Enkripsi Sederhana SMS (Short Message Service) Menggunakan Vigenere Cipher

Gagarin Adhitama - 13508089
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18089@students.if.itb.ac.id

Abstraksi – Dewasa ini penggunaan SMS (*Short Message Service*) sudah tidak asing lagi. SMS digunakan sebagai metode komunikasi paling mudah dan murah. Kegunaan SMS pun dapat bermacam-macam. Selain untuk berkomunikasi antar dua individu, SMS juga dapat digunakan untuk melakukan beberapa transaksi seperti SMS *banking*, transaksi penjualan pulsa, dan lainnya. Informasi yang ada di dalam SMS ini seharusnya terjaga kerahasiaannya. Namun, yang terjadi mungkin malah sebaliknya. Isi dari SMS tersebut mengalami ancaman dari segi keamanan. Ancaman yang ada dari berbagai pihak. Pihak yang pertama adalah pihak pemberi layanan SMS (*provider*) karena mereka dapat membaca isi SMS yang tertera di log mereka. Ancaman kedua yakni ketika alat komunikasi (*handphone*) sedang dipinjam orang dan mereka secara sengaja atau tidak dapat membaca isi SMS kita. Oleh karena itu, isi SMS yang mengandung informasi penting seperti kode transaksi, password SMS *banking*, dan informasi lainnya perlu diberikan pengamanan. Salah satu pengamanan yang dapat dilakukan yakni dengan mengenkripsi isi SMS yang akan dikirimkan. Algoritma sederhana seperti Vigenere Cipher pun dapat digunakan dalam mengamankan isi SMS yang dianggap penting dan rahasia.

Kata kunci: enkripsi SMS, Vigenere Cipher.

I. PENDAHULUAN

Setiap orang pasti membutuhkan suatu media komunikasi yang cepat, aman, mudah, dan murah. SMS dianggap sebagian orang adalah metode komunikasi yang tidak sulit, cepat, dan murah tentunya. Hanya dengan beberapa rupiah saja kita dapat menghubungi orang lain yang jaraknya ratusan kilometer dengan kita. SMS ini tidak hanya digunakan kalangan orang bawah saja atau orang kalangan elit saja. Kalangan menengah ke bawah menggunakan SMS sebagai alat komunikasi, sedangkan kalangan elit dapat menggunakan SMS ini sebagai alat bisnis yang mudah dan praktis.

Oleh karena fungsi SMS yang semakin berkembang, tidak hanya sebagai alat komunikasi dua arah saja, maka pengamanan isi dari SMS ini dianggap penting. Misal dalam melakukan transaksi bisnis, dalam SMS *banking*, kita selalu diminta untuk menyebutkan PIN dari SMS *banking*. Kalau saja data tersebut tidak diamankan dan terbaca oleh pihak yang tidak berwenang, data PIN tadi dapat digunakan oleh pihak tersebut untuk mencari keuntungan. Pihak tersebut dapat melakukan pencurian saldo menggunakan SMS banking karena telah mengetahui PIN kita. Selain SMS banking, saat ini sedang marak penjualan pulsa elektrik. Pedagangnya hanya memasukkan kode pulsa, nomor tujuan, dan kode (PIN) lalu mengirimkan SMS tersebut ke pusat server pulsa untuk melakukan transaksi. Server pulsa nanti akan memberikan respon dari permintaan pedagang tersebut dengan mengisikan pulsa ke nomor yang ditulis berdasarkan produk pulsa yang diminta oleh pedagang. Informasi transaksi ini juga cukup penting sehingga butuh untuk dirahasiakan. Contoh kasus, jika pedagang tadi lupa menghapus *sent*

item dari SMS yang dikirimkan kepada server tadi, kemudian *handphone* pedagang tersebut terbaca oleh orang lain, maka orang lain dapat melakukan transaksi pulsa dengan mudahnya dan mengisi pulsa untuk dirinya pribadi atau untuk kepentingan dirinya yang merugikan pedagang tadi.

Selain berasal dari kelalaian pengguna, ancaman SMS ini dapat berasal dari *provider* atau pemberi jasa layanan SMS. Pesan yang kita ketikkan pada SMS, dapat mereka buka dan mereka baca pada sistem *log* mereka. Sistem *log* tersebut disimpan ke dalam database mereka dan dapat dibaca kapan saja ketika dibutuhkan. Tentunya *provider* memiliki intelektual sebagai profesional untuk melayani pelanggannya dengan baik. Namun, siapa tahu terdapat oknum (pegawai) yang memanfaatkan keadaan karena dia dapat membuka akses *log* tersebut dengan mudah. Segala kemungkinan dapat terjadi, maka dari itu kita perlu mewaspadainya agar tidak terjadi hal yang tidak diinginkan.

Isi SMS memang biasanya singkat dan dianggap sepele. Namun untuk beberapa contoh di atas, maka pengamanan isi SMS ini dirasa perlu. Walau menurut orang lain mungkin hal tersebut agaknya tidak mungkin terjadi, atau menurut orang lain isi SMS tersebut dianggap biasa, tetapi hendaknya kita perlu menjaga privasi kita dalam berkomunikasi. Enkripsi SMS dapat digunakan menjadi salah satu metode pengamanan isi SMS agar orang lain yang tidak berwenang membaca pesan tersebut tidak dapat membacanya.

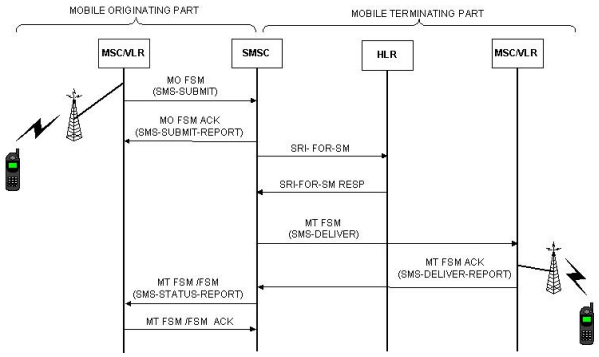
II. LANDASAN TEORI

A. Proses Pengiriman SMS

Secara tidak kita sadari, pengiriman SMS yang dirasa sangat cepat sebenarnya melalui proses yang cukup panjang. Berdasarkan pengalaman penulis yang sempat magang di PT Bakrie Telecom (ESIA), proses pengiriman SMS tersebut melalui beberapa tahap. Pada bagian ini akan dijelaskan secara ringkas mengenai bagaimana proses pengiriman SMS tersebut.

SMS yang kita kirim melalui *handphone* kita akan dikirimkan menggunakan sinyal melalui BTS dan diterima oleh server. Setelah diterima oleh server, maka perintah SMS tersebut akan dieksekusi oleh SMSC (*Short Message Service Center*). Yang dilakukan pertama oleh SMSC adalah pengecekan jumlah SMS yang dikirimkan, karena terdapat kemungkinan pengguna mengetikkan jumlah karakter SMS melebihi jumlah karakter dari satu SMS. Kemudian SMSC akan melakukan pengecekan saldo atau pulsa pengirim apakah cukup atau tidak untuk melakukan transaksi tersebut. Setelah tahap satu dan dua selesai, maka SMSC akan melakukan pengiriman ke nomor tujuan. Jika nomor tujuan tidak terdaftar atau tidak dalam jangkauan, maka SMSC akan mendapatkan *status report* dari jaringan yang ada.

Untuk menjelaskan bagaimana proses pengiriman SMS, dapat dilihat pada gambar 1 berikut yang merupakan diagram alir mengenai proses pengiriman SMS.



Gambar 1 Diagram Alir Pengiriman SMS [3]

Pada gambar tersebut lebih dijelaskan bagaimana SMS diterima dari pengirim ke SMSC dan bagaimana SMSC mengolah permintaan tersebut dan mengeksekusinya. SMSC ini merupakan pengendali utama dalam pengiriman SMS. Segala bentuk *log* disimpan pada SMSC ini. *Log* yang disimpan seperti nomor pengirim, nomor tujuan, status pengiriman, isi SMS, waktu pengiriman, dan waktu penerimaan.

B. Vigenere Cipher

Vigenere Cipher ini merupakan salah satu algoritma kriptografi klasik dengan enkripsi cipher abjad majemuk, dimana huruf yang sama dalam *plain text* belum tentu memiliki *cipher text* yang sama [4]. *Vigenere Cipher* ini memiliki tingkat keamanan yang lebih baik daripada algoritma kriptografi klasik sebelumnya yang merupakan cipher abjad tunggal. Sehingga kemunculan huruf pada *plain text* berbeda dengan *cipher text*-nya. Ketika kemunculan huruf

berbeda, maka penerkaan menggunakan metode kemunculan frekuensi huruf pada *cipher text* akan sulit digunakan dalam memecahkan pesan tersebut.

Penggunaan kunci pada *Vigenere Cipher* ini terdapat beberapa metode. Jika panjang kunci lebih pendek daripada *plain text*, maka kunci dapat diulang-ulangi sepanjang *plain text*. Namun, dapat juga kunci yang pendek tersebut disambung dengan *plain text* sehingga membentuk kunci yang panjang. Metode menyambung kunci dengan *plain text* tersebut sering dikenal dengan *auto-key Vigenere Cipher*. Selain dua metode yang disebutkan di atas, terdapat penggunaan kunci yang sangat panjang yang sering disebut dengan *running-key Vigenere Cipher*.

Algoritma *Vigenere Cipher* ini merupakan algoritma kriptografi klasik dengan metode sederhana, tetapi sudah dapat digunakan untuk mengamankan segala bentuk pesan yang ingin dirahasiakan.

C. Program SMS Android

Android merupakan salah satu pengembang *operating system* berbasis Linux untuk kebutuhan *mobile*. Banyak telepon pintar atau yang sering dikenal dengan *smart phone* berbasiskan *operating system* ini. Pada suatu telepon pintar, program untuk mengirimkan SMS tidak hanya berasal dari program bawaan dari *handphone* ketika kita membelinya. Sekarang, kita sudah dapat membuat suatu aplikasi untuk mengirimkan SMS dengan antarmuka yang kita inginkan. Berbeda dengan telepon jaman dahulu atau pada telepon bukan *smart phone*, dimana kita hanya dapat mengirimkan SMS menggunakan aplikasi bawaan dari pabrik mereka masing-masing.

Aplikasi pada telepon pintar Android ini merupakan aplikasi berbasiskan bahasa Java. Maka dari itu, aplikasi yang akan dibuat untuk eksplorasi kali ini adalah suatu aplikasi SMS dengan basis bahasa Java dan diimplementasikan pada perangkat telepon Android. Aplikasi ini dapat mengirimkan pesan SMS seperti aplikasi pada umumnya, hanya saja nantinya akan terdapat proses enkripsi dan dekripsi pada aplikasi ini. Fungsi utama dari program SMS Android ini adalah dapat mengirimkan pesan menggunakan basis layanan SMS, tetapi pesan yang dikirimkan merupakan pesan yang sudah terenkripsi. Program SMS Android ini juga dapat menerima pesan SMS dan dapat melakukan dekripsi pesan tersebut.

III. PENERAPAN DAN EKSPLORASI

A. Tahap Persiapan

Pada tahap persiapan ini, penulis mengumpulkan materi sebagai bahan pertimbangan dalam mengembangkan program enkripsi SMS tersebut. Terdapat aplikasi untuk melakukan enkripsi pada BBM (*Blackberry Messenger*) dan pengembangnya adalah orang Teknik Informatika ITB. Hanya saja ternyata terdapat perbedaan persepsi antara penulis dengan pengembang enkripsi BBM tersebut. Cara kerja enkripsi BBM tersebut bersifat untuk melakukan penguncian agar orang lain tidak dapat membaca isi BBM. Sehingga ketika pengguna *Blackberry* saling bertukar informasi, pesan yang dikirimkan adalah pesan berbentuk *plain text*. Percakapan disimpan pada perangkat *Blackberry* dalam bentuk *plain text* pula. Ketika pengguna ingin mengamankan pesan-pesannya di BBM, pengguna baru melakukan enkripsi menggunakan aplikasi enkripsi tersebut.

Sedangkan keinginan dan pemahaman penulis adalah pesan dikirimkan dalam bentuk terenkripsi. Hal ini berbeda dengan enkripsi BBM tadi. Karena ketika pesan yang dikirimkan masih dalam bentuk *plain text* berarti pengguna belum sepenuhnya aman dari ancaman kemanan informasi karena isi dari pesan dapat dibaca oleh operator penyedia layanan SMS (*porvider*).

Pada tahap persiapan ini pula penulis menyiapkan bagaimana proses enkripsi dan dekripsi dilakukan pada program SMS ini. Penggunaan algoritma *Vigenere Cipher* membutuhkan kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Vigenere Cipher* yang digunakan adalah *Vigenere Cipher* dengan panjang kunci yang berulang sepanjang *plain text*. Karena program ini berjalan pada perangkat *mobile*, tidak diberikan pilihan *Vigenere Cipher* yang digunakan. Hanya satu model *Vigenere Cipher* yang dipakai pada program ini yakni menggunakan kunci yang pendek dan berulang.

Proses *Vigenere Cipher* ini menggunakan metode pencarian *cipher text* dengan perhitungan sebagai berikut

$$C_{(i)} = (P + K_{(i)}) \bmod 26$$

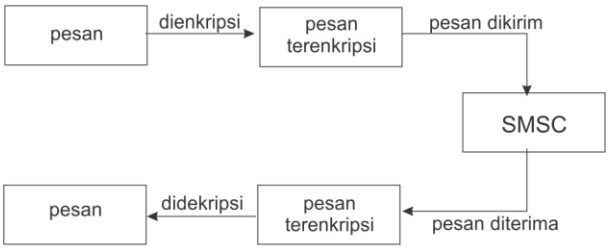
Jadi pada program Java nanti, setiap karakter di-*assign* menggunakan tabel Ascii agar dapat diparsing menjadi sebuah angka *integer*, begitu juga sebaliknya.

B. Tahap Pengembangan

Pada tahap pengembangan ini dibuat terlebih dahulu *daemon* yang bekerja untuk mengenkripsi dan mendekripsi file terlebih dahulu. Pada proses enkripsi, segala bentuk spasi dihilangkan. Sehingga ketika melakukan dekripsi, pembaca harus berpikir untuk memberikan spasi pada tiap-tiap kata. File disimpan dalam bentuk terenkripsi pada *sent item* di telepon genggam, sehingga orang lain yang memegang telepon tersebut tidak dapat mengerti apa isi sesungguhnya karena *sent item* dalam bentuk file terenkripsi. Tujuan dari program ini memang mengamankan isi SMS dari pihak luar yang mungkin meminjam telepon genggam tersebut, dan juga mengamankan isi SMS dari pihak luar yang merupakan operator penyedia layanan jasa SMS (*provider*).

Setelah teks berhasil dienkripsi, teks tersebut dikirimkan menggunakan layanan SMS pada umumnya. Sehingga *log* pada SMSC berisi teks yang terlah terenkripsi, sehingga jika ada pihak yang "usil" untuk melakukan sesuatu yang tidak seharusnya, maka dia akan mengalami kesulitan karena teks bukan dalam keadaan yang dapat dibaca dengan baik. Secara umum, SMSC akan mengirimkan pesan singkat tersebut kepada nomor tujuan.

Setelah SMSC berhasil mengirimkan pesan singkat tersebut, penerima akan menerima SMS dengan model terenkripsi. Sehingga pada *inbox* pesan singkat tersebut belum dapat dibaca. Namun, setelah dilakukan dekripsi maka penerima dapat membaca isi SMS tersebut. Program enkripsi SMS ini terintegrasi dengan layanan SMS di perangkat Android. Secara singkat, sistem kerja program enkripsi SMS ini dijelaskan pada gambar 2 berikut



Gambar 2 Alur Kerja Program Enkripsi SMS

Inti kerja dari program enkripsi SMS ini adalah melakukan enkripsi dan dekripsi pesan asli, sehingga teks yang ada pada inbox, sent item, dan log pada SMSC merupakan teks yang telah tereknripsi. Bahkan ketika kita membuka SMS menggunakan aplikasi bawaan dari *handphone* tersebut, teks yang terdapat pada inbox adalah teks terenkripsi. Sehingga untuk dapat membaca teks tersebut harus menggunakan program enkripsi SMS ini. Karena program ini dapat melakukan dekripsi teks tersebut.

Secara teknologi, program ini hanya mengubah teks yang seharusnya menjadi teks yang terenkripsi. Pada SMSC juga tidak mengalami perubahan apapun. Hanya saja pada *log* SMSC, isi pesan tidak dapat dibaca dengan baik.

C. Hambatan

Pada pengembangan program penerapan kriptografi di sini, hambatan yang paling utama adalah melakukan koneksi ke layanan SMS. Untuk melakukan otomasi ketika mengirim teks yang dienkripsi cukup rumit. Program aplikasi ini seharusnya dapat mengirimkan teks secara otomatis. Pengguna seharusnya hanya memasukkan isi pesan dan kunci ketika mengirimkan pesan, dan ketika menerima SMS, pengguna hanya memasukkan kunci untuk membacanya. Namun, yang terjadi adalah pengguna harus melakukan pemindahan teks agar dapat dikirim menggunakan layanan SMS normal.

IV. ANALISIS HASIL EKSPLORASI

Pada bagian ini akan dijelaskan mengenai hasil dari eksplorasi yang telah dilakukan. Hasil dari eksplorasi menunjukkan bahwa isi SMS telah dapat diamankan dengan metode kriptografi. Hanya saja masih banyak kendala dalam memanfaatkan teknologi kriptografi ini

ke dalam aplikasi SMS.

Kekurangan yang terjadi yakni masalah pertukaran kunci. Untuk mengenkripsi dan mendekripsi pesan, diperlukan kunci yang sama. Sedangkan ketika pengirim SMS belum memberikan kunci kepada penerima, maka penerima tidak dapat membuka isi pesan tersebut. Untuk melakukan pertukaran pesan, jika dilakukan menggunakan SMS biasa, maka akan dirasa kurang aman dalam mengamankan pesan tersebut. Maka, pertukaran kunci harus dilakukan di luar sms. Agar orang lain tidak dapat menerka-nerka apa isi pesan tersebut.

Kekurangan dari program ini adalah ternyata setelah dikembangkan, penulis baru menyadari bahwa program ini belum dapat digunakan untuk melakukan transaksi seperti SMS *banking* dan transaksi pulsa. Alasannya karena server e-banking dan server pulsa yang digunakan tidak mengaplikasikan program untuk mendekripsi pesan ini. Gambaran awal dari penulis adalah pesan ditulis dengan cara biasa, lalu dienkripsi oleh program, lalu dikirimkan melalui SMSC, dan secara otomatis dapat didekripsi dan dibaca. Ternyata tidak semudah itu. Dalam mendekripsi dibutuhkan effort dan tidak otomatis. Ketika program dibuat otomatis dapat mendekripsi, maka kunci yang digunakan selamanya sama. Jika hal ini dilakukan maka kunci akan mudah ditebak oleh kriptanalis. Kemudian jika program dijalankan secara otomatis ketika menerima SMS, maka *inbox* dan *sent item* berisi pesan yang berisi *plain text*. Sehingga keamanan data dari pihak yang meminjam telepon genggam kita belum dapat diamankan. Namun, pada log SMSC sudah dapat diamankan jika program dijalankan secara otomatis.

Program yang dikembangkan saat ini hanya merupakan program kriptografi sederhana yang hasil enkripsinya dapat dikirimkan menggunakan layanan SMS biasa. Secara tidak langsung, program ini dapat digantikan dengan program enkripsi lain yang tidak terintegrasi dengan layanan SMS, lalu hasil enkripsi dari program tersebut disalin ke dalam program SMS biasa dan mengirimnya. Kelebihan dari program enkripsi SMS ini adalah pengguna tidak perlu melakukan salin tulisan.

Perlu kajian lebih lanjut dan kerja keras yang lebih untuk menggunakan program enkripsi SMS pada transaksi perbankan dan jual beli yang berhubungan dengan server atau mesin lain. Karena perlu suatu kustomisasi dan instalasi pada server mereka dalam menerima dan mengirimkan SMS.

Kalau program enkripsi SMS ini hanya digunakan sebagai pengamanan dari pihak yang meminjam *handphone* kita saja (tanpa mengamankan isi SMS dari *log* SMSC), maka program ini tidak ada bedanya (secara tujuannya) dengan program SMS *lock*. SMS *lock* merupakan sebuah aplikasi dimana kita harus memasukkan password ketika ingin membuka aplikasi untuk SMS. Tujuan penulis pada awalnya adalah ingin membuat suatu terobosan dalam hal keamanan data sehingga isi pesan SMS dapat terjaga kerahasiaannya dari siapapun. Namun, ternyata dalam mengembangkan ke arah keamanan data SMS untuk bertransaksi elektronik cukup berat dan banyak hambatannya. Program enkripsi SMS masih bersifat lokal dan hanya dapat digunakan untuk dua pihak yang telah menginstal program tersebut dan telah saling bertukar kunci.

V. KESIMPULAN

Dalam mengembangkan program enkripsi SMS ini perlu dilakukan banyak riset dan kajian. Untuk mengamankan isi pesan SMS dari seluruh pihak, tantangan yang ada cukup berat. Program enkripsi SMS ini juga belum dapat dikembangkan pada transaksi elektronik yang menggunakan jasa SMS. Alasan utamanya adalah karena transaksi elektronik seperti SMS *banking*, jual beli pulsa, dan lain sebagainya menggunakan *server* atau mesin pengolah SMS dengan format yang telah ditentukan. Ketika kita ingin mengadopsi program enkripsi SMS pada transaksi-transaksi tersebut, maka yang harus dilakukan adalah melakukan kustomisasi pada *server* mereka. Lain daripada itu, kunci yang digunakan belum dapat di-*auto generate*. Sehingga pengirim dan penerima harus bertukar kunci terlebih dahulu. Permasalahan tukar kunci ini juga menambah kesulitan untuk mengaplikasikan program enkripsi SMS ini pada transaksi seperti SMS *banking* dan transaksi jual beli pulsa.

Walau masih banyak kekurangannya, program enkripsi SMS ini merupakan program sederhana yang dapat digunakan untuk mengamankan isi pesan SMS pada *handphone* berbasiskan OS Android. Dari hasil eksplorasi ini dapat disimpulkan beberapa hal yaitu

1. Isi pesan SMS itu walau sederhana, tetapi merupakan privasi dari pengirim dan penerimanya.
2. Algoritma *Vigenere Cipher* yang merupakan algoritma kriptografi klasik pun dapat digunakan sebagai salah satu alternatif pengamanan isi data SMS
3. Ancaman keamanan pesan SMS tidak hanya dari orang di sekitar kita yang sering meminjam perangkat telepon atau *handphone* kita, melainkan mungkin juga berasal dari pihak penyedia layanan jasa SMS.

REFERENSI

Petter Buba, Zirra, & Maksha Wajiga, Gregory. (2011). *Chryptographic Algorithms for Secure Data Communication*. International Journal of Computer Science and Security (IJCSS), Vol. 5.

Rahma Gayatri, Dianing. (2011). *Aplikasi Enktripsi SMS Berbasis J2ME Menggunakan Vigenere Chiper*. Tugas Akhir UPN "Veteran" Jawa Timur.

http://learntelecom.com/telephony/gsm/sms-in-gsm-network

http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Maret 2012

ttd

Gagarin Adhitama - 13508089