

USER MANUAL

**PERANGKAT LUNAK KRIPTOGRAFI SMS
MENGUNAKAN ALGORITMA VIGENERE**

*Diajukan Sebagai Salah Satu Syarat Untuk Menyelesaikan Program Study D III
Teknik Elektronika Fakultas Teknik Universitas Negeri Padang*



Oleh :

AGUNG VIRNANDO

2007/85152

Konsentrasi: Teknologi Sistem Komputer

Program Studi: D-3Teknik Elektronika

JURUSAN TEKNIK ELEKTRONIKA

FAKULTAS TEKNIK

UNIVERSITAS NEGERI PADANG

PADANG

2011

HALAMAN PENGESAHAN

Dinyatakan lulus setelah dipertahankan di depan tim penguji
Proyek Akhir Jurusan Teknik Elektronika Fakultas Teknik
Universitas Negeri Padang

Judul : Perangkat Lunak Kriptografi SMS Menggunakan
Algoritma Vigenere
Nama : Agung Virnando
BP/NIM : 2007/85152
Program Studi : D-3 Teknik Elektronika
Jurusan : Teknik Elektronika
Fakultas : Teknik

Padang, 18 Agustus 2011

Tim Penguji

	Nama	Tanda Tangan
Ketua	: Drs. Denny Kurniadi, M.Kom	1. _____
Anggota	: Drs. Zulhendra, M.Kom	2. _____
	Drs. Efrizon, MT	3. _____

ABSTRAK

Agung Virnando : Perangkat Lunak Kriptografi SMS Menggunakan
Algoritma Vigenere

Perancangan perangkat lunak kriptografi SMS bertujuan untuk membuat suatu aplikasi untuk keamanan pesan dengan fasilitas SMS yang membuat SMS tersebut tidak diketahui oleh orang yang tidak berhak mengetahuinya. Pesan yang akan dikirimkan akan dienkripsi dengan algoritma vigenere, aplikasi ini dibuat menggunakan bahasa Java yaitu karena dijalankan di telepon seluler maka bahasa Java yang digunakan ialah J2ME(Java 2 Micro Edition), dalam perancangan menggunakan pemodelan UML(unified Modelling Language). Dalam aplikasi ini disediakan fasilitas keamanan SMS. SMS yang akan dikirim akan dienkripsi dengan kunci yang hanya diketahui oleh pengirim dan penerima dan juga didekripsi oleh penerima dengan memasukkan kunci yang sama, maka kemungkinan pesan diketahui oleh orang lain sangat kecil.

Keyword : *Kriptografi, SMS, Kriptografi SMS, Enkripsi, Dekripsi, J2ME, Vigenere chipher.*

KATA PENGANTAR

Bismillaahirrahmaanirrahiim, Rasa Syukur Penulis ucapkan kehadiran Allah SWT, yang telah melimpahkan rahmat dan karunia Nya sehingga Penulis dapat menyelesaikan pembuatan proyek akhir ini sampai selesai yang berjudul **“Perangkat Lunak Kriptografi SMS Menggunakan Algoritma Vigenere”**, dan shalawat beserta salam semoga disampaikan Allah SWT, kepada Baginda Nabi Muhammad SAW yang menjadi suri tauladan bagi setiap umat manusia yang telah membawa kita dari zaman jahiliyah sampai zaman yang penuh dengan ilmu pengetahuan yang kita rasa sampai saat sekarang ini.

Tujuan pembuatan Proyek Akhir ini adalah merupakan salah satu untuk melengkapi persyaratan dalam menyelesaikan Diploma III (D3) pada Program Studi Teknik Elektronika Fakultas Teknik Universitas Negeri Padang. Pembuatan Proyek Akhir ini tidak lepas dari dukungan, bantuan, bimbingan dan motivasi dari berbagai pihak baik secara moril maupun materil. Untuk semua itu Penulis mengucapkan terima kasih kepada:

1. Bapak Drs. Denny Kurniadi selaku pembimbing penulis dalam membuat laporan dan pembuatan program.
2. Bapak Drs. Elfi Tasrif, MT selaku penasehat akademik, tempat mengadu bagi penulis jika ada permasalahan dalam mengerjakan proyek akhir.
3. Bapak Drs. Zulhendra, M.Kom selaku penguji I dalam proyek akhir ini.
4. Bapak Drs. Efrizon, M.T. selaku penguji II dalam proyek akhir ini.

5. Semua staf pengajar, dosen, teknisi dan pegawai administrasi di jurusan Teknik Elektronika Fakultas Teknik Universitas Negeri Padang

Penulis menyadari bahwa laporan ini memiliki banyak kekurangan. Oleh karena itu Penulis mengharapkan kritikan dan saran yang bersifat membangun demi kesempurnaan tulisan ini.

Akhir kata Penulis berharap semoga laporan ini dapat memberikan manfaat untuk para pembaca dan bagi diri Penulis pribadi. Amin.

Padang, 18 Agustus 2011

Penulis

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERYATAAN	iv
HALAMAN PERSEMBAHAN	v
ABSTRAK	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
BAB I PENDAHULUAN	
A. Latar Belakang Masalah.....	1
B. Identifikasi Masalah	3
C. Batasan Masalah	4
D. Rumusan Masalah	4
E. Tujuan	5
F. Manfaat	5
BAB II LANDASAN TEORI	
A. Kriptografi.....	6
B. J2ME	10

C. UML.....	14
BAB III METODOLOGI PERANCANGAN	
A. Rancangan Umum.....	18
B. Rancangan Sistem.....	19
C. Rancangan Antarmuka.....	31
BAB IV HASIL PERANCANGAN DAN PEMBAHASAN	
A. Pengujian.....	37
B. Pembahasan.....	45
BAB V KESIMPULAN DAN SARAN	
A. Kesimpulan	54
B. Saran.....	54
 DAFTAR PUSTAKA.....	 56
LAMPIRAN.....	57

BAB I

PENDAHULUAN

A. Latar Belakang masalah

SMS atau *Short Message Service* merupakan suatu layanan pengiriman pesan singkat melalui telepon seluler. Walaupun merupakan bagian dari kemampuan standard GSM fase pertama, SMS masih merupakan layanan yang banyak digunakan oleh masyarakat. Berbagai kemudahan yang ditawarkan oleh SMS antara lain informasi sesuai permintaan, pengunduhan nada dering, sampai dengan transaksi perbankan atau *mobile banking*.

Sejalan dengan perkembangan teknologi informasi, saat ini telepon seluler dapat menjalankan aplikasi Java. Java mengembangkan aplikasi berbasis *device* yang memungkinkan sebuah *device* menjadi lebih pintar. Java mengembangkan teknologinya khusus untuk *device* atau yang biasa disebut J2ME (*Java 2 Micro Edition*) mulai dari tampilan, suara, koneksi internet, *messaging*, bluetooth, video dan lainnya. Sehingga memungkinkan membuat sebuah aplikasi dalam telepon seluler dengan tampilan yang tidak kalah dengan aplikasi *desktop* komputer. Kelebihan ini membuat para pengembang memikirkan untuk mengembangkan aplikasi berbasis telepon seluler. Dengan memiliki kelebihan tidak membutuhkan ruang kerja, komputer, tempat tertentu dan waktu tertentu. Teknologi *mobile* bahkan dapat dilakukan dalam situasi apapun asalkan pengguna membawa telepon seluler.

Pada *Global Service for Mobile communications* (GSM) yang memiliki jumlah pengguna terbesar di dunia, memiliki beberapa kerentanan terhadap masalah keamanan. Dalam GSM hanya lalulintas udara di antara *Mobile Station* (MS) dan *Base Transceiver Station* (BTS) yang secara opsional dienkripsi dengan stream cipher yang lemah. SMS juga memiliki beberapa kerentanan terhadap SMS palsu (*fake SMS*) yang dapat dikirim melalui internet. Ketika seseorang melakukan roaming konten SMS melalui jaringan yang berbeda seperti internet maka ia akan dihadapkan pada kerentanan serangan keamanan. Kekhawatiran lainnya muncul ketika ada yang mendapatkan akses ke telepon dan membaca pesan yang tidak terlindungi.

Bagi seseorang atau kelompok yang tidak ingin informasinya diketahui, atau tindak tanduknya dimata-matai, maka diharapkan terdapat suatu pengamanan untuk kenyamanan berkomunikasi. Keamanan yang dipakai dengan metode kriptografi dimana suatu pesan atau informasi diubah menjadi pesan rahasia, dikirimkan ke penerima maka dengan metode kriptografi juga pesan rahasia dikembalikan menjadi pesan atau informasi. Kriptografi pada SMS bisa diwujudkan karena SMS berupa text, text bisa di ubah dengan metode, atau algoritma tertentu dienkripsi dan didekripsi.

Algoritma Vigènere termasuk kode abjad majemuk. Dipublikasikan oleh diplomat Perancis, Blaise de Vigènere pada tahun 1586. Algoritma Vigènere teks kode selalu mengganti nilai setiap teks asli tertentu. Pada teknik Vigènere setiap teks kode bisa memiliki banyak kemungkinan teks-asli.

Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut bujursangkar Vigenère . Bujursangkar Vigenère berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang.

Untuk mewujudkan keamanan berkomunikasi khususnya komunikasi menggunakan media SMS penulis tertarik membuat program akhir tentang **”Perangkat Lunak Kriptografi SMS Dengan Algoritma Vigènere”**

B. Identifikasi Masalah

Berdasarkan latar belakang masalah, dapat diidentifikasi masalah yang ada sebagai berikut :

1. Layanan SMS masih merupakan layanan komunikasi yang populer dimasyarakat, sehingga terdapat komunikasi bersifat rahasia, dan tidak adanya jaminan pesan yang dikirimkan aman, tidak akan diketahui oleh pihak lain.
2. Banyaknya bermunculan aplikasi-aplikasi penyadap SMS dan telepon, sehingga kenyamanan berkomunikasi akan terganggu.
3. Terdapat SMS palsu (*fake SMS*) yang dapat dikirim melalui media komunikasi lain seperti internet. Hal ini memacu kekhawatiran pada ruang lingkup pribadi dimana SMS biasa digunakan untuk melakukan pertukaran pesan yang sifatnya rahasia.

4. Dalam GSM hanya lalulintas udara di antara *Mobile Station* (MS) dan *Base Transceiver Station* (BTS) yang secara opsional dienkrpsi dengan *stream cipher* yang lemah.
5. Pada Aplikasi layanan SMS yang biasa, tidak adanya keamanan pesan, baik pesan tersimpan maupun pesan yang dikirimkan.

C. Batasan Masalah

Agar tidak terjadinya kerancuan dalam pembahasan maka penulis membatasi permasalahan yang ada yaitu :

1. Perancangan dan pembuatan aplikasi kriptografi untuk keamanan SMS pada telepon seluler.
2. Perancangan dan pembuatan aplikasi kriptografi SMS menggunakan bahasa pemrograman Java.
3. Perancangan dan pembuatan aplikasi kriptografi SMS menggunakan J2ME.
4. Perancangan dan pembuatan perangkat lunak kriptografi SMS menggunakan metode enkripsi dan dekripsi dengan algoritama vigenere.

D. Rumusan Masalah

Berdasarkan batasan masalah, dapat dirumuskan masalah yang akan dibahas adalah “Bagaimana merancang dan membuat perangkat lunak kriptografi SMS pada telepon seluler dengan metode Vigènere berbasis J2ME?”.

E. Tujuan

1. Tersedianya aplikasi kriptografi untuk keamanan SMS pada telepon seluler.
2. Tersedianya aplikasi kriptografi SMS menggunakan bahasa pemrograman J2ME.
3. Tersedianya perangkat lunak kriptografi SMS dengan metode enkripsi dan dekripsi menggunakan algoritama vigenere.

F. Manfaat

Manfaat yang dapat diperoleh dari Merancang dan implementasi perangkat lunak SMS pada telepon seluler dengan metode Vigènere berbasis J2ME adalah sebagai berikut :

1. Bagi kelompok atau perorangan yang privasinya sangat penting dan tidak ingin privasinya diketahui atau pun dirusak oleh pihak lain akan merasa nyaman berkomunikasi tanpa harus memikirkan gangguan dari pihak lain.
2. Aplikasi kriptografi SMS meningkatkan keamanan pada fasilitas SMS.