BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan dunia teknologi dari tahun ke tahun semakin maju. Terutama dalam persaingan *Gadget* yang saat ini saling menonjolkan fitur-fitur kelebihannya. Salah satunya *BlackBerry*, *BlackBerry* adalah Perangkat Selular yang memiliki kemampuan layanan *Push E-Mail*, Telepon, Sms, Menjelajah Internet, dan berbagai kemampuan nirkabel lainnya. Penggunaan Gadget canggih ini begitu fenomenal belakangan ini, Sampai menjadi suatu kebutuhan untuk *fashion*. BlackBerry pertama kali diperkenalkan pada tahun 1997 oleh perusahaan Kanada, *Research In Motion* (*RIM*). Kemampuannya menyampaikan informasi melalui jaringan data nirkabel dari layanan perusahaan telepon genggam hingga mengejutkan dunia. *BlackBerry* pertama kali diperkenalkan di Indonesia pada pertengahan Desember 2004 oleh operator Indosat dan perusahaan Starhub. Perusahaan Starhub merupakan pengejewantahan dari RIM yang merupakan rekan utama *BlackBerry*. Di Indonesia, Starhub menjadi bagian dari layanan dalam segala hal teknis mengenai instalasi *BlackBerry* melalui operator Indosat.

Produk yang menjadi andalan utama dan membuat BlackBerry digemari di pasar adalah surat-e gegas (*push e-mail*) , *Blackberry Messenger* dan teknologi SMS yang mudah ,cepat dan *realtime*. Produk ini mendapat sebutan surat-e gegas karena seluruh surat-e baru, daftar kontak, dan informasi jadwal (*calendar*) "didorong" masuk ke dalam *BlackBerry* secara otomatis. Sedangkan *Blackberry Messenger*, Mirip dengan Yahoo Messenger, namun dilakukan melalui jaringan *BlackBerry* dengan memasukan nomor identitas atau disebut juga PIN (*Personal Identification Number*).

Teknologi SMS yang digunakan di ponsel *Blackberry* sampai hari ini tetap menjadi media komunikasi yang populer oleh masyarakat, selain mudah digunakan biayanya juga lebih murah. Tapi di sisi lain dari teknologi SMS juga memiliki kelemahan. Teknologi SMS tidak menjamin keamanan dan kerahasiaan pesan yang dikirim. Beberapa risiko juga merupakan ancaman bagi keamanan termasuk SMS spoofing, SMS snooping, dan SMS interception. Dari beberapa ancaman terhadap risiko seperti pesan SMS, maka perlu untuk membangun sebuah aplikasi yang mampu mengamankan dan menyimpan pesan SMS rahasia, sehingga dalam hal terjadi ancaman dan pesan yang dibuka, isi pesan tetap rahasia. Salah satu solusi untuk mengamankan dan menjaga pesan untuk mengenkripsi pesan SMS sebelum pengiriman.

Untuk menangani masalah keamanan ini,salah satu teknik yang sudah dikembangkan untuk mengamankan data adalah dengan menggunakan algoritma penyandian data. Algoritma penyandian data saat ini telah semakin banyak

jumlahnya, sejalan dengan berkembangnya ilmu yang memperlajari penyandian data tersebut. Ilmu ini biasa disebut Kriptografi.

Dalam kriptografi terdapat beberapa metode yang cukup penting dalam pengamanan data yang dikirimkan agar terjaga kerahasiaan data salah satunnya adalah enkripsi (*encryption*). Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi *chipertext*. Sedangkan suatu proses yang dilakukan untuk mengubah pesan tersembunyi ke bentuk asalnya (teks-asli). Pesan biasa atau pesan asli disebut juga *plaintext*, sedangkan pesan yang telah dirubah sehingga tidak bias terbaca disebut juga *chipertext*.

Untuk mengatasi masalah keamanan teknologi SMS pada ponsel *Blackberry* ini, penulis melakukan pendekatan teknologi enkripsi data menggunakan algoritma kriptografi klasik teknik dasar substitusi kode *Vigenere Cipher* yang nantinya diimplementasikan ke dalam aplikasi pengiriman SMS pada ponsel *Blackberry* yang sudah terinstal *Code Signing Key*. *Code signing* adalah proses dimana sebuah kode ditandatangani secara digital oleh pengembang aplikasi dalam rangka untuk menjamin autentikasi dan integritas kode yang kuat bagi pengembang aplikasi. *Vigenere Cipher* adalah suatu algoritma kriptografi klasik yang menerapkan suatu metode cipher subtitusi abjad majemuk. Kode Vigenere telah digambarkan untuk pertama kalinya pada tahun 1553 oleh Giovan Batista Belaso dan dipublikasikan oleh seorang kriptologis Perancis Blaise de

Vigenere pada Abad 16, tahun 1586.[1] Algoritma ini sudah dapat dipecahkan oleh Babbage dan Kasiski melalui metode Kasiski pada Abad 19, maka sebab itu penulis melakukan modifikasi agar algoritma yang baru lebih sulit untuk dipecahkan dengan metode tersebut.

1.2 Rumusan Masalah

Algoritma ini sudah dapat dipecahkan dengan mengetahui panjang kuncinya dengan menggunakan melalui metode Kasiski, maka dilakukanlah modifikasi agar algoritma yang baru lebih sulit untuk dipecahkan dengan metode tersebut. Oleh karena itu skripsi ini diadakan guna menjelaskan tentang :

1. Bagaimana meningkatkan keamanan data algoritma enkripsi Kode *Vigenere Chiper* agar sulit untuk dipecahkan, mengingat Kode *Vigenere Chiper* dapat diketahui panjang kuncinya oleh metode Kasiski.
2. Bagaimana menerapkan algoritma *Vigenere Chiper* yang sudah dimodifikasi ke dalam aplikasi pengiriman SMS di ponsel *Blackberry*.
3. Bagaimana melakukan pengujian algoritma enkripsi yang telah dibuat dari hasil modifikasi teknik dasar *Vigenere Chiper*.

[1] Dony Ariyus, *Pengantar Ilmu KRIPTOGRAFI Teori Analisis dan Implementasi*, h. 65.

1.3 Batasan Masalah

Dari rumusan masalah di atas, maka penulis menentukan batasan masalah. Hal ini sebagai solusi permasalahan, serta untuk membatasi lingkup pembahasan masalah yang telah ditentukan. Yaitu sebagai berikut :

1. Pembuatan program aplikasi hanya menggunakan media pemrograman Java Eclipse Galileo 3.5 beserta Blackberry java plug-in v1.1 .
2. Algoritma Kriptografi Klasik yang digunakan untuk Enkripsi dan Dekripsi data ini jenis Algoritma Simetri yang telah dimodifikasi dari algoritma kriptografi teknik dasar *Vigenere Chiper*.
3. Permasalahan tidak mencakup cara pemecahan algoritma enkripsi yang menggunakan metode Kasiski.
4. Permasalahan tidak mencakup cara kerja *Code Signing Key* saat penginstalan ke ponsel *Blackberry*.
5. Aplikasi enkripsi ini hanya dapat berjalan khususnya di ponsel *Blackberry OS v.5* dan versi sebelumnya.

1.4 Tujuan Penelitian

Dalam penelitian ini ada beberapa tujuan yaitu :

1. Sebagai syarat memperoleh gelar sarjana pada Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

2. Untuk meningkatkan keamanan dalam proses enkripsi pada algoritma enkripsi Kode *Vigenere Chiper* sehingga sulit untuk dipecahkan oleh Kasiski, dan dapat diimplementasikan ke dalam aplikasi pengiriman SMS pada ponsel *Blackberry*.

3. Menerapkan ilmu matakuliah dari system keamanan jaringan, algoritma kriptografi, dan pemorgraman mobile yang menjadi salah satu matakuliah wajib.

1.5 Manfaat Penelitian

Dapat membantu meningkatkan sistem keamanan informasi dalam proses enkripsi teknik dasar Kode *Vigenere cipher* agar sulit untuk diketahui panjang kuncinya melalui metode Kasiski dan tidak hanya mampu melakukan enkripsi terhadap karakter alphabetis saja, namun juga karakter angka dan simbol khusus.

1.6 Metode Penelitian

metode penelitian merupakan cara atau teknik yang dilakukan peneliti untuk menyusun suatu karya tulis dan mengumpulkan data-data yang dibutuhkan. Dalam kasus ini penulis menggunakan beberapa metode pengumpulan data, yaitu:

a. Metode Observasi

Metode ini merupakan cara untuk melakukan pengamatan secara langsung terhadap objek penelitian. Mencari dan menyimpulkan masalah yang ada selama ini dan menentukan solusi permasalahan.

b. Metode Wawancara

Metode ini merupakan metode pengumpulan data dengan cara wawancara terhadap pihak-pihak yang bersangkutan dan orang-orang yang berkompeten di bidang IT khususnya bidang keamanan data sebagai nara sumber.

c. Metode Kepustakaan

Metode kepustakaan merupakan studi literatur untuk mengumpulkan data atau informasi yang berhubungan dengan objek penelitian yang dilakukan. Penulis melakukan studi literatur di perpustakaan STMIK AMIKOM Yogyakarta dan melakukan download data dari berbagai macam sumber dari internet.

d. Metode Eksperimental

Metode eksperimental dilakukan dengan cara uji coba perancangan dan system. Objek dalam hal ini penulis menyajikan simulasi enkripsi dan dekripsi data serta hasil dan analisanya.

1.7 Sistematika Penulisan Laporan

Sistematika penulisan disusun menggunakan dasar-dasar penulisan ilmiah. Metode ini dilakukan agar penyusunan laporan menjadi lebih teratur dan mudah dipahami. Sistematika ini dibagi dalam enam bab, yaitu sebagai berikut :

Bab I : Pendahuluan

Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan & manfaat penelitian, metode penelitian dan sistematika penulisan.

Bab II : Dasar Teori

Bab ini berisi tentang dasar-dasar teori yang digunakan dalam penelitian.

Bab III : Analisa dan Perancangan Sistem

Bab ini berisi mengenai analisa permasalahan dan perancangan program. Serta perancangan antar mukanya.

Bab IV : Implementasi Uji coba program

Bab ini berisi tentang implementasi rancangan perangkat lunak ke dalam antar muka, pengujian dan hasilnya.

Bab V : Penutup

Bab ini merupakan bab yang menyajikan kesimpulan penelitian serta saran.

1.8 Jadwal Penelitian

Tabel 1.1 Tabel Jadwal Penelitian

No:	Kegiatan	Target Output	April-Mei 2010				Juni-Juli 2010				Agustus-Sept 2010				Okt-Nov 2010				Des-Jan 2010			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur	1.Menentukan Permasalahan (latar belakang, rumusan , batasan dan tujuan masalah)																				
		2.Memahami cara kerja Kode *Vigenere Chiper* dan algoritma lainnya																				
		3.Mengumpulkan landasarn teori permasalahan																				
2	Perancangan Sistem	1.Menentukan software yang akan digunakan																				
		2.Menganalisa masalah perancangan																				
		3.Membuat Perancangan sistem																				
3	Uji Coba Rancangan	1.Simulasi Uji Coba Rancangan & Analisa Uji Coba Rancangan 2.Rancangan yang optimal																				
4	Implementasi	1.Mempelajari masalah implementasi sistem																				
		2.Implementasi rancangan ke dalam system																				
5	Uji Coba Sistem	1.Simulasi uji coba sistem 2.Analisa sistem																				
6	Penyusunan Laporan	1.Dokumentasi penelitian secara lengkap 2.Laporan skripsi																				