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.

Kriptografi merupakan 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.

Dalam kriptografi terdapat metode yang cukup penting dalam pengamanan data, yaitu dengan metode ElGamal untuk mengekripsi data yang berjalan pada sistem operasi *Android* sehingga pemilik telepon seluler 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 laporan skripsi dengan judul ***"Perancangan Aplikasi Enkripsi Data Pesan Singkat Dengan Menggunakan Algoritma ElGamal Berbasis Android".***

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah dari alat yang akan dirancang adalah :

1. Masih sedikitnya aplikasi yang mendukung pengamanan pesan pada perangkat phone SMS.
2. Sering terjadinya penyadapan pesan sms yang sangat merugikan pemilik pesan. Karena informasi yang terdapat pada pesan bersifat penting atau privasi.
3. Implementasi yang kurang baik dalam menjaga keamanan enkripsi dan dekripsi.

I.2.2. Perumusan Masalah

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

1. Bagaimana merancang sebuah aplikasi enkripsi pesan berbasis *android* dengan menerapkan algoritma ElGamal dengan bahasa pemrograman java ?
2. Bagaimana cara kerja algoritma ElGamal dalam melakukan Enkripsi dan Dekripsi pesan yang dikirimkan melalui telepon seluler ?
3. Bagaimana menerapkan Algoritma ElGamal untuk melakukan Enkripsi dan Dekripsi Pesan ?

I.2.3. Batasan Masalah

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

1. Perancangan yang dilakukan adalah mengembangkan aplikasi untuk *android mobile phone*.
2. Algoritma kriptografi yang digunakan adalah algoritma ElGamal.
3. Pengujian aplikasi dilakukan dengan emulator *android* atau *handphone* andoid.
4. Bahasa pemrograman yang dipergunakan dalam merancang aplikasi adalah eclipse.
5. Kunci public dan kunci *private* sudah di tentukan di dalam program.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun maksud dan tujuan dari pembuatan alat ini yaitu :

1. Merancang dan membuat sebuah aplikasi untuk keamanan pesan.
2. Untuk menerapkan Algoritma ElGamal untuk proses enkripsi dan dekripsi pesan.
3. Untuk menjaga keutuhan dan keamanan pesan dari pihak yang tidak berwenang.

I.3.2. Manfaat

Manfaat yang didapatkan setelah melakukan penelitian skripsi ini adalah :

1. Meningkatkan Keamanana terhadap pesan, sehingga keamanan pesan tersebut menjadi relatif aman.
2. Memberi kemudahan bagi pengguna telepon seluler berbasis *android* untuk mengirimkan informasi rahasia melalui SMS.
3. Menjadikan suatu aplikasi enkripsi dan dekripsi pesan dengan menggunakan algoritma Elgamal.

I.4 Metode 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 alat, teknik penggunaan komponen, teknik penggunaan alat dengan maksud 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. Dalam hal ini penulis melakukan *download* terhadap dokumentasi-dokumentasi, FAQ (*Frequently Asked Questions*), RFC (*Request For Comments*) dan *How to Manual* yang terdapat pada situs-situs yang berhubungan dengan masalah yang sedang dibahas.

3. Pengujian

Yaitu dilakukan pengujian alat yang dibuat, apakah sudah sesuai dengan sistem yang sudah diharapkan.

I.5. Keaslian Penelitian

Berikut adalah tabel keaslian penelitian, penelitian mengenai Perancangan Aplikasi Enkripsi Data Pesan Singkat Menggunakan Algoritma ElGamal Berbasis *Android*.

Tabel I.1. Keaslian Penelitian

No	Nama / Tahun	Judul	Hasil Penelitian
1.	Anandia Zelvina, Syahril Efendi, dan Dedy Arisandi, 2012	Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa	Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Plainteks yang akan dienkripsi dipecah menjadi blok-blok plainteks, selanjutnya proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti.
2.	Davie R Suchendra dan Charel Samuel M, 2013	Penerapan Sistem Kriptografi Menggunakan Algoritma ElGamal Pada Aplikasi Email Berbasis Web	Waktu yang dibutuhkan untuk sebuah sistem untuk melakukan proses enkripsi dan dekripsi Sistem Kriptografi Elgamal hingga 400 karakter adalah 0.004503 detik untuk proses enkripsi dan 0.00479 detik untuk proses dekripsi.
3.	Hari Kurniadi, 2015	Implementasi Algoritma Kriptografi ElGamal Untuk File Citra 2 Dimensi	Analisis histogram memperlihatkan bahwa histogram *cipher-image* berbentuk datar atau terdistibusi *uniform,* sehingga algoritma aman dari serangan analisis frekuensi.

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.

BAB II TINJAUAN PUSTAKA

Pada bab ini dibahas mengenai teori-teori yang mendukung pembahasan bab selanjutnya, aplikasi mikrokontroler dan perangkat-perangkat yang mendukungnya.

BAB III ANALISA DAN DESAIN SISTEM

Pada bab ini berisikan analisa permasalahan dan kebutuhan alat, serta permodelan sistem secara fungsional.

BAB IV HASIL DAN UJI COBA

Pada bab ini berisikan gambaran rancangan struktur alat secara keseluruhan dan kode program, serta implementasinya yaitu menguji untuk menemukan kesalahan.

BAB V KESIMPULAN DAN SARAN

Merupakan rangkuman dari laporan skripsi.