BAB I

PENDAHULUAN

I.1. Latar Belakang

Ponsel hadir dengan menyediakan media komunikasi seperti halnya *SMS* (*Short Message Service*). *SMS* merupakan suatu layanan yang memungkinkan pengguna ponsel untuk mengirim pesan singkat kepada pengguna ponsel 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 *SMS*C (*Short Message Service Center*) dan akan mengirimkan ketika tujuan sudah tidak sibuk. Namun kelebihan ini juga yang menjadikannya kelemahan, dengan tersimpannya pesan pada *SMS*C, maka penyerang dapat mendapatkan pesan dengan melakukan penyusupan pada *SMS*C tersebut.

Diperlukan adanya sebuah sistem untuk 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. Namun teknik kriptografi banyak yang sudah dapat terpecahkan persandiannya oleh para pencuri informasi karena kesederahanaannya. Oleh karena itu penulis memiliki ide untuk mengkombinasikan tiga metode kriptografi agar penyandiannya lebih kuat. Untuk itu penulis mengkombinasikan metode

vigenere cipher, *caesar cipher* dan *gronsfeld cipher*. *Vigenere Cipher* termasuk dalam *cipher* abjad majemuk (*polyalphabetic substitution chiper*) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, *Blaise de Vigenere* pada abad 16 (tahun 1586). *Vigenere Cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. (Arjana, dkk, 2012).

Dalam kriptografi, sandi *Caesar*, atau sandi geser, kode *Caesar* atau Geseran *Caesar* adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Pada *Caesar cipher*, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran huruf (yaitu 3). (Seftyanto, dkk, 2012).

Algoritma *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*. *System gronsfeld* menggunakan suatu kunci numeric yang biasanya cukup pendek misalnya 7341, kunci ini diulang secara periodic, sesuai dengan jumlah kata *plaintext*. Idenya adalah dengan mengganti huruf dengan bilangan decimal maka akan mengakibatkan *plaintext* tidak akan berupa huruf melainkan hanya berupa susunan angka. Kemudian enkripsi menggunakan prinsip yang sama dengan algoritma *vigenere* yaitu menggunakan tabel yang hanya berukuran

10x10.(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 menyimpulkan judul **"Penerapan Kombinasi Metode *Vigenere Cipher, Caesar Cipher* Dan *Gronsfeld Cipher* Untuk Keamanan *SMS* Perangkat *Android*".**

I.2. Ruang lingkup Permasalahan

Terdapat beberapa ruang lingkup masalah pada penelitian ini. Ruang lingkup masalah tersebut disajikan sebagai berikut :

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang di atas, maka identifikasi masalah untuk skripsi ini adalah :

1. Dibutuhkan sebuah metode yang tepat untuk mengamankan *SMS* perangkat *android*.
2. Dibutuhkan hasil dari kombinasi metode *vigenere cipher* dan *caesar cipher* dalam mengamankan *SMS* perangkat android.
3. Dibutuhkan sebuah aplikasi penerapan kombinasi metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher* untuk keamanan *SMS* perangkat *android.*

I.2.2. Perumusan Masalah

Setelah mendapatkan identifikasi masalah dari penelitian ini, maka diperoleh perumusan masalah sebaagai berikut :

1. Bagaimana mengkombinasikan metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher* ?
2. Bagaimana penerapan kombinasi metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher* untuk keamanan *SMS* pada perangkat *android* ?
3. Bagaimana menghasilkan aplikasi penerapan kombinasi metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher* untuk keamanan *SMS* perangkat *android* ?

I.2.3. Batasan Masalah

Dibutuhkannya batasan masalah di dalam sebuah penelitian agar pembahasan tidak menjadi panjang lebar. Batasan masalah pada penelitian ini dapat di lihat sebagai berikut :

1. Aplikasi hanya dapat berjalan pada sistem operasi *android*.
2. Aplikasi hanya untuk menyandikan pesan *SMS*.
3. *Input* aplikasi ini berupa teks *SMS* asli dan sandi.
4. *Output* aplikasi ini berupa teks *SMS* asli dan sandi.
5. Pembuatan Aplikasi ini menggunakan *Netbeans*.
7. Perancangan Aplikasi ini menggunakan pemodelan UML.

I.3. Tujuan Dan Manfaat

Tujuan dan manfaat yang terdapat pada penelitian ini dijabarkan dan dapat di lihat sebagai berikut :

I.3.1. Tujuan

Penelitian ini memiliki tujuan sebagai berikut :

1. Mengkombinasikan metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher.*
2. Menerapkan kombinasi metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher* untuk keamanan *SMS* pada perangkat *android*.
3. Menghasilkan aplikasi penerapan kombinasi metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher* untuk keamanan *SMS* perangkat *android.*

I.3.2. Manfaat

Penelitian ini memiliki manfaat sebagai berikut :

1. Kombinasi metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher* dapat mengamankan isi pesan *SMS* pada perangkat *android.*
2. Lebih memahami metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher*.
3. Mendapat wawasan dalam pembuatan perangkat lunak kriptografi.

I.4. Metodologi Penelitian

Pada tahap ini dilakukan dengan mempelajari teori dasar yang mendukung penelitian, pencarian dan pengumpulan data-data yang dibutuhkan. Untuk mengumpulkan data yang dibutuhkan, maka penulis memakai teknik :

1. Pengamatan Langsung (*Observation*)

   Melakukan pengamatan secara langsung ke tempat objek pembahasan yang ingin diperoleh yaitu bagian-bagian terpenting dalam pengambilan data yang diperlukan berkaitan tentang kriptografi.

2. Wawancara (*Interview*)

   Teknik ini secara langsung bertatap muka dengan pihak bersangkutan untuk mendapatkan penjelasan dari masalah-masalah yang sebelumnya kurang jelas yaitu tentang mekanisme sistem yang digunakan pada perusahaan dan juga untuk meyakinkan bahwa data yang diperoleh dikumpulkan akurat.

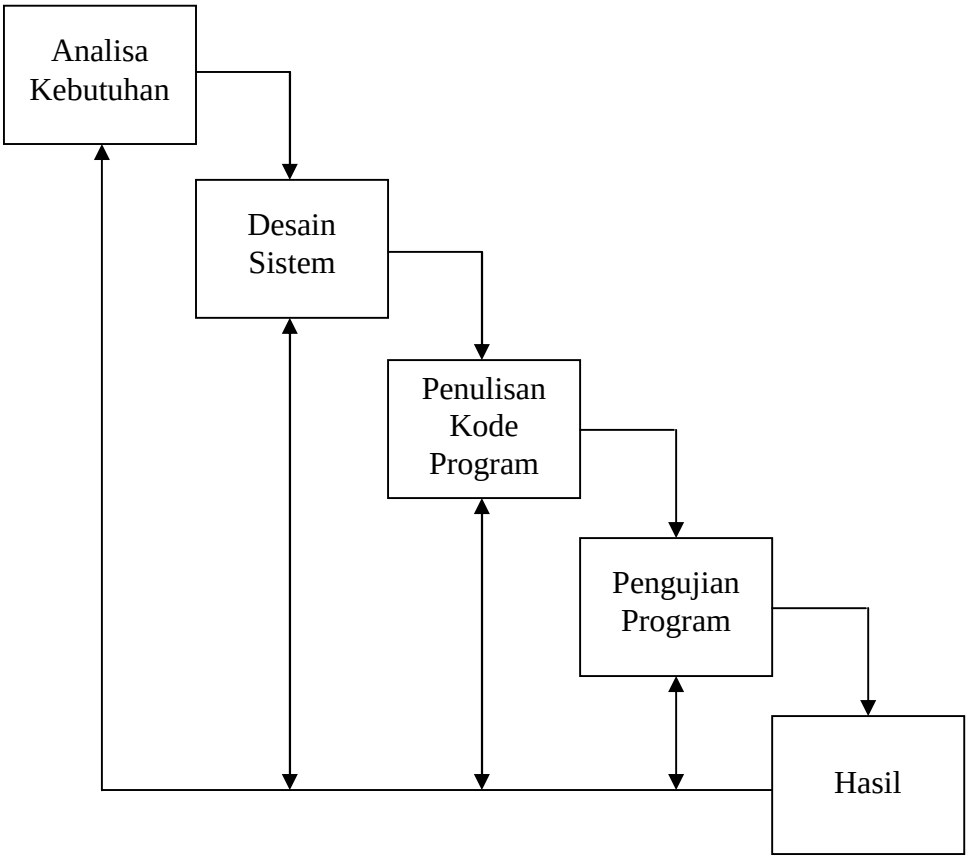
3. *Sampling*

   Meneliti dan memilih data-data yang tersedia dan sesuai dengan bidang yang dipilih sebagai berkas lampiran.

4. Penelitian perpustakaan (*Library Research*)

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

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



Gambar I.1. *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 teori yang terkait dengan kriptografi.

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. *Emulator Android*

Berikut adalah *hardware* yang digunakan untuk penerapan sistem :

a. *Laptop/ Computer*

b. *Hardisk*

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 dan dibuat dengan bahasa pemrograman *java* dan *XML*. Dimana *user* akan meng*input*kan teks *SMS*.

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 menyandikan teks *SMS.* Aplikasi yang dihasilkan akan menampilkan hasil penyandian teks *SMS* yaitu berupa *ciphertext* teks *SMS*.

I.5. Keaslian Penelitian

Berikut adalah tabel keaslian penelitian, penelitian mengenai kriptografi dan metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher*.

Tabel I.1. Keaslian Penelitian

No	Nama/ Tahun	Referensi	Judul	Hasil Penelitian	Tempat Terbit
1.	Arjana, dkk, 2012	Seminar Nasional Teknologi Informasi Dan Komunikasi	Implementasi Enkripsi Data Dengan Algoritma *Vigenere Chiper*	Implementasi program nkripsi data dengan *algoritma vigenere chiper* dapat meningkatkan tingkat keamanan pendataan penjualan, khususnya pada data harga.	STMIK Dharma Putra Tangerang
2.	Seftyanto, dkk, 2012	Prosiding	Peran Algoritma *Caesar Cipher* Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi	Kriptografi yang mudah di implementasikan pada kehidupan sehari hari secara nyata dengan rumus matematika yang tidak sulit untuk di mengerti dan untuk mewujudkan hal tersebut, diperlukan adanya pengenalan kriptografi khususnya *Caesar cipher*.	SekolahTinggi Sandi Negara

3.	Azanuddin, 2013	Jurnal Pelita Informatika Budi Darma	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

Perbedaan penelitian yang terdapat pada tabel I.1 adalah penelitian ini menghasilkan keamanan pesan teks *SMS* pada perangkat *android.* Dengan menerapkan teknik kriptografi menggunakan kombinasi metode *vigenere cipher*, *caesar cipher* dan *gronsfeld cipher* maka untuk mengamankan pesan teks *SMS* menjadi lebih aman.

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, batasan masalah, 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.