BAB I

PENDAHULUAN

I.1. Latar Belakang Masalah

Perkembangan teknologi dimasa sekarang begitu meningkat dengan pesat, Dengan adanya penemuan-penemuan teknologi baru akan sangat membantu dalam menyelesaikan pekerjaan manusia, salah satunya adalah ponsel, mulai dari ponsel yang hanya bisa menelepon dan SMS hingga ponsel cerdas. Ponsel cerdas atau juga dikenal dengan *smartphone* memiliki fitur dan kecanggihan yang banyak di dalamnya, kita dapat dengan mudah bermain game, chatting, berbisnis dan lain lain dengan jarak jauh. Berbagai macam perangkat lunak telah mengembangkan aplikasi yang banyak pada telepon seluler, Pada saat ini perangkat lunak yang cukup dikenal secara luas adalah android.

Aplikasi yang digunakan pada android untuk pengiriman pesan singkat tanpa kabel adalah SMS (*Short Message Service*). Tidak jarang orang menggunakan aplikasi SMS dalam pengiriman data informasi karena biaya yang cukup murah dan hanya menggunakan data teks, Tetapi dalam melakukan pengiriman dan penerimaan teks SMS tersebut masih belum cukup aman karena komunikasi melalui SMS pesannya akan disimpan di SMSC (*Short Message Service Center*), yaitu tempat dimana SMS disimpan sebelum dikirim ke tujuan. Pesan yang sifatnya *plaintext* ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. Akibatnya, informasi penting seperti *password*, nomer pin, dan lain-lain dapat diketahui oleh orang yang tidak berhak untuk mengetahuinya (Febrian Budi Utama, 2014:4), hal tersebut dapat mengakibatkan hal-hal yang tidak diinginkan oleh pengguna dalam pengiriman informasi penting secara pribadi.

Untuk mengatasi masalah keamanan pesan teks yaitu menggunakan penyandian data, penyandian data di dalam dunia komputer dikenal dengan teknik kriptografi yang sangat bermanfaat untuk mendukung keamanan data teks dari orang yang tidak bertanggung jawab. Saat ini banyak metode-metode kriptografi yang digunakan dalam pengamanan teks termasuk metode *vigenere cipher* dan *One Time Pad* (OTP).

Berdasarkan uraian di atas penulis akan membuat aplikasi pengamanan SMS, karena aplikasi SMS terbilang belum cukup aman untuk digunakan. Metode pengamanan teks menggunakan algoritma *vigenere cipher* dan *one time pad*. *vigenere cipher* dan *one time pad* adalah bagian dari algoritma kriptografi klasik. Pada kedua algoritma ini menggunakan kunci simetri untuk proses enkripsi dan dekripsinya, yang mana kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi. Selain algoritma *one time pad* telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan (Sumber: Sugeng Sutrisno, 2015:5), penulis akan menggunakan dua algoritma *vigenere cipher* dan *one time pad* membuat proses enkripsi ataupun dekripsi dengan dua kali proses perhitungan. Dengan dua kali proses perhitungan ini menjadikan kriptanalisis membutuhkan waktu untuk menemukan kunci yang digunakan sebelum melakukan dekripsi pada *ciphertext* oleh karena itu penulis akan mengangkat judul "**Perancangan Aplikasi Pengamanan SMS Dengan Algoritma *Vigenere Cipher* Dan *One Time Pad* (OTP) Pada Android**".

I.1.1. Identifikasi Masalah

Adapun identifikasi masalah yang telah dirangkum oleh penulis adalah:

1. Pengiriman teks SMS ke penerima yaitu dalam bentuk byte plain sehingga mudah untuk disadap oleh orang yang tidak bertanggung jawab.

2. Mengenkripsi isi pesan SMS dengan menggunakan metode kriptografi agar pesan tersebut sulit untuk dibaca.
3. Menggunakan dua metode kriptografi agar keamanan pesan pada SMS lebih aman.

I.1.2. Rumusan Masalah

Adapun rumusan masalah yang di angkat oleh penulis dalam penyusunan skripsi ini adalah:

1. Bagaimana cara merancang sebuah aplikasi yang dapat mengamankan pesan SMS agar tidak bisa dibaca oleh orang lain.
2. Bagaimana cara menerapkan algoritma *vigenere cipher* dan *one time pad* pada aplikasi yang dirancang.

I.1.3. Batasan Masalah

Adapun batasan masalah yang dibuat oleh penulis adalah sebagai berikut:

1. Merancang sebuah aplikasi Pengamanan pesan teks SMS pada perangkat *mobile phone* android.
2. Algoritma yang dibahas dalam pembuatan laporan ini adalah *Vigenere Cipher* dan *One Time Pad*.
3. Bahasa pemograman yang digunakan penulis adalah J2SE (*Java 2 Standart Edition*) dengan editor pemograman Eclipse dan SDK Android.

I.2. Tujuan Dan Manfaat

I.2.1. Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Untuk membuat sebuah aplikasi pengamanan teks SMS dengan menggunakan konsep kriptografi.
2. Untuk menerapkan algoritma *vigenere cipher* dan *one time pad* ke dalam aplikasi SMS berbasis android.
3. Untuk menghasilkan sebuah aplikasi yang dapat bermanfaat dalam mengamankan data SMS pada *smartphone* android.

I.2.2. Manfaat Penelitian

Manfaat dalam penulisan skripsi ini adalah:

1. Menyajikan sebuah aplikasi untuk pengguna agar dapat mengamankan pesan teks SMS dengan algoritma *vigenere cipher* dan *one time pad*.
2. Membantu pemahaman tentang kriptografi terutama mengenai algoritma *vigenere cipher* dan *one time pad*.
3. Memberikan kenyamanan dan kemudahan kepada pengguna dalam menggunakan SMS yang dilengkapi dengan database.

I.3. Metodologi Penelitian

Metodologi yang digunakan untuk menyelesaikan perancangan ini adalah metode pengumpulan data, yaitu:

1. Studi Pustaka

Adalah teknik pengumpulan data dengan menghimpun dan menganalisis dokumen. Dokumen-dokumen yang termasuk didalamnya yaitu penelitian-penelitian terdahulu, buku, artikel dan jurnal yang berkaitan dengan objek penelitian.

2. *Studi Literatur*

Melakukan studi perbandingan dan analisis antara aplikasi yang pernah dibuat oleh seseorang dengan aplikasi yang penulis buat. Termasuk kelebihan dan kekurangan aplikasi yang telah di buat.

I.4. Keaslian Penelitian

Keaslian penelitian dilakukan pengembangkan aplikasi yang dirancang dengan membandingkan aplikasi-aplikasi yang telah dibuat sebelumnya. Berikut Penulisan penelitian yang terkait dengan perancangan ini:

Tabel I.1. Daftar Keaslian Penelitian

No	Peneliti	Judul Penelitian	Hasil Penelitian
1	Febrian Budi Utama (2014)	Aplikasi SMS Kriptografi Dengan Metode RSA Pada Smartphone Android	Tingkat Keamanan Untuk Algoritma RSA Masih Cukup Aman. Kerena Algoritma RSA Mengandalkan Kekuatan Sulitnya Memfaktorkan Bilangan Yang Besar.
2	Putu H. Arjana, Tri Puji Rahayu, Yakub, Hariyanto, (2012)	Implementasi Enkripsi Data Dengan Algoritma *Vigenere Chiper*	Implementasi Program Enkripsi Data Dengan Algoritma *Vigenere Chiper* Dapat Meningkatkan Tingkat Keamanan Pendataan Penjualan, Khususnya Pada Data Harga.
3	Sugeng Sutrisno	Rancang Bangun Aplikasi Pesan Menggunakan Algoritma *Vigenere Cipher* Dan *One Time Pad*	Penggunaan Algoritma *Vigenere Cipher* Dan *One Time Pad (OTP)* Pada Sistem Enkripsi Pesan Menjadikan Pesan Yang Dikirimkan Menjadi Lebih Aman. Supaya Dapat

Membuka Pesan Maka
Pengguna Memerlukan
Kunci Enkripsi Yang Mana
Kunci Enkripsi Hanya Akan
Diberikan Kepada Pengguna
Yang Berhak Menerima
Pesan Saja.

I.5. Sistematika Penulisan

Adapun susunan sistematika penulisan skripsi ini terdapat beberapa bagian bab yang akan dijelaskan sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menjelaskan secara ringkas tentang latar belakang, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan menfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menjelaskan tentang teori-teori yang berhubungan dengan perancangan, bahasa program yang digunakan, algoritma dan perangkat yang digunakan penulis.

BAB III : ANALISIS DAN DESAIN SISTEM

Pada bab ini membahas tentang analisa permasalahan, pemodelan sistem secara fungsional dan perancangan program yang akan dibuat penulis.

BAB IV : HASIL DAN UJI COBA

Pada bab ini mengemukakan tentang hasil implementasi perancangan aplikasi SMS secara keseluruhan beserta kode program yang digunakan, menentukan kelebihan dan kekurangan sistem yang telah dibuat pada penulisan skripsi ini.

BAB V : KESIMPULAN DAN SARAN

Merupakan kesimpulan yang didapat dari hasil perancangan aplikasi pengamanan SMS serta saran agar aplikasi yang telah dibuat dapat menjadi lebih baik.