

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 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.

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. Untuk itu penulis merekomendasikan metode *one time pad* sebagai algoritma penyandian isi SMS. Algoritma *vernam cipher* atau biasa dikenal dengan sebutan *one time pad (OTP)* merupakan algoritma berjenis *symmetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream cipher* yang berasal dari hasil *XOR* antara *bit plaintext* dan *bit key*. Pada metode ini *plain text* diubah kedalam kode *biner* dan kemudian dikenakan operasi *XOR* terhadap kunci yang sudah diubah ke dalam kode *biner*.

(M. Sholeh dan J.V. Hamokwarong, 2011). 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 KRIPTOGRAFI SMS MENGGUNAKAN METODE OTP 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 identifikasi masalah dari penulis untuk skripsi ini adalah:

1. Pengiriman SMS pada perangkat *android* belum terbilang aman.
2. Dibutuhkan keamanan untuk SMS pada perangkat *android*.
3. Dibutuhkan metode yang dapat mengamankan teks SMS.

I.2.2. Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian ini yaitu:

1. Bagaimana cara mengamankan pengiriman SMS?
2. Bagaimana menciptakan keamanan untuk SMS pada perangkat *android*?
3. Bagaimana metode *One Time Pad* dapat mengamankan SMS?

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 SMS perangkat *android*.
2. Aplikasi tidak menyandikan pesan gambar atau pesan suara.
3. *Input* aplikasi ini berupa teks untuk disandikan.
4. *Output* aplikasi ini berupa teks yang tersandikan.
5. Pembuatan Aplikasi ini menggunakan bahasa pemrograman *java* dan *xml*.
6. Perancangan Aplikasi ini menggunakan pemodelan *UML*.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk menghasilkan sebuah perangkat lunak *android* yang dapat menyandikan isi teks SMS.
2. Untuk mengetahui dan memahami cara kerja dari metode *one time pad* 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

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Diharapkan dapat mengembangkan ilmu pengetahuan mengenai kriptografi.
2. Diharapkan dapat membantu pengguna *android* dalam pengamanan pesan SMS.
3. Diharapkan penulis mendapat wawasan yang luas mengenai keamanan pesan SMS pada perangkat *android*.

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.

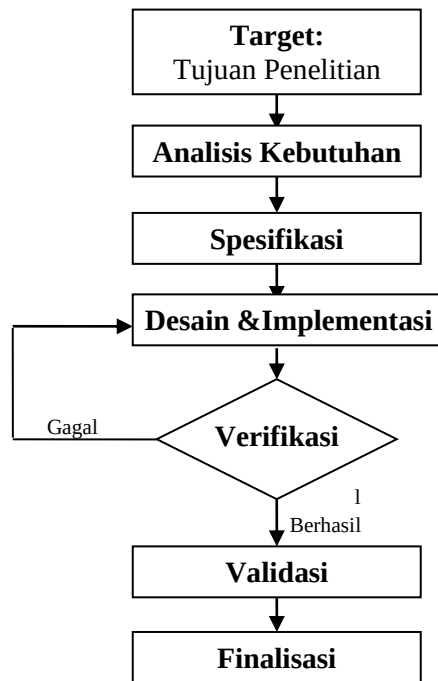
2. Penelitian perpustakaan (*Library Research*)

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.

I.4.1. Analisa tentang sistem yang ada

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



Gambar 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 *one time pad*.

c. Spesifikasi dan Desain

Perancangan sistem menggunakan bahasa pemrograman *java* dan *xml*. *Netbeans* sebagai *IDE (Integrated Environment Development)* Spesifikasi komputer yang direkomendasikan adalah *Core I3*, *RAM 2 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.

- a. Menganalisis beberapa kesalahan yang ada pada sistem yang lama.
- b. Melakukan pengujian aplikasi yang baru untuk meminimalisir kesalahan.
- c. 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.

- a. Setelah aplikasi dibuat maka selanjutnya akan dijalankan pada komputer apakah telah sesuai dan berjalan dengan baik.
- b. Menjalankan aplikasi yang baru untuk di uji pada sistem yang lama serta melakukan perawatan sistem.
- c. 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.

I.4.2. Pengujian / Uji Coba sistem yang sudah dibuat

Proses pengujian atau uji coba sistem yang dilakukan hanya sebatas pengujian secara teroris dan aplikatif, dimana aplikasi belum diuji coba dalam kasus yang sebenarnya. Pengujian perangkat lunak ini menggunakan pengujian *Black Box*. *Black Box* adalah metode pengujian perangkat lunak yang menguji fungsionalitas aplikasi yang bertentangan dengan struktur internal.

I.5. Keaslian Penelitian

Berikut adalah tabel keaslian penelitian, penelitian mengenai penyandian SMS menggunakan metode *one time pad*.

Tabel I.1. Keaslian Penelitian

No	Nama / Tahun	Judul	Hasil Penelitian
1.	Azanuddin, 2013	Penyandian Short Message Service (SMS) Pada Telepon Selular Dengan Menggunakan Algoritma Gronsfield	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.
2.	M. Sholeh Dan J.V. Hamokwarong, 2011	Aplikasi Kriptografi Dengan Metode Vernam Cipher Dan Metode Permutasi Biner	Aplikasi ini menggunakan dua metode enkripsi dan dekripsi agar lebih aman dan terjamin kerahasiaan data.
3.	Aman Julianto Pakpahan, 2013	Aplikasi Penyandian Data Dengan Menggunakan Algoritma Noekeon	Perangkat lunak yang dihasilkan diharapkan dapat menambah perbendaharaan aplikasi kriptografi

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 : ANALISIS 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 UJI COBA

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.