SISTEM KEAMANAN SMS DENGAN METODE VIGENERE CIPHER BERBASIS J2ME

Mei Lestari

Teknik Informatika, Fakultas Teknik, Matematika dan Ilmu Pengetahuan Alam Universitas Indraprasta PGRI
Jl. Nangka No. 58C Tanjung Barat (TB Simatupang), Jagakarsa, Jakarta Selatan, DKI Jakarta 12530, Indonesia
mei_6s@yahoo.co.id

ABSTRAK

Salah satu fasilitas yang sangat sering disediakan telephone selular adalah untuk melakukan pengiriman data berupa pesan singkat melalui SMS (Short Message Service). SMS merupakan media paling banyak digunakan saat ini dikarenakan biayanya murah dan prosesnya cepat. Layanan pengiriman pesan singkat ini sangatlah standar dan tidak jarang para pengguna telephone selular menggunakan layanan SMS (Short Message Service) ini untuk mengirimkan suatu pesan yang penting dan rahasia, namun para pengguna layanan SMS (Short Message Service) tersebut sering kali tidak mengetahui bahwa jalur komunikasi SMS (Short Message Service) memiliki banyak sekali celah yang memungkinkan untuk terjadinya serangan pada pesan teks yang dikirim. dari permasalahan tersebut, penulis mencoba membuat suatu aplikasi untuk pengamanan data SMS (Short Message Service) dengan salah satu metode enkrip di atas. Aplikasi tersebut diberi judul "Sistem Keamanan SMS dengan Metode Vigenere Cipher Berbasis J2ME". Aplikasi ini berhasil meningkatkan keamanan pengiriman pesan SMS (Short Message Service) melalui telephone selular karena pesan yang dikirimkan terenkripsi menggunakan kunci (key) yang dimasukkan berulang sehingga akan menyulitkan proses dekrip bagi yang tidak tahu kunci sebenarnya. Kunci dekrip berbeda jika proses enkripsi dilakukan lebih dari satu kali atau berulang.

Kata kunci: ***ciphertext,* enkripsi, *vigenere,* SMS *(Short Message Service)***

I. PENDAHULUAN

A. Latar Belakang Masalah

Teknologi Java merupakan sebuah teknologi yang berkembang sangat pesat akhir-akhir ini. Teknologi Java banyak digemari dan digunakan dikalangan praktisi *software* dalam mengembangkan beragam tipe aplikasi, mulai dari aplikasi-aplikasi *desktop*, *applet*, aplikasi *web* dan aplikasi yang dapat di jalankan didalam perangkat-perangakat kecil seperti *telephone* selular, *pager* maupun PDA (*Personal Digital Assistant*).

Aplikasi yang mempelajari bahasa pemrograman lewat aplikasi *mobile* yang terdapat didalam *telephone* selular. Yang cukup dikenal luas adalah J2ME (*Java Micro Edition*). Salah satu fasilitas yang sangat sering disediakan *telephone* selular adalah untuk melakukan pengiriman data berupa pesan singkat melalui SMS (S*hort Message Service*) Merupakan media paling banyak digunakan saat ini dikarenakan biayanya murah dan prosesnya cepat. SMS (S*hort Message Service*) merupakan fitur dari suatu jaringan GSM (*Global System for Mobile Communication*) yang dikembangkan dan distandarisasi oleh ETSI (*European Telecommunication Standards Institute*). Layanan pengiriman pesan singkat ini sangatlah standar dan tidak jarang para pengguna *telephone* selular menggunakan layanan SMS (*Short Message Service*) ini untuk mengirimkan suatu pesan yang penting dan rahasia, namun para pengguna layanan SMS (*Short Message Service*) tersebut sering kali tidak mengetahui bahwa jalur komunikasi SMS (*Short Message Service*) memiliki banyak sekali celah yang memungkinkan untuk terjadinya serangan pada pesan teks yang dikirim. Pada saat kita mengirim pesan SMS (*Short Message Service*) dari *telephone* selular maka pesan *S*MS (*Short Message Service*) tersebut tidak langsung dikirim ke *telephone* selular tujuan, akan tetapi terlebih dahulu dikirim ke SMS (*Short Message Service*) dengan prinsip *Store and Forward* (disimpan dan teruskan), setelah itu baru dikirmkan ke *telephone* selular tujuan.

Dengan tersimpannya pesan SMSC (*Short Message Service Center*) maka penyerang bisa mendapatkan pesan dengan melakukan penyusupan pada SMSC (*Short Message Service Center*) tersebut. Hal ini membuktikan bahwa jalur komunikasi SMS (*Short Message Service)* memerlukan sebuah teknologi enkripsi yang mampu menghalangi semua ancaman keamanan tersebut. Untuk mengurangi resiko yang ditimbulkan dari celah-celah yang terdapat pada layanan SMS (*Short Message Service*) tersebut salah satu penanggulangannya adalah dengan menerapkan suatu kriptografi pada pesan yang dikirmkan. Dengan terenskripsinya pesan maka informasi pesan teks yang dapat dicuri dari SMSC (*Short Message Service Center*) tersebut akan sulit diketahui isinya.

Salah satu metode enkripsi yang digunakan adalah metode Vigenere Cipher, yang akan meminta *password* untuk setiap SMS (*Short Message Service*) yang akan dikirimkan. *Password* yang diberikan akan men-generate isi berita SMS (*Short Message Service*). Sehingga akan membentuk deretan kode yang hanya bisa dibaca oleh penerima yang mengetahui kode

password yang bersangkutan. Vigenere Cipher mungkin adalah contoh terbaik dari Cipher alphabet-majemuk 'manual' sangat dikenal karena mudah dipahami dan implementasikan.

Berangkat dari permasalahan tersebut diatas, penulis mencoba membuat suatu aplikasi untuk pengamanan data SMS (*Short Message Service*) dengan salah satu metode enkrip di atas. Aplikasi tersebut diberi judul "Sistem Keamanan SMS dengan Metode Vigenere Cipher Berbasis J2ME".

B. Perumusan Masalah

Penyampaian pesan teks berbasis SMS (*short message service*) dari pengirim dan penerima seringkali mempunyai kerentanan dari aspek *privacy* atau kerahasian pribadi. Lalu lintas pesan dalam media *transmisi* SMS (*Short Message Service*) saat ini dapat disadap dan di buka dengan perangkat penyadapan untuk keperluan *intelijen,* penyidikan *tipikor,* dan pengawasan terhadap orang yang dicurigai melakukan suatu tindak pelanggaran peraturan perundang-undangan yang ada.

Pengguna (*User*) piranti *telephone* selular menginginkan transmisi baik pengiriman maupun penerimaan SMS (*short message service*) dari/ke seseorang terjamin *security*-nya. Hal ini menyangkut aspek kerahasian pribadi yang sudah menjadi hak pengguna (*User*) piranti *telephone* selular , dimana *property* yang ditransmisikan dalam penyampaian data elektronik dalam bentuk *binary* data, hanya pengirim dan penerima sejalah yang mempunyai Hak Akses (*previllage*) terhadapnya. ITU (*International Telecommunication Union*) mengatur secara ketat, pengecualian terhadap ketentuan *privacy* dalam penyampaian data elektronik tersebut.

J2ME (*Java 2 Micro Edition*) sebagai suatu sistem yang secara *default* memungkinkan suatu aplikasi *mobile device* berupa MIDlet adalah sebutan aplikasi-aplikasi yang dibuat didalam *telephone* selular dengan menggunakan profil MIDP (*Mobile Information Device Profile*). Dapat mengenskripsi sinyal yang dikirim dari perangkat *telephone selular* yang telah di*instal* aplikasi pengenskripsi pesan. Dari penjelesan di atas, dapat di ambil identifikasi masalah yang menjadi pembahasan penelitian yaitu.

1. Bagaimanakah merancang sebuah sistem aplikasi pesan teks yang terenskripsi secara Vigenere Cipher ?
2. Apa kelebihan dan kekurangan dari pesan teks yang terenskripsi dengan metode Vigenere Cipher ?
3. Apakah jenis operator dan jenis *telephone selular* yang digunakan berpengaruh dalam proses enkrip dan deskrip ?

C. Tujuan Penelitian

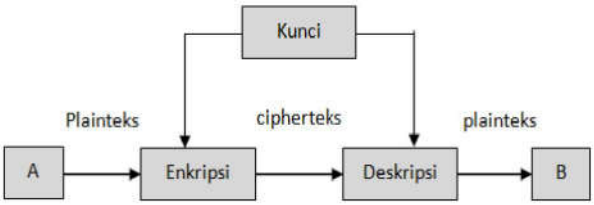
Ada beberapa maksud dan tujuan yang diharapkan bisa tercapai dari pembuatan Aplikasi yang dibuat, diantaranya adalah :

1) Aplikasi ini dapat digunakan untuk keamanan data khususnya pada SMS (*Short Message Service*) agar tidak mudah untuk dipahami oleh pihak- pihak lain yang tidak berkepentingan.
2) Memahami cara pembuatan aplikasi enkripsi dengan menggunakan *software Netbeans* 7.0.1 simulasi J2ME (*Java 2 Micro Edition*)
3) Mendapat keamanan data pada SMS (*Short Message Service*) dengan menggunakan Metode Vigenere Cipher.
4) Memperdayakan pemrograman Java dalam membuat aplikasi keamanan data SMS (*Short Message Service*) menggunakan Metode Vigenere Cipher, sehingga dengan biaya yang murah (*Freeware*) tetap akan mendapatkan program yang berkualitas dan banyak dibutuhkan masyarakat.

II. PENDAHULUAN

A. Sistem Kriptografi Kunci Simetri

Sistem kriptografi kunci simetris merupakan sistem kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci deskirpsi. Kriptografi kunci simetris ini mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka saling berkomunikasi. Kemananan kriptografi kunci simetris tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkripsi dan mendeskripsi pesan. Agar komunikasi tetap aman, kunci harus tetap dirahasiakan. Berikut adalah gambar skema kriptografi kunci simetris[1].



Gambar 1. Skema Kriptografi Kunci Simetri

Kelebihan kriptografi kunci simetris, di antaranya adalah:

1) Algoritma krioptografi kunci simetris dirancang sehingga proses enkripsi/deskirpsi membutuhkan waktu yang singkat
2) Ukuran kunci simetris *relative* pendek. Algoritma kriptografi kunci simetris dapat digunakan untuk membangkitkan bilangan acak.
3) Otentikasi pengirim pesan langsung diketahui dari *ciphertext* yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima pesan saja.

Kelemahan kriptografi kunci simetris

1) Kunci simetris harus dikirim melalui saluran yang aman. Kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci ini.
2) Kunci harus sering diubah, mungkin pada setiap sesi komunikasi.

B. Vigenere Cipher

Vigenere Cipher merupakan salah satu algoritma klasik dengan teknik subtitusi. Nama vigenere diambil dari seorang yang bernama *Blaise de Vigenere*. Vigenere Cipher menggunakan suatu kunci yang memiliki panjang *plaintext.* Jika panjang kunci kurang dari panjang *plaintext,* maka kunci

yang tersebut akan diulang secara periodik hingga panjang kunci tersebut sama panjang *plaintext*[2].

Algoritma enkripsi vigenere cipher :

$$Ci = (Pi+Ki) \bmod 26$$

Algoritma dekripsi vigenere cipher :

$$Pi = (Ci-Ki) \bmod 26$$

Dimana :
Ci = nilai desimal karakter *ciphertext* ke-i
Pi = nilai desimal karakter *plaintext* ke-i
Ki = nilai desimal karakter kunci ke-i

Sebagai contoh, jika *plaintext* adalah THEBEAUTYANDTHEBEAST dan kunci adalah ABC maka proses eknripsi yang terjadi adalah sebagai berikut :

Plaintext : THEBEAUTYANDTHEBEAST
Kunci : ABCABCABCABCABCABCAB
Ciphertext : TIGBFCUUAAOFTIGBFCSU

Pada contoh di atas kata kunci ABC diulang sedemikian rupa hingga panjang kunci sama dengan panjang *plaintext*-nya. Kemudian setelah panjang kunci sama dengan panjang *plaintext*, proses enkripsi dilakukan dengan melakukan menggeser setiap huruf pada *plaintext* sesuai dengan huruf kunci yang bersesuaian dengan huruf *plaintext* tersebut. Pada contoh di atas *plaintext* huruf pertama adalah T akan dilakukan pergeseran huruf dengan kunci Ki = 0 (kunci huruf pertama adalah T akan dilakukan pergeseran huruf dengan kunci Ki=0 (kunci huruf pertama adalah A yang memiliki Ki=0) menjadi T huruf kedua pada *plaintext* adalah H akan dilakukan pergeseran huruf dengan kunci Ki=1 (kunci huruf adalah B yang memiliki Ki=1) menjadi I. Begitu seterusnya dilakukan pergeseran sesuai dengan kunci pada tiap huruf hingga semua *plaintext* telah *terenkripsi* menjadi *ciphertext.*

C. Sistem Pengiriman SMS (*Short Message Service*)

SMS (*Short Message Service*) adalah mekanisme pengiriman pesan singkat melalui jaringan *mobile*. Terdapat sebuah penyimpanan dan penerusan dari pesan yang dikirimkan dari dan ke *mobile.* Pesan (hanya teks) dari *mobile* tujuan. Artinya, apabila penerima tidak aktif, pesan singkat disimpan terlebih dahulu dan dapat dikirimkan kemudian. Setiap pesan singkat tidak boleh lebih dari 160 karakter apabila hanya karakter latin yang digunakan jika terdapat non latin *alphabet* seperti karakter Arab atau China, maka hanya 70 karakter. Karakter dapat berupa *text* (*alphanumeric*) atau binary *non-text*[3].

D. Cara Kerja SMS (*Short Message Service*)

Saat ini SMS (*Short Message Service*) digunakan oleh pengguna dalam pertukaran pesan antar orang, layanan informasi, peringatan *internet email*, layanan *download*, aplikasi *chat*, penetuan posisi kendaraan, pemonitor, sedangkan pemanfaatan SMS (*Short Message Service*) oleh operator antara lain SIM *lock*, SIM *update*, indikator pesan yang tertunda, *Wap Push.*

Implementasi layanan SMS (*Short Message Service*) berdampak pada penambahan berbagai elemen dalam arsitektur jaringan (*GSM, GPRS, UTMS*). Dua komponen penting yang dibutuhkan yaitu SMSC (*Short Message Service Center*) dan *Email gateway*. SMSC (*Short Message Service Center*) memegang peranan penting dalam arsitektur SMS (*Short Message Service*)

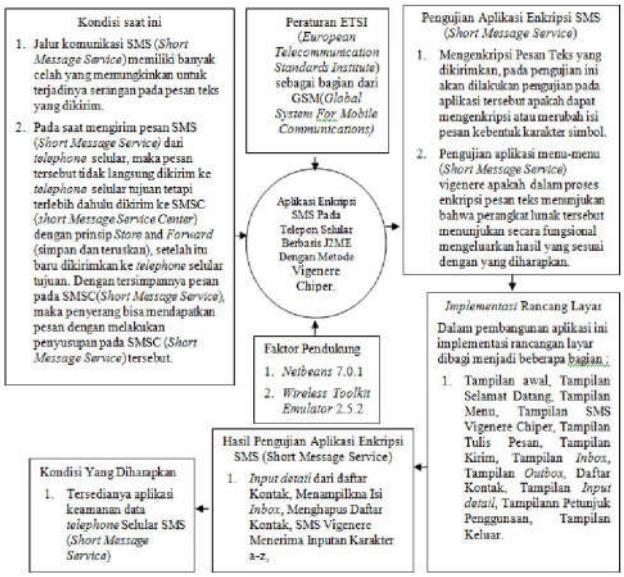
Fungsi utama dari SMSC (*Short Message Service Center*) adalah menyampaikan pesan di antara SME (*Short Message Entities*), mengirimkan pesan pendek. Secara teori, satu SMSC (*Short Message Service Center*) dapat mengatur SMS (*Short Message Service*) untuk beberapa operator jaringan *telephone* selular membuat persetujuan untuk bertukar pesan diantara jaringan. Sebuah pesan yang dikirim dari SME (*Short Message Entities*) ke jaringan A dapat diterima pada SME (*Short Message Entities*) lainnya milik jaringan B. Sedangkan *Email gateway* berfungsi sebagai penghubung antara Email ke SMS (*Short Message Service*) dengan menghubungkan antara SMSC (*Short Message Service Center*) dengan *internet.*

Dengan teknologi GSM/GPRS (*Global System For Mobile Communications , General packet Radio Service*) operator jaringan *telephone* selular dapat dengan mudahnya melakukan pertukaran pesan dari jaringan yang berbeda. Pemetaan sinyal dilakukan di antara dua jaringan *telephone* selular. Dalam pemetaan dua jaringan ini, SMSC (*Short Message Service Center*) dari pembuat SME (*Short Message Entities*) mengolah HLR (*Home Location Register*) jaringan tujuan untuk mendapatkan informasi mengenai penerima dan mengirimnya langsung. Dalam contoh ini, SMSC (*Short Message Service Center*) penerima pesan tidak berpengaruh
Untuk pengiriman pesan di antara teknologi jaringan yang berbeda seperti *GSM/GPRS* dan *CDM* (*Global System For Mobile Communications, General Packet Radio Service, Code Division Multiple Access*), dilakukan dengan menyambungkan dua *gateway* jaringan *telephone* selular dengan menggunakan *protocol* pertukaran.

Dalam pengiriman antar dua teknologi jaringan yang berbeda terdapat tahap. Pertama pesan dibuat dan kirimkan oleh SME (*Short Message Entities*) ke SMSC (*Short Message Service Center*) pengirim. Selanjutnya SMSC (*Short Message Service Center*) pengirim meneruskan pesan melalui SMSC (*Short Message Service Center*) penerima dan SMSC (*Short Message Service Center*) penerima mengirimkan pesan ke SME (*Short Message Entities*) penerima. Jika status *report* diminta oleh pengirim pesan, maka SMSC (*Short Message Service Center)* penerima membuat status dan mengirimkannya ke SME (*Short Message Entities*) pengirim[4].

E. Kerangka Berpikir

Kerangka berpikir pada penelitian ini dijelaskan dalam gambar berikut:



Gambar 2. Kerangka Berfikir Penelitian

III. METODOLOGI PENELITIAN

Dalam melakukan penelitian senantiasa diperlukan suatu metode penelitian yang sesuai dengan pokok permasalahan yang akan diteliti, sedang penelitian itu sendiri adalah suatu metode yang digunakan dalam penelitian yang dapat berbentuk metode penelitian *survei, ex post facto*, eksperimen, naturalistic, *policy research* (penelitian *policy*), *action research* (penelitian tindakan), evaluasi[5].

Metode penelitian yang digunakan oleh peneliti dalam perancangan aplikasi pada tugas akhir ini penulis menggunakan metode *Waterfall*. Metode *Waterfall* adalah metode yang menyarankan sebuah pendekatan yang sistematis dan sekuensial melalui tahapan-tahapan yang ada pada SDLC (*System Development Life Cycle*), Siklus Hidup Pengembangan Sistem) untuk membangun sebuah perangkat lunak.

IV. HASIL DAN PEMBAHASAN

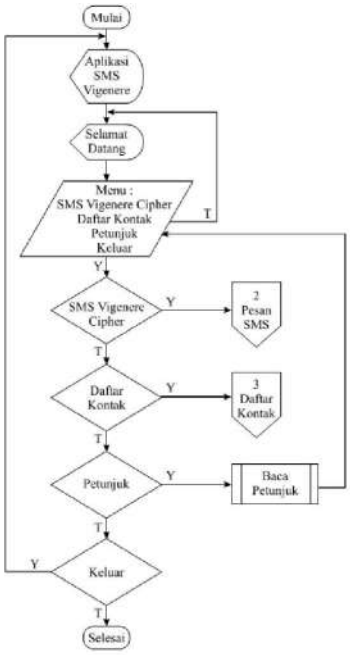
A. Algorima Penyelesaian dengan Flowchart dan Pseudocode

1. Flowchart

Flowchart untuk "**Aplikasi Enkripsi SMS Pada Telepon Selular Berbasis J2ME Dengan Metode Vigenere Cipher**" adalah sebagai berikut :

a) *Flowchart* Menu Utama

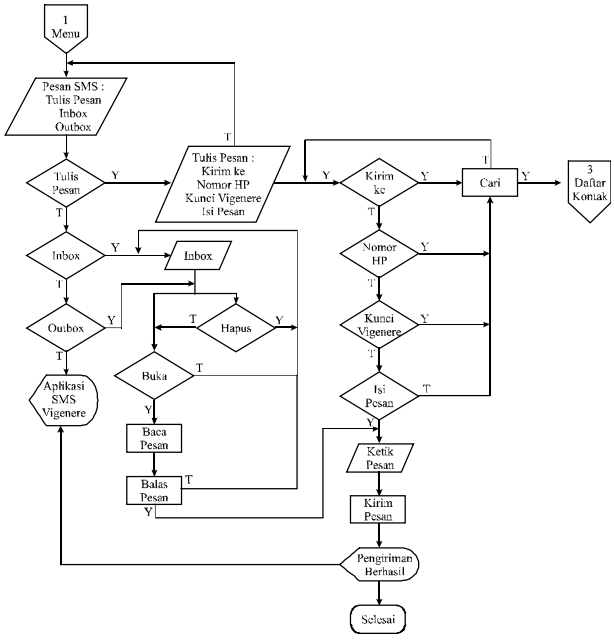
Menu pilihan terdiri dari menu SMS Vigenere Cipher, Daftar Kontak, Petunjuk, dan Keluar.



Gambar 3. Flowchart Menu Utama

b) *Flowchart* Submenu SMS Vigenere Cipher

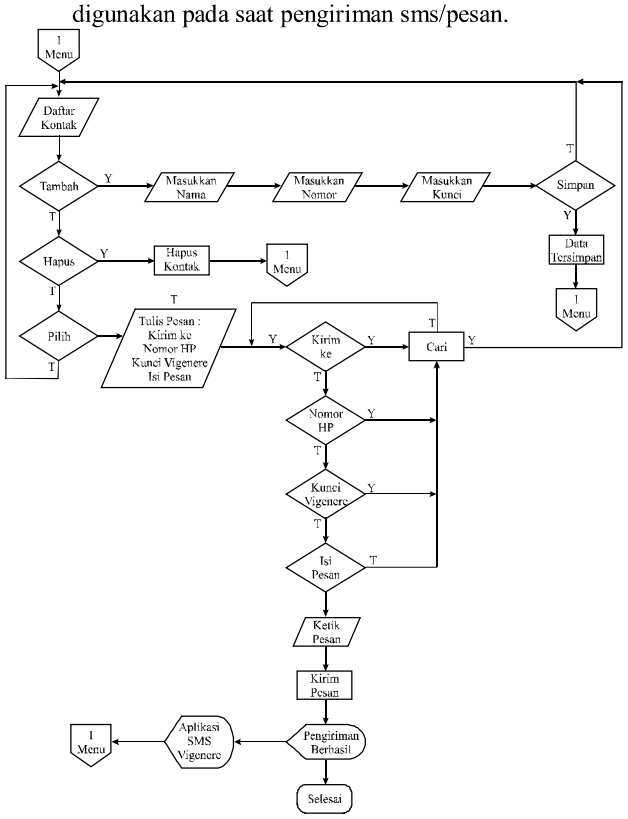
SMS Vigenere Cipher berguna untuk membuat pesan baru, melihat pesan yang masuk melalui submenu *inbox*, dan melihat pesan yang keluar/telah dikirim melalui submenu *outbox*.



Gambar 4. Flowchart Submenu SMS Vigenere Cipher

c) *Flowchart* Submenu Daftar Kontak

Submenu Daftar Kontak berfungsi untuk menambah, menghapus dan memilih data kontak yang akan digunakan pada saat pengiriman sms/pesan.



Gambar 5. Flowchart Submenu Daftar Kontak

2. Pseudocode

a. Pseudocode Menu

DISPLAY Aplikasi SMS Vigenere
DISPLAY Selamat Datang
INPUT SMS Vigenere Cipher, Daftar Kontak, Petunjuk, Keluar
Jika tidak melakukan INPUT maka kembali ke DISPLAY Selamat Datang
Pernyataan kondisi :
Jika SMS Vigenere bernilai 'Ya', maka proses ke modul Pesan SMS
Jika SMS Vigenere bernilai 'Tidak', maka proses ke kondisi Daftar Kontak
Jika Daftar Kontak bernilai 'Ya', maka proses ke modul Daftar Kontak
Jika Daftar Kontak bernilai 'Tidak', maka proses ke kondisi Petunjuk
Jika Petunjuk bernilai 'Ya', maka Baca Petunjuk dan kembali ke INPUT SMS Vigenere Cipher, Daftar Kontak, Petunjuk, Keluar
Jika Petunjuk bernilai 'Tidak', maka proses ke modul Keluar
Jika Keluar bernilai 'Ya', maka kembali ke DISPLAY Aplikasi SMS Vigenere
Jika Keluar bernilai 'Tidak', maka proses Selesai
Proses Selesai

b. Pseudocode Menu ditransformasikan dalam bahasa pemrograman Java

```
public void listMenuUtamaAction() {
String__selectedString=getListMenuUtama().getString
(getListMenuUtama().getSelectedIndex());
 if (__selectedString != null) {
 if (__selectedString.equals("SMS VIGENERE
CIPHER")) {
    switchDisplayable(null, getListMenuMessaging());
 } else if (__selectedString.equals("DAFTAR
KONTAK")) {
    switchDisplayable(null, getListDaftarKontak());
    lookListKontak();
 } else if (__selectedString.equals("PETUNJUK")) {
    switchDisplayable(null,
getFormPetunjukPenggunaan());
 } else if (__selectedString.equals("KELUAR")) {
    switchDisplayable(null, getSplashScreenOut());
 }
 }
 }
public SplashScreen getSplashScreenCome() {
 if (splashScreenCome == null) {
 splashScreenCome = new SplashScreen(getDisplay());
 splashScreenCome.setTitle("");
 splashScreenCome.setTicker(getTicker1());
 splashScreenCome.setCommandListener(this);
 splashScreenCome.setImage(getImage1());
 splashScreenCome.setText("SELAMAT DATANG");
 splashScreenCome.setTextFont(getFont1());
 splashScreenCome.setTimeout(10000);
 }
return splashScreenCome;
}
public Ticker getTicker1() {
if (ticker1 == null) {
  ticker1 = new Ticker("APLIKASI ENKRIPSI
SMS");
}
return ticker1;
}
```

B. Hasil Uji Coba

1. Input Detail Dari Daftar Kontak

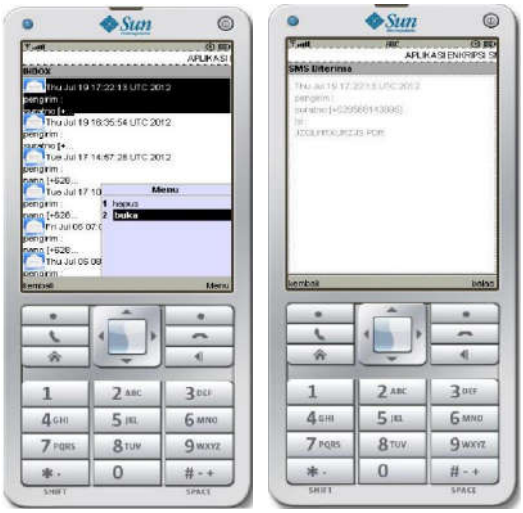
Input detail dari daftar kontak pada aplikasi pengujian enkrip pesan yang akan dikirim dapat melakukan pengiriman pesan dari pengambilan *database* daftar kontak yang sudah terdaftar sesuai dengan kesepakatan kunci vigenere. Dan dapat

melakukan pengiriman pesan yang terenkripsi. Dalam tujuan ini disebut juga *user friendly* (memudahkan sistem penggunaan pada *user*)

Gambar 6. Tampilan awal Menu Enkripsi

2. Menampilkan Isi Inbox

Pada pengujian penerimaan pesan dapat mendekripsikan *ciphertext* sesuai kunci pengirim yang sudah tersedia. Kemudian setiap dekripsi pesan berhasil yang sudah terbaca akan masuk ke dalam *database inbox*. Ketika *user* mencoba kembali untuk membuka pesan yang pernah terkirim, maka pada bagian *inbox* tidak akan bisa dapat lagi mendekripsikan, karena dalam hal ini *ciphertext* hanya sekali terbaca pada saat penerimaan.



Gambar 7. Tampilan isi inbox pesan

3. Menghapus data Daftar Kontak

Pada pengujian aplikasi menu daftar kontak dapat melakukan penghapusan data dari *database* yang sudah terdaftar pada daftar kontak. Dalam hal ini jika ada kesalahan dalam input data yang sudah tersimpan, maka perubahan data tidak dapat di *edit*. Salah satunya adalah dengan penghapusan *database* daftar kontak yang sudah tersimpan dan membuat daftar kontak baru sesuai yang di harapkan.

Gambar 8. Tampilan Hapus Data Daftar Kontak

4. SMS Vigenere Menerima Inputan Karakter a-z

SMS Vigenere hanya membaca inputan karakter (plainteks maupun kunci) dalam karakter a-z. untuk karakter di luar a-z akan ditolak oleh aplikasi secara otomatis.

Gambar 9. Tampilan SMS Vigenere Menerima Inputan Karakter a-z

V. SIMPULAN DAN SARAN

Dari pembahasan sebelumnya, dapat ditarik kesimpulan bahwa:

1. Aplikasi ini berhasil meningkatkan keamanan pengiriman pesan SMS (*Short Message Service*) melalui *telephone* selular karena:
   a) Pesan yang dikirimkan terenkripsi
   b) Kunci (*key*) yang dimasukkan berulang sehingga akan menyulitkan proses dekrip bagi yang tidak tahu kunci sebenarnya.
   c) Kunci dekrip berbeda jika proses enkripsi dilakukan lebih dari satu kali atau berulang.

2. Kunci antara dua orang *user* pengirim dan penerima harus memiliki kunci yang sama untuk bias melakukan enripsi-dekripsi yang sesuai.
3. Hasil pengujian terhadap aplikasi enkripsi pada *telephone* selular berbasis metode vigenere cipher menunjukan bahwa perangkat lunak tersebut secara fungsional mengeluarkan hasil yang sesui dengan yang diharapkan.
4. Aplikasi tersebut dapat berjalan dan berfungsi normal pada *telephone* selular yang mempunyai karakteristik java MIDP 2.0.
5. Komunikasi kirim terima SMS (*Short Message Service*) hanya bisa dilakukan oleh sesama pengguna aplikasi vigenere cipher. SMS (*Short Message Service*) yang akan dikirim akan diterima oleh aplikasi dan masuk kedalam inbox aplikasi, bukan kedalam *inbox* SMS (*Short Message Service*) *default* bawaan *telephone* selular

Untuk perbaikan dan pengembangan aplikasi enkripsi SMS (*Short Message Service*) lebih lanjut disarankan sebagai berikut :

1. Pada penerimaan pesan yang sudah mendekripsikan *ciphertext* sesuai kunci pengirim yang sudah tersedia. Kemudian setiap dekrip pesan berhasil yang sudah terbaca akan masuk ke dalam database *inbox*. Ketika user mencoba kembali untuk membuka pesan yang pernah terkirim dapat mendekripsikan *ciphertext* kembali.
2. Pada aplikasi menu daftar kontak dapat melakukan *edit database* yang sudah terdaftar dalam kesalahan *input* data yang tersimpan.

DAFTAR PUSTAKA

[1] Yusuf Kurniawan, ”Kriptografi Keamanan Internet dan Jaringan Komunikasi ”, penerbit informatika, 2004.
[2] Susanto, T., *Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (MD5),* Mahasiswa Teknik Elektro Universitas Diponegoro, Semarang, 2004.
[3] M. Shalahudin dan Rosa A.S., 2006, Pemrograman J2ME Belajar Cepat Pemrograman Perangkat Telekomunikasi Mobile, Bandung : Informatika.
[4] Andri Kristanto, ”Keamanan Data pada Jaringan Komputer”, Gava Media, 2003.
[5] Al - Bahra bin Ladjamudin. 2005. Analisis dan Desain Sistem Informasi. Yogyakarta : Graha Ilmu.