Aplikasi Enkripsi pesan *SMS* dengan Algoritma Kriptografi *Block Chiper* DES Berbasis Android

Agus Abdullah
Teknik Informatika, Universitas Dian Nuswantoro
Gibs_21@yahoo.com

Abstrak

Perkembangan teknologi pada zaman sekarang ini tidak dipungkir isangatlah cepat, khusus teknologi informasi salah satunya telpon seluler .fitur dan kecanggihan pada telpon seluler mulai bermuncul sampai dengan adanya yang disebut smart phone, yang memiliki berbagai fungsi seperti multimedia, multiplayer games, transfer data, video streaming dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup dikenal luas adalah pada platform smartphone khususnya Android.

Salah satufasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui Short Message Service (SMS). Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS.

Dengan adanya aplikasi kriptografi (enkripsi dan dekripsi) yang menerapkan algoritma simetris Block Chiper DES diharapkan pesanatau SMS seseorang akan aman dan tidak bocor dari penyadap atau pihak yang tidak bertanggungjawab.

Kata Kunci :Kriptografi, *Block Chiper DES*

I. Pendahuluan

Perkembangan teknologi pada zaman sekarang ini tidak dipungkiri sangatlah cepat, khusus teknologi informasi salah satunya telpon seluler. fitur dan kecanggihan pada telpon seluler mulai bermuncul sampai dengan adanya yang disebut smart phone, yang memilikiberbagaifungsiseperti multimedia, multiplayer games, transfer data, video streaming dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan,

diantaranya yang cukup dikenal luas adalah pada platform smartphone khususnya Android.

Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui Short Message Service (SMS). Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS.

Pada Negara yang maju pemanfaatan SMS untuk mengirim pesan rahasia telah lebih dulu dikembangkan. Misalnya di Inggris sebuah perusahaan operator teleponselular, staellium UK, mengeluarkan layanan bernama "stealth text" yang dapat digunakan untuk mengirim pesan dengan aman, yaitu dengan cara menghapus pesan secara otomatis segera setelah 40 detik pesan dibaca atau yang dikenal dengan nama selfdestruct text message. Kini dengan memanfaatkan Wireless Messaging API (Application Programming Interface) dari J2ME parapembuat program Java dapat mengembangkan sendiri sebuah aplikasi pengiriman pesan singkat atau SMS yang dimodifikasi untuk mengamankan pesan.

Salah satu teknik untuk pengamanan data adalah dengan menggunakan penyandian dokumen. Algoritma penyandian saat ini semakin banyak jumlahnya, sejalan dengan berkembangnya ilmu yang mempelajari penyandian data tersebut. Ilmu ini biasa disebut Kriptografi.

Dalam kriptografi terdapat metode yang cukup penting dalam pengamanan data, salah satunya adalah enkripsi (*encryption*). Enkripsi adalah proses yang dilakukan untuk mengubah pesan asli menjadi pesan yang telah diubah, supaya tidak mudah dibaca (*chipertext)*. Sedangkan proses untuk mengubah pesan tersembunyi menjadi pesan biasa (*plain text*) disebut dekripsi.

Atas dasar pertimbangan hal tersebut diatas maka penulis merasa perlu untuk membangun aplikasi keamanan teks yang ditujukan untuk membantu mengatasi masalah keamanan data yang diperuntukkandalampertukaran data melalui*sms*dari pencurian dokumen – dokumen baik yang tidak penting maupun yang penting dan rahasia, sehingga orang lain tidak dapat mengetahui

isi dari data- data tersebut.Berdasarkan hal-hal yang terjadi seperti tersebut di atas, penulis mengambil judul “Aplikasi Enkripsipesan*sms*dengan Algoritma Kriptografi *Block Chiper* DES Berbasis Android”

1. MetodePenilitian

1.1 ObjekPenelitian

Penulis melakukan penelitian terhadap pembangunan aplikasi pengamanan pesansms dengan algoritma kriptografi *Block Chiper DES* Aplikasi pengamanan ini secara umum memiliki 2 (dua) fungsi utama yaitu mengenkripsikan pesan sms dan mendekripsikannya kembali.

1.2 Metode Pengumpulan Data

Metode yang digunakan dalam pengumpulan data adalah studi pustaka dan *Research and Site Visits* (Penelitian dan Mengunjungi Situs)

1.3 Alur Penlitian

1. Perencanaan Sistem/Plannnig

   Kegiatan yang dilakukan pada tahapan ini yaitu dengan mengenali dan mendefinisikan masalah pengamana pesan sms dan mencari alternatif pemecahannya.

2. Analisis Sistem

   Analisis terhadap kebutuhan perangkat keras dan perangkat lunak merupakan proses pengumpulan kebutuhan yang diperlukan dalam pembangunan sistem yang diinginkan. Dengan adanya analisis ini, diharapkan kebutuhan akan perangkat keras dan perangkat lunak dalam mengembangkan sistem akan terpenuhi. Sehingga akan menghasilkan sebuah system yang sesuai dengan tujuan dari penelitian ini.

3. Implementasi Sistem dan Coding

   Padatahapinidilakukan proses transformasipesansmskebentukkode yang dapatdiimplementasikanolehmesin. Tahap implementasi ini akan menggunakan beberapa *tool* pengembangan sistem yang meliputi : mengkonversi pesansms menjadi suatu rangkaian bit, mengenkripsi *plaintext* dan mendekripsi *chipertext* dengan menggunakan kriptografi *Block Chiper DES.*

4. Pengujian (*Testing*) dan evaluasi

   Tahap pengujian ini dilakukan dengan *Black box testing* untuk menjamin aplikasi pengamanan pesansms yang dikembangkandapatbenar-benarbebasdari kesalahan-kesalaham pada *interface*, kesalahan pada performansi dan fungsi yang salah atau hilang. Tahap pengujian ini juga bertujuan untuk menunjukan tentang cara beroprasinya, apakah masukan data dan keluaran data telah berjalan sebagaimana yang diharapkan. Evaluasi dari pengamanan pesan sms ini berbasis pada kuesioner.

5. Pemeliharaan dan Incremental Release

   Proses ini dilakukan setelah sistem yang dihasilkan di sampaikan ke pada pengguna, terutama jika system mengalami permasalahan yang belum ditemukan pada saat proses pengujian, permasalahan ini dapat berkaitan dengan permintaan pengguna yang membutuhkan perkembangan fungsional system maupun adanya penyesuaian dengan lingkungan eksternal seperti adanya perubahan peripheral atau perubahan sistem operasi. Fase pemeliharaan akan mengakibatkan pengembang mengaplikasikan lagi setiap fase pengembangan system mulai dari awal, namun tidak membuat sistem yang baru.

2. Hasil dan Pembahasan

Pada bagian hasil dan pembahasan ini, dibahas mengenai langkah-langkah dan rekayasa yang dilakukan demi mewujudkan aplikasi tersebut serta implementasi dan evaluasi dari system tersebut. Adapun tahapan–tahapan dalam pengembangan aplikasi tersebut, yaitu:

I. Unit Bahasa Pemodelan

a. Use Case Diagram

Dalam bahasa pemodelan ini, penulis menggunakan 1 (satu) buahactor yaitu user. User pada aplikasi ini adalah seseorang yang nantinya akan menjalankan aplikasi MySMSCrypt ini.

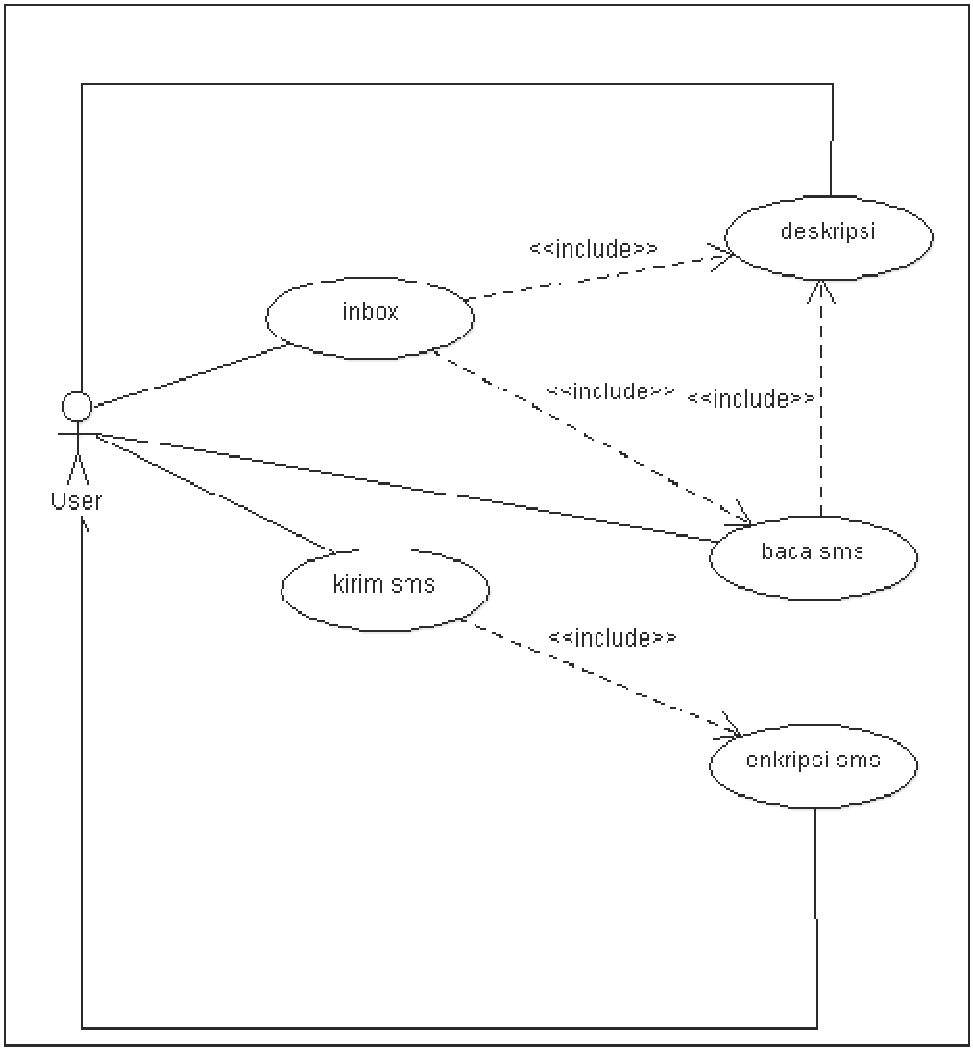
Email Use Case : • Proses KirimdanEnkrip Email
Primary actor : • User
Goal : • User bisamengirimdanmengenkripsms
Precondition : • User mengisikankonfigurasidenganbenar • User mengisikannomortelepontujuandanmengisi key enkripdenganbenar
Trigger : • User inginmelakukanpengirimandanenkripsi email
Scenario : • User membuka menu Kirim SMS • User mengisikannomortelepon yang dituju, isipesandantekantombolenkrip, mengisikan key untukmengenkripsipesan. • User mengeksekusifungsiaplikasienkripdankirimsms. Alternate Flow :
• User keluardariaplikasi
Priority : • Moderate priority
Frequency of use : • Frequent

Tabel :Skenario Use Case Proses KirimdanEnkrip

Use Case : • Proses Inbox Dekripsi
Primary actor : • User
Goal : • User terhubungke Provider dan dapat melihat daftar sms masuk, mendekripsi
Precondition : • User mengisikan konfigurasi dengan benar • User mengisikan key untuk dekripsi sms dengan benar
Trigger : • User ingin masuk ke dalam kotak masuk sms pada provider.
Scenario : • User membuka menu Inbox • User memilih pesan yang akan didekripsi dan memasukkan kunci
Alternate Flow : • User keluar dari aplikasi
Priority : • Moderate priority
Frequency of use : • Frequent

Tabel :Skenario Use Case Proses Inbox Dekripsi

Dibawah ini merupakan pemodelan use case yang penulis pakai pada pembuatan aplikasi ini.

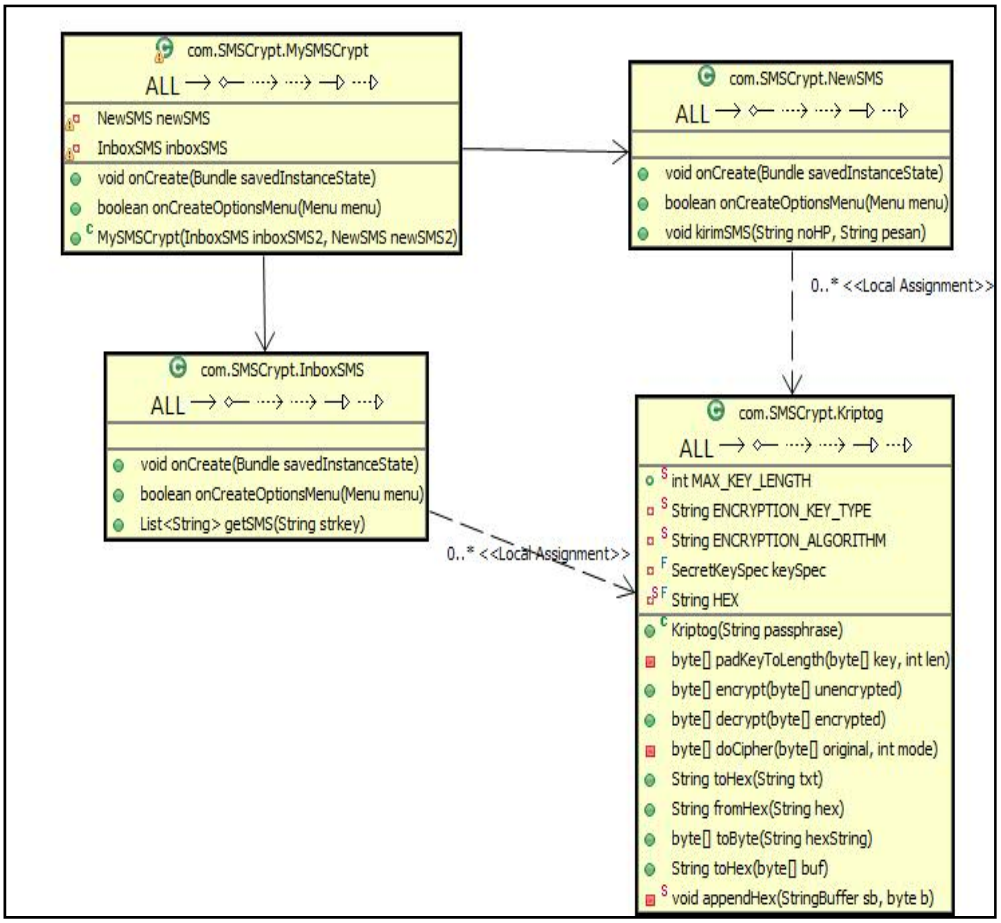


Gambar : Use Case Aplikasi MySMSCrypt

b. Class Diagram

Pada class diagram, penulis menggunakan 4 macam kelas yaitu : MySMSCrypt, NewSMS, InboxSMS, dan Kriptog. Kelas- kelas tersebut saling berhubungan dan mempunyai ke terkaitan. Di bawah ini merupakan gambar dan penjelasan class diagram yang penulis maksud :

- MySMSCrypt : Class yang berisikan tentang menu- menu yang akan di jalankan pada aplikasi.
- NewSMS : Class yang dijalankan untuk pemprosesan pengiriman dan pengenkripsian SMS.
- InboxSMS : Class untuk menampilkan isi dan pendeskripsian SMS
- Kriptog : Class public untuk enkripsi dan deskripsi SMS.



Gambar : Class Diagram Aplikasi MySMSCrypt

II. Implementasi

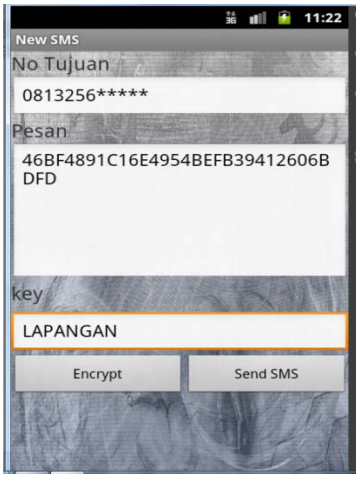
Gambar : Main Menu Aplikasi MySMSCrypt

1. Analisa Percobaan

Penulis akan melakukan beberapa percobaan untuk membuktikan kinerja program yang telah dibuat. Berikut adalah langkah-langkah percobaan yang penulis lakukan untuk mengetahui kinerja program.

1.1 Kirim Pesan

Gambar
Menu Kirim SMS



Gambar
Tampilan Pesan Terenkrip

Gambar Tampilan Pesan Terkirim

Pada gambar diatas penulis melakukan percobaan pada fungsi kirim pesan ke nomor tujuan 085727188888 dengan isi pesan serta dengan kunci seperti yang tertera didalam gambar 4.15, serta mengenkripsi pesan tersebut dengan kunci "test" bentuk chipertext dan pesan berhasil dikirim.

1.2 Kotak Masuk

Gambar

Menu Kotak Masuk

Gambar

Tampilan Pesan Terdekrip

Pada percobaan fungsi Kotak Masuk, penulis menggunakan smartphone sebagai ujicoba fungsi kotak masuk SMS. SMS masuk yang telah diterima akan ditampung pada sebuah tabel, dan untuk membaca pesan yang masuk cukup dengan memasukkan key dekripsinya. Untuk fungsi dekripsi user harus memasukkan kunci untuk mendekripsi SMS tersebut.

2. Hasil Analisa Percobaan

Dari analisa percobaan tersebut diatas penulis melakukan testing pengujian menggunakan metode blackbox. Berikut hasil dari pengujian penulis :

No	Kasus Uji	Skenario	Hasil yang Diharapkan	Hasil Nyata	Ket
1	Pengisian no tujuan	User memasukkan nomor tujuan	User dapat mengirim SMS	Sukses mengirim SMS	Valid
2	Pengisian plaintext	User mengisikan isi pesan yang akan dikirimkan	User dapat mengirim SMS yang akan Dienkripsikan	Isi pesan dapat dienkripsikan	Valid
3	Memasukkan Kunci	User memasukkan kunci untuk proses Enkripsi	Kunci yang dimasukkan dapat digunakan untuk mengenkripsikan isi SMS	Isi SMS dapat dienkripsi dengan kunci yang dimasukkan user	Valid
4	Isi SMS terenkripsi	Isi SMS dienkrip oleh aplikasi Dengan kunci yang telah dimasukkan user	Isi SMS dapat terenkripsi dengan baik	SMS terenkripsi dan tidak dapat dibaca	Valid
5	Pengiriman Chipertext	User mengirimkan Chipertext	Chipertext dikirimkan	Chipertect Dikirimkan dan dapat diterima oleh user penerima	Valid

Tabel : Pengujian Pengiriman dan Enkripsi Pesan

No	Kasus Uji	Skenario	Hasil yang Diharapkan	Hasil Nyata	Ket
1	Penerimaan SMS	User mendapatkan SMS chipertext	User mendapatkan Chipertext yang terkirim	User dapat menampilkan chipertext untuk didekripsikan	Valid
2	Memasukkan Kunci	User memasukkan kunci yang sama dengan proses enkripsi	Kunci yang dimasukkan dapat digunakan untuk Proses dekripsi	Dekripsi chipertext dapat dilakukan dengan kunci yang sama	Valid
4	SMS terdekripsi	Isi SMS dapat terdekripsi setelah user memasukkan Kunci	Isi SMS dapat Didekripsi dengan baik	SMS berhasil didekripsi	Valid

Pengujian Penerimaan dan Dekripsi Pesan

Dari pengujian yang penulis lakukan maka penulis memperoleh beberapa kelebihan dan kekurangan dari metode yang dipakai dalam penelitian ini yaitu.

1. Kelebihan
   a. Penggunaan library standart dari java yang sudah disediakan pada JDK 1.7 meminimalkan pembengkakan coding program, dan menjadikan aplikasi menjadi lebih ringan.
   b. Pengenkripsian dan pendekripsian berjalan dengan lancar dan sempurna, tidak ada kesalahan secara fundamental.
2. Kekurangan
   a. Aplikasi hanya mampu membaca SMS dengan bersifat sementara.

3. Kesimpulan

Berikut adalah kesimpulan yang dapat ditarik dari pembahasan masalah ini:

1. Aplikasi ini dapat melakukan pengamanan terhadap pesan pada SMS dengan metode *Block Chiper DES* (enkripsi dan dekripsi).
2. Penggunaan kamus fungsi standar dari java dan sun microsystem meminimalkan pembengkakan coding pada aplikasi ini.

4. Saran

Saran-saran yang berguna untuk pengembangan aplikasi ini adalah sebagai berikut :

1. Penambahan fungsi pengambilan nomor tujuan dari *contacs phone*.
2. Penambahan fungsi untuk pembacaan SMS yang berbentuk content .agar pembacaan SMS tidak bersifat sementara.

DAFTAR PUSTAKA

[1] http://prihadipati.blogspot.com/2011/04/cybercrime-dan-keamanan-data.html, diakses tanggal 26 maret 2013

[2] Jogiyanto, H. (1999). Analisis dan disain : sistem informasi; pendekatan terstruktur teori dan praktek aplikasi bisnis. Yogyakarta : Andi Offset.

[3] http://id.wikipedia.org/wiki/Layanan_pesan_singkat. 6 April 2013

[4] Munir, Rinaldi (2006). Kriptografi. Bandung : Informatika.

[5] A. Menezes, P. Van Oorschot, and S. Vanstone. (1996). Handbook of Applied Cryptography. USA : CRC Press

[6] Ariyus, D. (2008). Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi. Yogyakarta : Andi.

[7] Schneier, Bruce. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition (Paperback). USA: Wiley.

[8] Drs. Azhari SN,MT, Wahyu Wahyu Nur Hidayat, (2009), Tutorial Pemprograman Mobile (J2ME),Yogyakarta: Gava Media

[9] S.Michel Ivan, N. Yusuf Ronald, Siendow Welly, Wino.W William (2010), Mengembangkan Aplikasi Enterprise Berbasis android. Yogyakarta. Gava Media Yogyakarta

[10] http://deviachrista.blogspot.com/2013/04/pengertian-model-extreme-programming.html. 30 April 2013

[11] http://octarapribadi.blogspot.com/2012/10/contoh-enkripsi-dengan-algoritma-des.html. 5 Mei 2013