BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi pada zaman sekarang ini tidak dipungkiri sangatlah cepat, khusus teknologi informasi salah satunya telepon seluler, fitur dan kecanggihan pada telpon seluler mulai muncul sampai dengan adanya yang disebut *smartphone*, yang memiliki berbagai fungsi seperti multimedia, multiplayer games, transfer data, vidio streaming dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan diantaranya yang cukup dikenal luas adalah pada platform *smartphone* khususnya Android.

Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *Short Message Service* (SMS). Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitsas SMS.

Pada negara yang maju pemanfaatan SMS untuk mengirim pesan rahasia telah lebih dulu dikembangkan. Misalnya di inggris sebuah perusahaan oprator telepon selular, stellium UK, mengeluarkan layanan bernama *"stealth text"* yang dapat digunakan untuk mengirim pesan dengan aman, yaitu dengan cara menghapus pesan secara otomatis segera setelah 40 detik pesan dibaca atau yang dikenal dengan nama *selfdestruct text message*. Kini dengan memanfaatkan *Wireless Messaging API* (*Application Programming Interface*) dari *Java*, para

pembuat program Java dapat mengembangkan sendiri sebuah aplikasi pengiriman pesan singkat atau SMS yang dimodifikasi untuk untuk mengamankan pesan.

Salah satu teknik pengamanan data adalah dengan menggunakan penyandian dokumen. Algoritma penyandian saat ini semangkin banyak jumlahnya, sejalan dengan berkembangnya ilmu yang mempelajari penyandian data tersebut, ilmu ini biasa disebut kriptografi.

Teknologi SMS dikembangkan pertama kali oleh Frindhelm Hillebrand, *"stealth text"* yang dapat digunakan untuk mengirim pesan secara aman karena pesan akan terhapus jika pesan telah terbaca. Masalah umum tentang keamanan data melalui SMS yaitu masalah pesan yang dikirim oleh seseorang dapat disadap oleh orang ketiga sehingga pesan yang disampaikan tidak sama dengan pesan yang dikirim.

Dalam kriptografi terdapat metode yang cukup penting dalam pengamanan data, salah satunya adalah *Data Encryption Standart* (DES) untuk mengekripsi data yang berjalan pada sistem oprasi Android sehingga pemilik telepon selular yang berbasis android dapat melakukan pertukaran data SMS dengan lebih aman dan nyaman. Dalam menjaga kerahasian SMS, dibutuhkan suatu cara untuk mengamankan informasi yang sifatnya penting atau rahasia, yaitu dengan melakukan enkripsi terhadap teks SMS maka tingkat keamanan informasi dari pesan tersebut dapat ditingkatkan.

Berdasarkan uraian di atas secara garis besar yang disajikan dalam bentuk laporan skripsi dengan judul "***Perancangan Aplikasi Pengamanan Data SMS dengan Algoritma DES Pada Android***".

I.2 Ruang Lingkup Permasalahan

I.2.1 Identifikasi Masalah

Berdasarkan analasis judul yang telah diambil, maka penulis membahas masalah pengamanan data SMS dengan algoritma DES :

1. Membangun aplikasi pada telepon seluler yang mampu melakukan proses enkripsi pesan menggunakan algoritma DES.
2. Membangun aplikasi enkripsi SMS yang digunakan pada telepon seluler yang mendukung aplikasi Java.
3. Mendefenisikan masalah pengamanan pesan SMS dan mencari alternatif penguncian pesan.

I.2.2 Perumusan Masalah

Adapun rumusan masalah yang penulis lakukan dalam menyusun skripsi yang dibahas diatas, sebagai berikut :

1. Bagaimana cara enkripsi pesan SMS yang dikirimkan melalui telepon selular ?
2. Bagaimana cara memanfaatkan layanan SMS yang dikenal mudah dalam penggunaan agar dapat mengirim dan menerima pesan yang bersifat rahasia ?

I.2.3 Batasan Masalah

Mengingat luasnya permasalahan yang ada, maka penulis membuat batasan masalah sebagai berikut :

1. Spesifikasi SMS disesuaikan dengan standar teknologi *Global System for Mobile* (GSM).

2. Pengujian aplikasi hanya dilakukan dengan emalator android.
3. Aplikasi ini tidak memiliki *inbox* (pesan masuk) sehingga pesan yang masuk tidak dapat disimpan untuk dibaca kemabali.
4. Bahasa pemrograman yang digunakan adalah Eclipse.

I.3 Tujuan dan Manfaat

I.3.1 Tujuan

Adapun tujuan dari penulisan skripsi ini adalah :

1. Menghasilkan suatu aplikasi pada telepon selular yang dapat digunakan untuk mengirim dan menerima pesan teks.
2. Memiliki fasilitas untuk mengamankan atau menyembunyikan informasi dari pesan yang dikirim.
3. Menentukan proses enkripsi teks dengan menggunakan algoritma DES.

I.3.2 Manfaat

Manfaat dari penulisan skripsi dan pembuatan aplikasi tersebut adalah :

1. Meningkatkan keamanan informasi yang terkandung dalam SMS.
2. Aplikasi dapat digunakan dalam berbagai bidang, misalnya transaksi online, SMS banking dan lain sebagainya.

I.4 Metode Penelitian

Penulis melakukan penelitian terhadap pembangunan aplikasi pengamanan pesan SMS dengan algoritma kriptografi *DES.* Aplikasi pengamanan ini secara umum memiliki 2 (dua) fungsi utama yaitu mengenkripsikan pesan dan mendekripkannya kembali. Adapun tahapan metodologi penelitian sebagai berikut:

1. Metode pengumpulan data, metode yang digunakan dalam pengumpalan data adalah studi pustaka dan *Research and Site Visitis* (Penelitian dan Mengunjungi Situs).
2. Alur penelitian :
   a. Perencanaan Sistem / Planning, kegiatan yang dilakukan pada tahapan ini yaitu dengan mengenali dan mendefenisikan masalah pemngaman pesan SMS dan mencari alternatif pemecahannya.
   b. Analisa Sistem, analisa terhadap kebutuhan perangkat keras dan perangkat lunak merupkan proses pengumpulan sistem yang diinginkan. Dengan adanya analisis ini, diharapkan kebutuhan akan perangkat keras dan perangkat lunak dalam mengembangkan sistem akan terpenuhi. Sehingga akan menghasilkan sebuah sistem yang sesuai dengan tujuan penelitian.
   c. Implementasi Sistem dan *Coding*, pada tahap ini dilakukan proses transformasi pesan SMS kebentuk kode yang dapat diimplentasikan oleh mesin. Tahap implementasi ini akan menggunakan beberapa *tool* pengembangan sistem yang meliputi : mengkonversi pesan SMS menjadi rangkaian bit, mengenkripsi *plaintext* dan mendekripsi *Chipertext* dengan menggunakan algoritma *Data Encryption Standart* (DES).

I.5 Keaslian Penelitian

Pada pembuatan skripsi ini penulis akan menerangkan keaslian penelitian yang terdapat dalam jurnal yang dikutip :

No	Peneliti/Tahun	Hasil Penelitian
1	Kiki Maria Al Qibriyah, UIN, 2010	Implementasi yang dilakukan menggunakan sebuah perangkat komputer untuk membangun perangkat lunak dan sebuah telepon seluler yang digunakan untuk melakukan uji coba perangkat yang telah dibangun dengan menggunakan algoritma RSA.
2	Jurnal Universitas Jember, 2013	Aplikasi merupakan kumpulan dari beberapa algoritma yang mempunyai fungsi-fungsi tertentu, karena itu dalam perencanaan apliksi dibangun denngan algoritma dan fungsi didapatkan pada tahap analisa data. Adapun penjelasan hail penelitian pengamanan SMS degan algoritma LUC sebagai berikut : 1. Pembangkitan kunci publik Kunci publik dibangkitkan dengan menggunakan dua bilangan prima misalkan : bilangan perima p = 47 dan q = 241. Untuk nilai N adalah hasil dari perkalian dari bilangan dua prima p dan q $N = p$ x q = 47 x 241 = 11327. 2. Proses Enkripsi Proses enkripsi dilakukan oleh pihak yang akan mengirim pesan dan diasumsikan pihak pengirim telah mendapatkan kunci public yang diberikan pihak penerima. Setiap karakter dalam blok akan diubah menjadi nnilai ASCII dan dihitung dengan fungsi lucas. 3. Pembangkitan kunci Privat Pembangkitan kunci privat dilakukan juka telah meneima chipertext, hal ini dikarenakan D = c^2 – 4 diamana c adalah nilai ascii dari chipertext
3	Bayu Kristian nugroho, 2010	Hasil penelitian yang dilakukan yang ada di dalam jurnal ini merupakan hasil pengujian aplikasi kripto SMS menggunakan mtode *blackbox*. Proses ini berfungsi untuk mengenkripsi pesan dan mengirimkan pesan ke nomor tujuan. Langkah-langkah yang dilakukan *user* dalam melakukan proses : 1. *Input* pesan *User* diminta untuk meng*input*kan pesan yang akan dikrim. Pesan tersebut akan dienkripsi terlebih dauhulu sebelum dikirimkan ke nomor tujuan.

		2. *Input* nomor tujuan *User* diminta untuk memasukan nomor tujuan diamana pesan akan dikirim. 3. *Input password* *Password* yang di*input*kan merupakan *key* yang akan dipakai untk mengenkripsi pesan.

I.6 Sistematika Penulisan

Sistematika penulisan skripsi ini dibagi menjadi lima bab yang merangkum tiap tahapan yang penulis lakukan, antara lain:

BAB I PENDAHULUAN

Pada bab ini berisikan konsep dasar penyusunan laporan skripsi. Pengamanan data SMS dengan algoritma DES pada android.

BAB II TINJAUAN PUSTAKA

Pada bab ini dibahas mengenai teori-teori yang mendukung pembahasan bab selanjutnya, aplikasi pengamanan data sms dengan menggunakan algoritma des pada android

BAB III ANALISA DAN DESAIN SISTEM

Pada bab ini berisikan analisa permasalahan dan kebutuhan rancangan program, serta pemodelan sistem secara fungsional.

BAB IV HASIL DAN UJI COBA

Pada bab ini berisikan gambaran rancangan aplikasi pengamanan data sms secara keseluruhan dan kode program dan imple mentasi program.

BAB V KESIMPULAN DAN SARAN

Merupakan rangkuman dari laporan skripsi.