atau yang lebih dikenal dengan sebutan sms. Sms merupakan suatu bentuk komunikasi yang saat ini banyak digunakan, karena

yang sifatnya efisien dan biayanya yang murah. Informasi yang bersifat penting diharapkan dalam pengirimannya dapat dikirim dengan aman kepada penerima informasi.

Penggunaan pesan singkat didalam sistem android, bisa dilakukan melalui aplikasi bawaan atau aplikasi pihak ke tiga yang bisa digunakan dengan sangat mudah dan cepat. namun dengan kemudahan yang diberikan tidak menutup kemungkinan bisa jadi pesan yang ditujukan kepada seseorang bisa saja diambil oleh pihak yang tidak diinginkan. dengan dunia kriptografi saat ini semakin dipermudah dengan adanya aplikasi kriptografi dimana pengguna tidak lagi membutuhkan waktu yang lama, rumit dan berpotensi kesalahan dengan menggunakan algoritma yang ada, dikarenakan jumlah aplikasi kriptografi yang ada saat ini sangat sedikit terutama aplikasi kriptografi yang ada pada sistem operasi android, penulis ingin mencoba merancang sebuah aplikasi kriptografi untuk telepon seluler berbasis android dengan algoritma Blowfish, yaitu menggunakan blok kode.

1.2 Rumusan Masalah

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

1. Aplikasi kriptografi berbasis android ini menerapkan algoritma Blowfish, sebagai algoritma penyandiannya.
2. Merancang aplikasi kriptografi yang dapat mengimplementasikan kriptografi algoritma Blowfish untuk keamanan pesan.

3. Aplikasi kriptografi berbasis android menggunakan Eclipse sebagai software untuk membangunnya.

1.3 Batasan Masalah

Supaya penelitian ini bisa lebih maksimal dan terfokus dan tidak terlalu meluas, penulis membatasi penelitian sebatas:

1. Penelitian ini dibuat dengan menerapkan algoritma blowfish sebagai algoritma kriptografi.
2. Informasi yang akan diproses berbentuk teks atau pesan.
3. Aplikasi hanya bisa dijalankan pada mobile yang mendukung sistem operasi minimal android versi Kitkat versi 4.4.2
4. Pembuatan aplikasi kriptografi ini menggunakan eclipse sebagai softwarena pembangunnya.
5. *Java Development Kit (JDK)*, *Android Software Development Kit (SDK)* , *Android Development Tools*, sebagai pengkompilasi kode-kode java menjadi aplikasi java.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan penelitian ini adalah:

1. Perancangan dan pembuatan aplikasi kriptografi berbasis android yang berfungsi untuk mengamankan pesan-pesan yang bersifat privasi pada fitur SMS (*Short Message Service*).

2. Menghasilkan aplikasi kriptografi yang berguna untuk menyandikan pesan sebelum pesan tersebut dikirim. Juga bisa mengembalikan pesan dalam bentuk pesan asli.

1.4.2 Manfaat penelitian ini adalah

1. Aplikasi ini dapat menjaga kerahasiaan pesan yang dikirim maupun diterima pada pesan yang bersifat privasi dari penyadap atau *Attacker*.
2. Menambah jenis aplikasi kriptografi di playstore.

1.5 Metode Penelitian

Metode penelitian yang dilakukan pada penelitian ini:

1. Metode Pengumpulan Data

Metode pengumpulan data dalam penelitian ini adalah sebagai berikut:

a. Studi Pustaka

Diambil dari beberapa buku, jurnal, majalah, maupun internet, Menjelaskan bahwa aplikasi kriptografi adalah aplikasi yang sangat bermanfaat untuk digunakan sebagai pengamanan data-data penting dan mempelajari hubungan antara ilmu kriptografi, eclipse dan bahasa pemrograman java.

- b. Percobaan dilakukan dengan menguji program yang dihasilkan kedalam handphone android dengan versi Kitkat 4.4.2

2. Analisis Data

Melakukan analisa pada data-data yang telah diperoleh agar data yang akan digunakan dapat benar-benar menunjang aplikasi yang akan dibuat sehingga dapat mencapai tujuan yang diinginkan.

3. Perancangan Aplikasi

Pada tahapan ini dilakukan perancangan aplikasi sebelum membangun aplikasi yang sebenarnya. Pada tahap ini berisi hasil analisis berupa flowchart dan user interface.

4. Implementasi

Pada tahapan ini aplikasi dibangun berdasarkan hasil rancangan pada tahap sebelumnya menjadi sebuah aplikasi.

5. Pengujian Aplikasi

Pada tahapan pengujian adalah untuk memastikan fungsi-fungsi aplikasi telah berjalan dengan baik sesuai dengan rencana.

1.6 Sistematika Penulisan

Penyusunan dan penulisan skripsi ini meliputi lima bab dengan susunan sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan yang merupakan pengantar pokok permasalahan yang dibahas dalam penyusunan skripsi ini.

BAB II : LANDASAN TEORI

Pada bab ini membahas tentang teori-teori yang berhubungan dengan perancangan aplikasi mobile yang difokuskan pada aplikasi android dan ilmu kriptografi, dan teori tentang algoritma Blowfish.

BAB III : ANALISIS DAN PERANCANGAN

Bab ini membahas tentang analisis sistem, perancangan sistem dan interface atau tampilan aplikasi.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Bab ini akan membahas bagaimana aplikasi digunakan dan apakah berfungsi dengan baik. Serta memaparkan hasil dari tahapan-tahapan penelitian.

BAB V : PENUTUP

Bab ini akan membahas kesimpulan yang didapat dari keseluruhan laporan dan perancangan aplikasi, serta kritik dan saran yang berguna baik bagi penulis maupun penulis lain yang berminat menjadikan skripsi ini untuk dikembangkan.

DAFTAR PUSTAKA

Daftar pustaka akan menyantumkan referensi-referensi yang telah digunakan pada penelitian ini, seperti buku-buku, makalah, jurnal, skripsi atau sumber-sumber dari internet lainnya.