BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi yang ada saat ini mampu menghasilkan perangkat keras yang mempermudah komunikasi, telephone seluler adalah salah satu dari sekian perangkat keras komunikasi yang sering digunakan. Dalam menjalankan kinerjanya sebagai perangkat keras komunikasi, telephone seluler mempunyai beberapa fungsi seperti *Short Message Service* (SMS), *Multimedia Message Service* (MMS), video phone, transfer data, perangkat lunak pemutar audio (mp3) dan lain – lain. Salah satu dari beberapa fungsi telephone seluler adalah SMS. SMS merupakan fungsi dari telephone seluler yang digunakan untuk mengirim atau menerima pesan teks. Pada proses pengiriman dan penerimaan pesan, diperlukan suatu media transmisi, media transmisi tersebut salah satunya berupa jalur komunikasi *Global System for Mobile Communication* (GSM).

Pada proses pengiriman dan penerimaan pesan sangat rentan terhadap upaya pencurian, penyadapan, pembajakan, pemerasan dan banyak hal lain terhadap suatu informasi, sehingga dapat dibaca oleh pihak lain, misalnya dalam sebuah lingkungan bisnis, seorang pemimpin perusahaan telah membuat keputusan yang akan mempengaruhi produksi suatu barang dan keputusan itu dikirim kepada manager produksi. Karena kurangnya sistem keamanan pada proses pengiriman atau penerimaan pesan maka informasi yang terkandung pada pesan tersebut dapat

dimanipulasi. Hal ini, bisa menyebabkan keuntungan bagi perusahaan, jika informasi itu bebas dari proses manipulasi. Dan menyebabkan kerugian jika informasi tersebut telah dimanipulasi oleh pihak yang tidak bertanggung jawab.

Contoh nyata dari rentannya keamanan pesan SMS, adalah penyadapan SMS yang diduga dilakukan oleh pihak berwajib dan provider telkom, dalam mengungkap kasus penggelapan pajak PT.Asian Agri, yang disebut sebagai kasus terbesar di tahun 2008, kepada Metta Dharmasaputra yang merupakan wartawan dari surat kabar tempo dan Vincentius Amin Susanto sebagai narasumber, adalah salah satu karyawan PT.Asian Agri, sekaligus saksi kunci dari penggelapan pajak senilai 1,4 Triliun, yang dilakukan PT. Asian Agri. Penyadapan ini diketahui beberapa pekan setelah metta melakukan investigasi [1], kemudian beredar rekaman percakapan melalui layanan pesan singkat (SMS) antara metta dengan narasumbernya [2].

Dari pihak berwajib, Kepala Satuan Fiskal Moneter dan Devisa pada Satuan Reserse dan Kriminal Khusus Polda Metro Jaya melalui jumpa persnya , membantah telah memerintahkan TELKOM selaku provider untuk menyadap SMS wartawan tempo, Metta Dharmasaputra, terkait kasus penggelapan pajak PT.Asian Agri [3]. Dari kasus tersebut dapat disimpulkan, masih terdapatnya kelemahan dalam menjaga kerahasiaan suatu pesan terutama dari pihak operator selaku penyedia layanan komunikasi.

---

[1] http://www.tempo.co/read/news/2007/09/14/055107641/Dewan-Pers-Kecam-Penyadapan-Telepon-Wartawan-Tempo

[2] http://www.tempo.co/read/news/2007/09/12/055107469/Penyadapan-Telepon-Wartawan-Dikecam

[3] http://news.liputan6.com/read/183198/penyadapan-telepon-wartawan-tempo-adalah-pelanggaran-hukum

Permasalahan lain yang menyebabkan suatu pesan rentan terhadap manipulasi informasi adalah kesalahan dalam memasukkan nomor tujuan, hal ini sering disebut *human error*, ada pula pemaksaan langsung kepada pemilik telephone seluler untuk memperlihatkan pesan yang dikirim maupun diterima. Serta pihak operator seluler selaku penyedia layanan yang masih bisa melihat dan membaca pesan yang dikirim oleh pelanggan.

Karena beberapa hal diatas, penerapan kriptografi sangat dibutuhkan dalam menjaga kerahasiaan suatu pesan. Pesan yang dikirim hanya dapat dibaca oleh pihak yang menjadi tujuan pengirim pesan, karena pesan tersebut hanya berupa kode maupun karakter acak yang tidak bisa dibaca, untuk dapat mengetahui pesan tersebut, harus digunakan kunci rahasia atau suatu metode tertentu untuk dapat membacanya.

Dengan berprinsip pada definisi enkripsi super yaitu, suatu konsep enkripsi yang menggunakan kombinasi dari dua atau lebih teknik subtitusi dan permutasi kode, untuk mendapatkan suatu algoritma yang lebih handal (sulit terpecahkan). Maka penulis mencoba untuk menggabungkan konsep kriptografi klasik berupa fungsi yang menggunakan kode Caesar Cipher ROT13, ROT13 adalah subtitusi kode dengan melakukan pergeseran sebanyak k=13. Digabungkan dengan teknik algoritma encoding karakter base64. Base64 adalah sebuah encoding karakter yang mewakili data biner dalam format string ASCII dengan menerjemahkannya ke dalam representasi 64.

Berdasar pada uraian diatas, penulis mencoba mengimplementasikan kedua algoritma tersebut didalam satu aplikasi perangkat lunak dan sekaligus menjadi

bahan penelitian skripsi dengan judul "**IMPLEMENTASI ALGORITMA CEASAR CIPHER ROT13 DAN BASE64 UNTUK ENKRIPSI DAN DEKRIPSI PESAN PADA HANDPHONE BERBASIS ANDROID**".

1.2 Rumusan Masalah

Berdasarkan atas latar belakang masalah yang telah dijelaskan diatas, maka pokok permasalahan yang dikaji meliputi sebagai berikut:

1. Bagaimana mengimplementasikan algoritma Caesar Cipher ROT13 dan Base64 untuk enkripsi dan dekripsi pesan teks pada handphone berbasis android?

1.3 Batasan Masalah

Agar penelitian ini menjadi seperti yang diharapkan dan tidak meluas maka penelitian serta rancangannya terdiri dari :

1. Prinsip enkripsi dan dekripsi Caesar Cipher ROT13 berdasar pada urutan tabel ASCII.
2. Prinsip encoding dan decoding sesuai aturan algoritma Base64 dan berdasar pada tabel Base64.
3. Pengiriman pesan teks melalui SMS.
4. Diimplementasikan pada handphone berbasis android versi 2.3.5 (Gingerbread).

5. Aplikasi yang dibangun, hanya melakukan enkripsi dan dekripsi pesan.
6. Program yang digunakan untuk membangun perangkat lunak adalah eclipse indigo.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Membuat perangkat lunak untuk enkripsi dan dekripsi pesan menggunakan Caesar Cipher ROT13 dan Base64.
2. Sebagai syarat kelulusan bagi program pendidikan pada jenjang Strata 1 jurusan Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta.

1.5. Manfaat Penelitian

Dalam penelitian ini diharapkan dapat bermanfaat bagi berbagai pihak yaitu

1. Bagi penulis, dengan adanya penelitian dan perancangan perangkat lunak ini dapat menambah pengetahuan serta pengalaman yang luas terutama berkaitan dengan pemrograman java yang diimplementasikan pada handphone berbasis android.
2. Penelitian ini diharapkan dapat memberikan kontribusi kepustakaan pendidikan, terutama dalam hal pengamanan pengiriman pesan *teks* pada telepon selular.

1.6 Metodologi Penelitian

Metodologi penelitian merupakan urutan langkah – langkah dari proses penelitian yang sistematik, berikut langkah – langkah yang akan ditempuh dalam proses penelitian selama pengerjaan skripsi ini adalah sebagai berikut .

1. Study literatur

   Study literatur merupakan study kepustakaan atau metode pengumpulan data yang digunakan dalam menyusun sebuah karya tulis. Dalam penelitian ini, dimulai dengan mengumpulkan bahan – bahan referensi baik dari buku, artikel, paper, jurnal, makalah, situs internet mengenai algoritma Caesar Cipher ROT13 dan Base64, pemrograman yang digunakan untuk membuat aplikasinya dan konsep dasar matematis dari kedua algoritma tersebut serta beberapa referensi yang dapat menunjang pencapaian akhir dari penelitian ini.

2. Analisis sistem

   Pada Tahap ini digunakan untuk mendefinisikan dan menggambarkan kebutuhan sistem. Hal ini dilakukan untuk memahami sifat program yang dibangun, unjuk kerja dan antarmuka yang diperlukan.

3. Perancangan sistem

   Pada tahap ini, mengubah kebutuhan yang masih berupa konsep menjadi representasi perangkat lunak.

4. Implementasi sistem

Proses representasi rancangan unit program yang telah diverifikasi, untuk diimplementasikan ke sebuah program.

5. Uji coba sistem

Uji coba program yang telah dihasilkan dengan tujuan, dapat mengetahui kesalahan – kesalahan dan melihat proses berjalannya program, sehingga program berjalan dengan optimal.

6. Penyusunan laporan

Menyusun laporan tentang hasil analisis dan perancangan program, ke dalam format penulisan skripsi, disertai penarikan kesimpulan.

1.7 Sistematika Penelitian

Secara keseluruhan, penulisan skripsi ini terdiri dari 5 bab, yaitu :

BAB I PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang permasalahan, pokok permasalahan, metode penelitian, tujuan dan manfaat penulisan, kerangka penelitian serta sistematika penulisan skripsi.

BAB II LANDASAN TEORI

Bab ini berisi tentang beberapa teori yang mendasari penulisan Skripsi, antara lain : Algoritma Caesar Cipher, base64, bahasa pemrograman java berbasis Android dan pengertian SMS.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan mengenai analisis terhadap masalah – masalah yang sering terjadi dan menjadikannya sebagai dasar dalam penelitian ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Deskripsi mengenai pengujian dan analisis performa aplikasi perangkat lunak BSecure.

BAB V PENUTUP

Bab ini berisi kesimpulan yang berkaitan dengan beberapa hal yang telah disampaikan sebelumnya, serta saran yang dapat dimanfaatkan untuk pengembangan lebih lanjut.