

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, maka penyerang dapat mendapatkan pesan dengan melakukan penyusupan pada SMSC 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* dan *vigenere* sebagai algoritma penyandian isi SMS. Metode *gronsfeld* adalah satu *cipher* substitusi 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 periodik, sesuai dengan jumlah kata *plaintext*. *Vigenere cipher* merupakan *cipher* yang setiap *plaintext*-nya mempunyai beberapa kemungkinan

ciphertext, ini terjadi karena panjang kuncinya lebih dari satu. *Cipher* ini mempunyai fungsi matematika yang sama dengan *caesar cipher*. 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 Environment Development)* dan juga *emulator* sebagai tampilan hasil eksekusinya. Dengan latar belakang diatas maka penulis mengambil judul **“Rancang Bangun Aplikasi Penyandian SMS Menggunakan Metode Gronsfeld Dan Metode Vigenere Berbasis 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 indentifikasi masalah dari penulis untuk skripsi ini adalah:

1. Pengiriman SMS belum terbilang aman.
2. Diperlukan aplikasi untuk menyandikan pesan teks SMS.
3. Diperlukan metode yang dapat memecahkan masalah penyandian SMS.

I.2.2. Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian ini yaitu:

1. Bagaimana tampilan antarmuka aplikasi penyandian SMS menggunakan Metode Gronsfeld Dan Metode Vigenere Berbasis *Android*?
2. Bagaimana metode *gronsfeld* dan *vigenere* dapat menyandikan isi SMS?
3. Bagaimana menerapkan aplikasi penyandian data 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 menyandikan isi teks SMS perangkat *android*.
2. Aplikasi tidak dapat menyandikan pesan pada gambar.
3. *Input* aplikasi ini berupa teks untuk disandikan.
4. *Output* aplikasi ini berupa teks yang tersandikan.
5. Perancangan dan pembuatan Aplikasi ini menggunakan bahasa pemrograman *java*.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

1. Untuk menghasilkan sebuah perangkat lunak *android* yang dapat menyandikan isi teks SMS.
2. Untuk mengetahui dan memahami cara kerja dari metode *gronsfeld cipher* dan *vigenere cipher* di dalam penyandian isi teks SMS.
3. Perangkat lunak ini dapat berjalan dengan baik dan penulis mendapatkan wawasan luas didalam bidang komputer terutama dalam pembuatan perangkat lunak kriptografi.

I.3.2. Manfaat

1. Aplikasi ini dapat menyandikan pesan SMS pada perangkat *android*.
2. Penulis lebih memahami penggunaan metode *gronsfeld cipher* dan *vigenere cipher* dalam penyandian SMS.
3. Penulis mendapat wawasan dalam pembuatan perangkat lunak.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematis untuk mengerjakan suatu permasalahan. Untuk itu penulis menggunakan beberapa cara untuk memperolehnya, diantaranya :

1. Pengumpulan Data

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 :

a. 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 SMS *android*.

b. 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 benar-benar akurat.

c. *Sampling*

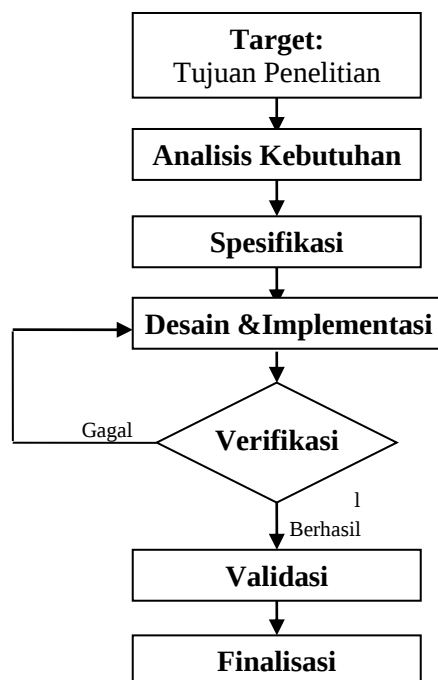
Meneliti dan memilih data - data yang tersedia dan sesuai dengan bidang yang dipilih sebagai berkas lampiran.

2. Penelitian perpustakaan (*Library Research*)

Pada metode ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi yang dikutip dapat berupa teori ataupun beberapa pendapat dari beberapa buku bacaan. Ini dimaksudkan untuk memberikan landasan teori yang kuat melalui buku-buku yang tersedia di perpustakaan, yang berhubungan dengan penulisan Laporan Skripsi ini.

1.4.1 Analisa tentang sistem yang ada

Langkah-langkah yang dilakukan untuk mencapai tujuan perancangan adalah sebagaimana ditunjukkan pada Gambar I.1 berikut ini:



Gambar I.1. Prosedur Perancangan

Keterangan :

a) Target/Tujuan Penelitian

Target penelitian dilakukan untuk membuat suatu perangkat lunak untuk penyandian isi SMS pada *android*.

b) Analisis Kebutuhan

Berisi tentang hal-hal yang harus ada pada hasil perancangan agar mampu menyelesaikan masalah yang ada sesuai tujuan. Beberapa hal-hal yang harus dipenuhi adalah :

- 1) Adanya perangkat lunak yang dijalankan untuk menyandikan isi SMS *android*.
- 2) Adanya perangkat *android* yang dapat menjalankan aplikasi penyandian SMS menggunakan metode *gronsfeld* dan *vigenere*.

c) Spesifikasi dan Desain

Perancangan sistem menggunakan bahasa pemrograman *java* dan *xml*. *Netbeans* sebagai *IDE* (*Integrated Environment Development*) Spesifikasi komputer yang digunakan minimal *Core I3*, *RAM* 1 Gb serta *Hard Drive* 360 Gb.

d) Implementasi dan Verifikasi

Berisi langkah-langkah yang dilakukan dalam pembuatan alat serta tahapan-tahapan pengujian yang dilakukan untuk masing-masing blok peralatan yang dirancang.

- 1) Menganalisis beberapa kesalahan yang ada pada sistem yang lama.
- 2) Melakukan pengujian aplikasi yang baru untuk meminimalisir kesalahan.
- 3) Melakukan perawatan sistem yang baru apabila terjadi kesalahan.

e) Validasi

Berisi langkah-langkah yang dilakukan saat pengujian peralatan secara keseluruhan, besaran-besaran yang akan diuji, dan ukuran untuk menilai apakah alat sudah bekerja dengan baik sesuai spesifikasi.

- 1) Setelah aplikasi dibuat maka selanjutnya akan dijalankan pada komputer apakah telah sesuai dan berjalan dengan baik.
- 2) Menjalankan aplikasi yang baru untuk di uji pada sistem yang lama serta melakukan perawatan sistem.
- 3) Melihat hasil informasi dari aplikasi yang dibuat dengan spesifikasi komputer yang digunakan.

f. Finalisasi

Pada tahapan ini adalah tahapan hasil dari sistem yang sudah dirancang dan berjalan dengan rencana.

1.4.2 Pengujian / Uji Coba sistem yang sudah dibuat

Proses pengujian atau uji coba sistem yang dilakukan hanya sebatas pengujian secara teoritis dan aplikatif, dimana aplikasi belum diuji coba dalam kasus yang sebenarnya. Pengujian sistem yang dibuat menggunakan metode *black box testing*.

I.5. Keaslian Penelitian

Berikut adalah tabel keaslian penelitian, penelitian mengenai aplikasi penyandian SMS menggunakan Metode *Gronsfeld* Dan Metode *Vigenere* Berbasis *Android*.

Tabel I.1. Keaslian Penelitian

No	Nama / Tahun	Judul	Hasil Penelitian
1.	Andi Kurniawan Dwi P, 2012	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

			<i>snooping</i> maupun <i>interception</i> .
2.	Azanuddin, 2013	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 <i>chiperteks</i> , sehingga akan sulit untuk dimengerti penyerang.
3.	F. Wiwiek Nurwiyati dan Indra Yatini B, 2013	Enkripsi Dekripsi Data Menggunakan Metode Stream Dan Vigenere Cipher	Kombinasi algoritma metode <i>stream cipher</i> dan <i>vigenere cipher</i> ini menghasilkan algoritma yang cukup handal karena menggunakan 2 kunci berbeda, satu kunci dibangkitkan dengan karakter <i>plaintext</i> dan satu kunci di <i>input</i> kan secara manual.

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.