BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi pada zaman sekarang ini begitu cepat, khusus teknologi informasi salah satunya telepon seluler, fitur dan kecanggihannya pada telepon seluler mulai muncul sampai dengan adanya yang disebut *smartphone,* yang memiliki berbagai fungsi seperti *multimedia*, *multiplayer games*, *transfer data*, *video streaming* dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponsel pun bermunculan diantaranya yang cukup dikenal luar adalah pada *platform smartphone* khususnya Android.

Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pegiriman data berupa pesan singkat melalui *Short Message Service* (SMS). Namun dengan fasilitas SMS yang ada, sering muncul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. (Harry Abdurachman, Erwin Gunadhi, 2015)

Salah satu teknik pengamanan data adalah dengan menggunakan penyandian dokumen. Algoritma penyandian saat ini semangkin banyak jumlahnya, sejalan dengan berkembangannya ilmu yang mempelajarin penyandian data tersebut, ilmu biasa di sebut kriptografi. (Yusuf Kurniawan, 2006, 73)

Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (*message*). Kriptografi telah banyak diimplementasikan di banyak hal.

Diantaranya *Smart card*, Anjungan Tunai Mandiri (*ATM*), *Pay TV*, *Mobile Phone*, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya. Kriptografi merupakan kajian ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman.(Rifkie Primartha, 2011, 371)

Dalam kriptografi terdapat metode yang cukup penting dalam pengamanan data, yaitu dengan memilih dua metode *Data Encryption Standart* (DES) atau *Advanced Encryption Standart* (AES) untuk mengekripsi data yang berjalan pada sistem operasi *Android* sehingga pemilik telepon selulur yang berbasis android dapat melakukan pertukuran 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 kemanan informasi dari pesan tersebut dapat ditingkatkan.

Berdasarkan uraian di atas secara garis besar yang disajikan dalam bentuk skripsi dengan judul ***"Perancangan Aplikasi Keamanan Data Pesan Singkat (SMS) Berbasis Android Dengan Menggunakan Algoritma DES Atau AES".***

I.2. Ruang Lingkup Permasalahan

Berdasarkan latar belakang di atas, penulis melakukan identifikasikan terhadap masalah yang akan diangkat dalam skripsi, merumuskannya serta membatasi permasalahan tersebut agar tidak terjadi luas.

I.2.1 Identifikasi Masalah

Adapun identifikasi masalah dari latar belakang yang dibahas adalah :

1. Masih kurangnya aplikasi pada telepon seluler yang mampu melakukan proses enkripsi pesan menggunakan algoritma DES atau AES.
2. Mendefenisikan masalah pengamanan pesan SMS dan mencari *alternative* penguncian pesan.
3. Implementasi yang kurang baik dalam menjaga keamanan enkripsi dan dekripsi.
4. Ketidaksempurnaan sistem dalam pengenkripsian pesan SMS.

I.2.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan di atas, maka dapat diambil suatu rumusan masalah sebagai berikut:

1. Bagaimana cara enkripsi pesan SMS yang dikirimkan melalui telepon seluler ?
2. Bagaimana cara memanfaatkan layanan SMS yang dikenal mudah dalam penggunaan agar dapat mengirim dan menerima pesan yang bersifat rahasia ?
3. Bagaimana melakukan penerapan metode kriptografi yang sesuai sehingga keamanan dan kebutuhan pesan SMS tetap terjaga ?
4. Bagaimana mengimplementasi kriptografi dengan metode DES atau AES ?

I.2.3. Batasan Masalah

Dikarenakan banyaknya cakupan permasalahan yang terdapat pada perancangan aplikasi, maka penulis perlu untuk membatasi batasan masalah yaitu:

1. Penggunaan modem GSM serial *wavecom* sebagai media penerima SMS yang dikirimkan melalui *handphone*.
2. Pengujian aplikasi dilakukan dengan emulator android atau *handphone* andoid.
3. Proses enkripsi dan dekripsi teks menggunakan dua pilihan metode yaitu DES atau AES
4. Data yang menjadi masukan terhadap sistem yaitu berupa teks
5. Bahasa pemrograman yang digunakan adalah *Eclipse*.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari skripsi ini yaitu :

1. Merancang dan membuat sebuah aplikasi untuk keamanan pesan SMS.
2. Melakukan proses enkripsi dan dekripsi terhadap pesan menggunakan metode DES atau AES.
3. Untuk menjaga keutuhan dan keamanan pesan SMS dari pihak yang tidak berwenang.

I.3.2. Manfaat

Adapun manfaat yang akan di kemukakan dari penanganan masalah yang ada, yaitu:

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

3. Menjadikan suatu aplikasi enkripsi dan dekripsi pesan SMS dengan menggunakan metode DES atau AES.

I.4. Metodologi Penelitian

Dalam menyelesaikan perancangan alat ini penulis menggunakan beberapa metode antara lain :

1. Studi Kepustakaan *(Library Research)*

Yaitu dengan cara memperoleh data dengan menggunakan buku-buku yang relevan berhubungan dengan masalah yang dihadapi dalam pembuatan skripsi untuk mendapatkan data yang tepat.

2. Internet *(Surfing)*

Yaitu penulis mencari memperoleh data dari situs-situs *internet* yang berhubungan dengan masalah yang sedang dibahas dan men-*download*-nya sebagai bahan referensi.

3. Diskusi

Berupa konsultasi dengan dosen pembimbing dan rekan-rekan mahasiswa mengenai masalah yang timbul dalam penulisan.

I.5. Keaslian Penelitian

Berikut adalah tabel keaslian penelitian, penelitian mengenai Perancangan Aplikasi Keamanan Data Pesan Singkat (SMS) Berbasis Android Dengan Menggunakan Algoritma DES Atau AES.

Tabel I.1 Keaslian Penelitian

No	Nama / Tahun	Judul	Hasil Penelitian	Perbedaan
1.	Rifkie Primartha, 2011	Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma *Data Encryption Standard* (DES)	Proses subtitusi menggunakan 8 buah kotak-S (S-Box). Kotak S adalah matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit lainnya.	Penerapan enkripsi dan dekripsi Keamanan Pesan SMS menggunakan Algoritma *Data Encryption Standard* (DES) atau *Advanced Encryption Standard* (AES).
2.	Yusuf Kurniawan, Adang Suwandi Ahmad, M. Sukrisno Mardiyanto, Iping Supriana, Sarwono Sutikno, 2006,	Analisis Sandi Diferensial Terhadap AES, DES dan AE1	AES-128 memiliki ketahanan yang besar untuk menghadapi ASD, karena 4 ronde memiliki $DP_{min} = 2^{-150}$, sedangkan AES-128 memiliki ronde 10. Bandingan dengan DES lengkap yang dapat dipecahkan ASD dengan 2^{47} pasang *plaintext* yang dipilih.	Perancangan Aplikasi ini membahas mengenai keamanan Data SMS yang dimana menggunakan bahasa pemrograman *Android* menggunakan aplikasi *eclipse*.
3.	Ahmad, 2015	Perancangan Aplikasi Komoditas Pertanian Berbasis *Android.*	Memberikan kemudahan bagi masyarakat khususnya petani dalam mengakses informasi mengenai komoditas pertanian seperti harga, varietas tanaman, produksi dan hal lainnya yang berkaitan dengan komoditas	Perancangan aplikasi keamanan SMS dengan menggunakan metode DES atau AES dengan berbasis *Android*.

			pertanian melalui perangakat *smartphone* yang berbasis android.	
4.	Retno Wardhani dan Moh Husnul Yaqin, 2013	*Game* Dasar-Dasar Hukum Islam Dalam Kitab Mabadi'ul Fiqh Jilid 1	Aplikasi *game* ini berbentuk *quiz* yang semua isi materinya tentan dasar-dasar hukum islam yang di ambilkan dari kitab Mabadi'ul Fiqh jilid I.	Membuat Keamanan Pesan Singkat (SMS) berbasis *Android*.
5.	Harry Abdurachman, Erwin Gunadhi, 2015	Keamanan Komunikasi Data SMS Pada *Android* dengan Menggunakan Aplikasi Kriptografi *Advance Encryption Standard* (AES)	Sistem keamanan ini dapat di gunakan untuk mengamankan komunikasi data sms dari ancaman-ancaman yang tidak berhak.	Aplikasi yang digunakan adalah *eclipse* dan di jalankan melalui *android mobile phone.*

I.6. Sistematika Penulisan

Sistematika penulisan ini terdiri dari 5 bab, dengan tujuan untuk mempermudah dalam pembahasan. Adapun sistematika penulisan tersebut adalah sebagai berikut :

BAB I PENDAHULUAN

Pendahuluan BAB ini menerangkan tentang latar belakang. Ruang limgkup permasalahan, tujuan dan manfaat, metode penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada BAB ini menerangkan tentang teori dasar yang berhubungan dengan program yang dirancang, serta bahasa pemrograman yang digunakan.

BAB III ANALISA MASALAH DAN RANCANGAN PROGRAM

Pada BAB ini mengemukakan tentang analisis masalah program yang akan dirancang dan rancangan program yang digunakan dalam penulisan skripsi ini.

BAB IV IMPLEMENTASI DAN ANALISIS PROGRAM

Pada BAB ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan, serta perangkat yang dibutuhkan, serta analisa sistem yang dirancang untuk mengetahui kelebihan dan kelemahan sistem yang dibuat.

BAB V KESIMPULAN DAN SARAN

Pada BAB ini berisi kesimpulan penelitian dan saran dari penelitian sebagai perbaikan di masa yang akan datang.