BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dunia keamanan semakin berkembang seiring dengan pesatnya teknologi dan informasi, perkembangan ilmu pengetahuan, banyak informasi baru bermunculan, baik yang layak disebarluaskan atau dirahasiakan. Nyatanya, sebuah informasi kadang bisa bernilai sangat besar seperti halnya data nasabah suatu bank, organisasi, data pribadi dan strategi perusahaan bahkan yang lebih besar dan berskala internasional yang menyangkut hajat hidup suatu negara. Untuk mengamankan informasi tersebut, digunakanlah ilmu Kriptografi.

Ilmu kriptografi sangat cepat berkembang, tidak hanya bisa digunakan di komputer tetapi juga digunakan di beberapa perangkat dan sistem operasi, seperti Blackberry, Android, iPhone dan masih banyak lagi. Terutama disini adalah Android, sistem operasi yang dikembangkan oleh Google ini mengalami peningkatan jumlah pengguna dan tentu saja perangkat yang menggunakan sistem operasi ini menjamur dan sangat laris di pasaran. Setiap telepon selular membutuhkan komunikasi, SMS merupakan suatu bentuk komunikasi yang saat ini banyak digunakan oleh semua orang, karena efisien dan biayanya yang murah. Seseorang dapat dengan mudah bertukar informasi antara satu dengan yang lain menggunakan layanan pesan singkat atau SMS. Namun, kemudahan

ini sering disalahgunakan oleh beberapa pihak dengan mencoba mencuri informasi yang bukan hak mereka. Disinilah diperlukan cara agar suatu informasi yang penting dapat terjaga keamanan dan kerahasiannya.

Dunia kriptografi saat ini semakin mudah dengan adanya aplikasi kriptografi dimana pengguna tidak lagi membutuhkan waktu yang lama, rumit dan berpotensi 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 selular 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. Aplikasi ini bernama Aplikasi Kriptografi *Advanced Encryption Standard* (AES).

1.2 Rumusan Masalah

Bedasarkan latar belakang yang telah diuraikan diatas, dapat dirumuskan sebagai berikut :

1. Bagaimana merancang aplikasi kriptografi *Advanced Encryption Standard* (AES) pada ponsel berbasis android ?

2. Apakah aplikasi kriptografi ini mampu menjaga kerahasiaan pesan atau informasi data yang telah di enkripsi ?

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 Eclipse Indigo.
2. Metode yang digunakan adalah algoritma *Rijndael* 128 bit.
3. Kunci yang dimasukkan untuk proses dekripsi yaitu sama dengan kunci yang digunakan pada saat proses enkripsi.
4. Kedua belah pihak 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. Membuat aplikasi kriptografi AES berbasis Android untuk melakukan 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 literatur yaitu dengan mencari informasi di berbagai *website* yang memiliki konten berkaitan dengan dunia kriptografi modern.

2. Metode Kepustakaan

Metode kepustakaan dengan membaca buku-buku literatur, dokumen, catatan kuliah dan bacaan lainnya 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 diuraikan secara lengkap tentang tahap-tahap perancangan dan pembuatan program. Tentang cara kerja sistem dan pembahasan, serta melakukan pengujian aplikasi yang dibuat.

BAB V : PENUTUP

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