BAB I

PENDAHULUAN

I.1. Latar Belakang

SMS merupakan suatu layanan yang memungkinkan pengguna telepon genggam untuk mengirim pesan singkat kepada pengguna telepon genggam lainnya dengan cepat dan hanya memakan biaya yang sedikit. SMS memiliki banyak celah yang memungkinkan para pencuri atau perusak informasi untuk mengambilnya. Kelebihan dari SMS ini adalah ketika tujuan sedang sibuk, pesan tetap dapat dikirimkan dengan menyimpan pesan tersebut pada SMSC (*Short Message Service Center*) dan akan mengirimkan ketika tujuan sudah tidak sibuk. Namun kelebihan ini juga yang menjadikannya kelemahan, dengan tersimpannya pesan pada SMSC (*Short Message Service Center*), maka penyerang dapat mendapatkan pesan dengan melakukan penyusupan pada SMSC (*Short Message Service Center*) tersebut.

Untuk itu diperlukan adanya sebuah sistem dan cara yang dapat mengamankan isi SMS agar kecurian pesan dapat diatasi. Caranya adalah dengan menerapkan suatu metode kriptografi pada isi SMS. Dengan tersandikannya isi SMS, maka seseorang yang berhasil mencuri informasi SMS akan kesulitan untuk mengetahui isi dari SMS tersebut. Untuk itu penulis merekomendasikan metode *gronsfeld* sebagai algoritma penyandian isi SMS. Metode *gronsfeld* adalah satu *cipher* subsitusi sederhana *polyalphabetic.* Gaspar Schot adalah seorang kriptografer abad ke 17 di Jerman, yang belajar *cipher* ini selama perjalanan

antara Mainz dan Frankfurt dengan menghitung *Gronsfeld*, maka terciptalah nama dari *chipper* tersebut yaitu *gronsfeld*. Sistem *gronsfeld* menggunakan suatu kunci numeric yang biasanya cukup pendek misalnya 7341, kunci ini diulang secara periodik, sesuai dengan jumlah kata *plaintext*. (Aznuddin, 2013). Akan tetapi kriptografi tersebut tidak akan berjalan tanpa adanya aplikasi tambahan pada telepon genggam yang digunakan. Untuk itu, digunakan bahasa pemrograman *java android* dan menggunakan *Netbeans* sebagai *IDE* (*Integrated Environtment Development*) dan juga *emulator* sebagai tampilan hasil eksekusinya. Dengan latar belakang diatas maka penulis mengambil judul **"Aplikasi Pertukaran Pesan Pendek Rahasia Menggunakan Metode Gronsfeld Pada Android.**

I.2. Ruang lingkup Permasalahan

Adapun beberapa tahap yang dilakukan dalam membuat ruang lingkup permasalahan adalah :

I.2.1. Identifikasi Masalah

Dengan mengetahui latar belakang pemilihan judul di atas, maka identifikasi masalah dari penulis untuk skripsi ini adalah :

1. Kurangnya keamanan pertukaran pesan pendek pada perangkat *android*.
2. Belum adanya metode yang tepat untuk menyandikan SMS.
3. Dibutuhkan aplikasi penyandian SMS pada perangkat *android*.

I.2.2. Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian ini yaitu :

1. Bagaimana mengamankan pertukaran pesan pendek pada perangkat *android*?
2. Bagaimana metode *gronsfeld* dapat menyandikan isi SMS?
3. Bagaimana menerapkan aplikasi penyandian SMS pada perangkat *android*?

I.2.3. Batasan Masalah

Disebabkan banyaknya permasalahan dan waktu yang terbatas, maka agar pembahasan masalah tidak melebar penulis membatasi masalah sebagai berikut :

1. Aplikasi hanya untuk penyandian SMS perangkat *android*.
2. Aplikasi hanya dapat berjalan pada sistem operasi berbasis *android*.
3. *Input* aplikasi ini berupa teks SMS.
4. *Output* aplikasi ini berupa *Ciphertext* SMS.
5. Pembuatan Aplikasi ini menggunakan bahasa *java android* dan *xml*.
6. Perancangan Aplikasi ini menggunakan pemodelan *UML*.
7. Metode yang digunakan adalah metode *Gronsfeld Cipher*.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Mengamankan pertukaran pesan pendek pada perangkat *android*.
2. Mengetahui dan memahami cara kerja dari metode *gronsfeld* dalam menyandikan isi SMS pada perangkat *android*.

3. Menerapkan aplikasi penyandian SMS pada perangkat *android*.

I.3.2. Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Aplikasi ini dapat menyandikan pesan SMS pada perangkat *android*.
2. Memahami penggunaan metode *gronsfeld* dalam pengamanan SMS pada perangkat *android*.
3. Mendapat wawasan dalam pembuatan perangkat lunak.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan.

1.4.1. Pengumpulan Data

Metode penelitian yang dipakai oleh penulis adalah metode penelitian deskriptif atau disebut juga metode penelitian analitis. Dalam metode penelitian deskriptif ini digunakan teknik-teknik analisis, klasifikasi masalah, survei, studi kepustakaan terhadap masalah-masalah yang berhubungan dengan skripsi yang penulis susun, wawancara (*interview*) dengan seseorang yang mengerti tentang keamanan pesan, observasi, dan teknik *Test* terhadap objek penelitian yang telah ada.

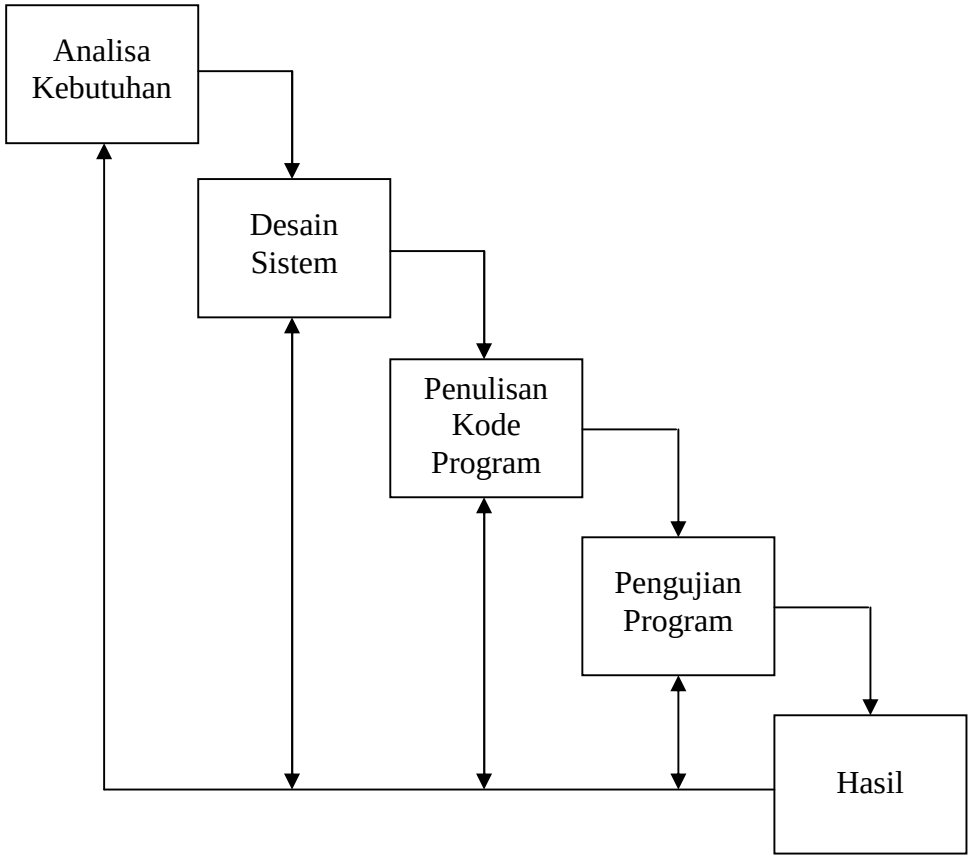
Penulis menggunakan metode penelitian deskriptif dikarenakan pemecahan masalah yang aktual yaitu masalah yang berkembang pada bidang *artifisial intelligence* yang sekarang sedang berkembang pesat. Dengan metode deskriptif,

aplikasi yang telah penulis kumpulkan mula-mula disusun, dijelaskan, dianalisis, dan kemudian diimplementasikan dalam sebuah perangkat lunak

1.4.2. Penelitian perpustakaan (*Library Research*)

Pada metode ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi yang dikutip dapat berupa teori.

Tahapan dalam penelitian ini dapat di modelkan pada diagram *waterfall*. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :



Gambar I.1. Diagram *Waterfall* Metodologi Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan pengumpulan data-data tentang kriptografi dan SMS.

Pada tahapan ini juga ditentukan *software* dan *hardware* yang akan digunakan untuk mengimplementasikan dan menguji hasil penelitian. Berdasarkan data-data yang ada ini kemudian dilakukan tahap selanjutnya, yaitu desain sistem.

Berikut adalah *software* yang digunakan untuk pembuatan sistem :

a. Sistem operasi *windows* 7
b. *Netbeans* 8.0
c. *Android Emulator*

Berikut adalah *hardware* yang digunakan untuk penerapan sistem :

a. *Laptop/ Computer*
b. *Hardisk*
c. *USB Cable*
d. *Android 6.0*

2. Desain Sistem

Proses desain akan menerjemahkan syarat kebutuhan sebuah perancangan perangkat lunak yang dapat diperkirakan sebelum dibuat kode program. Proses ini berfokus kepada : struktur data, arsitektur perangkat lunak, representasi *interface*, dan *detail* (algoritma) prosedural. Dokumen inilah yang akan digunakan untuk

melakukan aktivitas pembuatan sistemnya. Pada tahap ini dilakukan desain perangkat lunak menggunakan pemodelan *uml* yaitu *use case diagram*, *class diagram, activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Kode program merupakan terjemahan *design* dalam bahasa yang bisa dikenali komputer. Pada tahap ini desain sistem diimplementasikan ke dalam kode program. Pemrograman dimulai dengan bahasa pemrograman *java android* dan *xml.*

4. Pengujian Program

Pengujian program merupakan langkah yang dilakukan setelah penulisan kode program. Pengujian program dilakukan untuk mengetahui hasil dari perancangan sistem yang telah dibuat dan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik.

5. Hasil

Pada tahap ini program akan diterapkan untuk mengamankan pesan pendek pada perangkat *android*. Kemudian program secara otomatis akan menampilkan hasil dari perancangan sistem. Aplikasi ini menampilkan teks SMS yang tersandikan dan yang belum tersandikan.

I.5. Keaslian Penelitian

Berikut adalah tabel keaslian penelitian, penelitian yang berkaitan mengenai aplikasi penyandian SMS.

Tabel I.1 Keaslian Penelitian

No	Nama/ Tahun	Referensi	Judul	Hasil Penelitian	Tempat Terbit
1.	Dwi P, 2012	Makalah IF3058	Penerapan Algoritma Vigenere Cipher Pada Aplikasi SMS Android	Pesan yang bersifat personal atau rahasia tidak aman jika dikirimkan melalui aplikasi SMS biasa. Orang lain dapat dengan mudah mencuri informasi dari SMS tersebut dengan cara *snooping* maupun *interception*. Untuk mengatasi celah keamanan pada layanan SMS ini dibutuhkan aplikasi SMS yang mampu mengenkripsi dan mendekripsi isi pesan SMS, sehingga hanya orang yang memiliki kunci yang sama yang dapat membaca makna dari pesan.	Institut Teknologi Bandung, Bandung
2.	Sholeh, dkk, 2013	Jurnal Algoritma Sekolah Tinggi Teknologi Garut	Mengamankan Skrip Pada Bahasa Pemograman Php Dengan	Dengan diterapkan Sistem Informasi untuk pelayanan pasien rawat-	Sekolah Teknologi Garut, Garut

			Menggunakan Kriptografi Base64	inap memungkinkan bagian-bagian yang terlibat dapat melakukan proses administrasi dan aktifitas lainnya dengan mudah dan cepat. Seperti dalam halnya mengetahui data dokter, data kamar yang tersedia dan dalam hal pelaporan Data Rawat-Inap kepada Kepala Rumah Sakit.	
3.	Azanuddin, 2011	Jurnal Pelita Informatika Budi Dharma	Penyandian Short Message Service (Sms) Pada Telepon Selular Dengan Menggunakan Algoritma Gronsfeld	Dengan menerapkan Algoritma Gronsfeld dalam penyandian SMS, maka dapat mencegah dari ancaman penyadapan dan pencurian SMS karena SMS yang dikirim bukan berupa SMS yang asli melainkan berupa *chiperteks*, sehingga akan sulit untuk dimengerti penyerang.	STMIK Budi Darma, Medan

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan Skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan serta perangkat yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisikan berbagai kesimpulan yang dapat dibuat berdasarkan uraian yang telah disimpulkan, serta saran kepada perusahaan.