

Desain Aplikasi Algoritma MD5 (Message Digest 5) Pada Media SMS Berbasis Android Mobile

Zaiful Bahri¹, Joko Risanto² dan Evfi Mahdiyah³

^{1,2,3}Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Riau
Jl. HR. Soebrantas Km.12,5 Simpang Baru, Panam, Pekanbaru, 28293
Email: ¹zaifulbahri@unri.ac.id, ²jokorisanto@yahoo.com, ³evfi.mahdiyah@gmail.com

Abstrak

Tulisan ini membahas tentang desain Aplikasi Algoritma MD5. Dalam desain ini dibuat model kirim dan terima SMS aman. Dari model ini bisa dibuat desain aplikasi berbasis objek menggunakan Unified Modeling Language (UML), State Machine untuk menggambarkan status pengiriman pesan dan Graphical User Interface (GUI) yang user friendly menggunakan Android Studio 2.3.3 dan gradle 3.3. Desain ini juga memerlukan sebuah database. Hasil desain ini dapat digunakan untuk membangun aplikasi mengirim dan menerima pesan aman secara umum dan khususnya aplikasi algoritma MD5 menggunakan Android.

Kata kunci : Aplikasi, algoritma MD5, Android, SMS aman

Abstract

This paper discusses the design of MD5 Algorithm application. In design is created a model to send and receive secured SMS. From this model is made an application design which is based on object using Unified Modeling Language (UML), State machine to give describing state of send and recive message and Graphical User Interface (GUI) which is user friendly using Android Studio 2.3.3 and Gradle 3.3. The application design also uses a database. The result of design can be used to create an application to send and receive a secure message in general and especially message digest 5 algorithm using Android.

Keywords : Application, MD5 algorithm, Android, secure SMS

1. Pendahuluan

Banyak fitur-fitur aplikasi yang disediakan oleh Android sebagai aplikasi operasi telepon seluler seperti pemutaran video, push email, mengakses layanan internet, call, Short Message Service (SMS), Multimedia Messaging Service (MMS) dan sebagainya. Dari sekian banyak fitur yang dimiliki oleh Android, yang masih banyak digunakan yaitu SMS, bahwa pengguna dapat mengirim dan menerima pesan singkat kepada pengguna ponsel lainnya.

Layanan SMS yang menggunakan aplikasi SMS bawaan ponsel masih banyak digunakan oleh setiap orang, dan bukan merupakan jalur yang aman dalam pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi. Selain itu pengiriman SMS yang dilakukan oleh pengirim tidak langsung sampai ke penerima, akan tetapi pengiriman SMS harus melalui Short Message Service Center (SMSC) yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima.

Dalam buku [1] disebutkan bahwa seorang operator bisa saja mendapatkan informasi atau membaca SMS di dalam SMS Center. Hal ini dapat dibuktikan dari beberapa kasus yang

ditangani pihak kepolisian, kejaksaan atau KPK, di mana pihak-pihak tersebut meminta transkrip SMS ke operator GSM untuk dijadikan bahan penyelidikan di persidangan.

Dengan demikian dibutuhkan suatu metode dan aplikasi yang dapat mempertimbangkan solusi *encrypted end to end* menurut [1][2] dengan melakukan enkripsi terhadap pesan SMS. Enkripsi adalah proses mengubah suatu pesan asli yang disebut sebagai *plaintext* menjadi sebuah sandi atau kode yang tidak terbaca dan disebut sebagai *chipertext* dan tidak dapat dimengerti. Untuk mengembalikan pesan yang dikirim menggunakan suatu algoritma enkripsi tertentu ke bentuk aslinya biasanya diperlukan suatu proses yang disebut sebagai dekripsi. Namun dalam tulisan ini proses dekripsi tidak dapat dilakukan, dikarenakan algoritma MD5 merupakan algoritma satu arah. Untuk itu diperlukan sebuah database melalui hosting untuk menampung data yang terkirim. Data SMS terkirim ke SMSC juga terkirim database. Dengan demikian data yang tersimpan di tabel database bisa dicek kebenarannya. Jika data yang dikirim tidak sama dengan data yang dienkripsi maka data sudah diubah. Jika data tidak ada perubahan, maka data bisa dikembalikan ke bentuk semula melalui sebuah query Data Manipulation Language (DML). Enkripsi dimaksudkan di sini untuk melindungi dan menyamarkan informasi atau pesan agar tidak terlihat dan dimengerti oleh orang lain.

Namun dalam tulisan ini yang menjadi masalah utama adalah bagaimana merancang sebuah aplikasi yang komprehensif dan lengkap. Jarang sekali aplikasi yang dibangun menggunakan rancangan yang utuh dan jelas untuk membangun perangkat lunak seperti yang digambarkan dalam [3] hanya dijelaskan tentang perancangan secara deskriptif dan perancangan *graphical user interface*. Dalam tulisan [4][5] juga hanya menjelaskan rancangan aplikasi secara global untuk membangun perangkat lunak. Untuk itu diperlukan sebuah rancangan yang utuh dan lengkap untuk pembangunan perangkat lunak. Perangkat lunak yang dibangun merupakan perangkat lunak yang diterapkan pada telepon selular berbasis sistem operasi Android menggunakan algoritma message digest 5 (MD5) yang banyak diterapkan di dalam dunia web untuk meng-enkripsi *password* [2][6][7][8] karena memiliki fungsi untuk melakukan enkripsi yang sangat kuat. Perangkat lunak ini dapat mengirim dan menerima pesan. Pengguna berinteraksi dengan perangkat lunak melalui *graphical user interface* yang disediakan oleh perangkat lunak. Pengguna memasukkan data dengan menggunakan keypad yang dimiliki oleh telepon selular. Pesan yang telah dibuat dikirimkan ke telepon selular lain melalui jaringan SMS, secara umum arsitektur global perangkat lunak seperti gambar berikut :

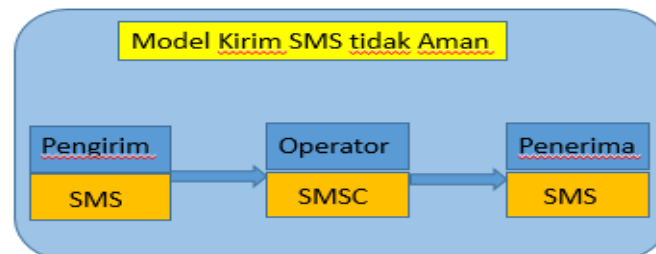


Gambar 1. Arsitektur Global Perangkat Lunak

2. Metode Penelitian

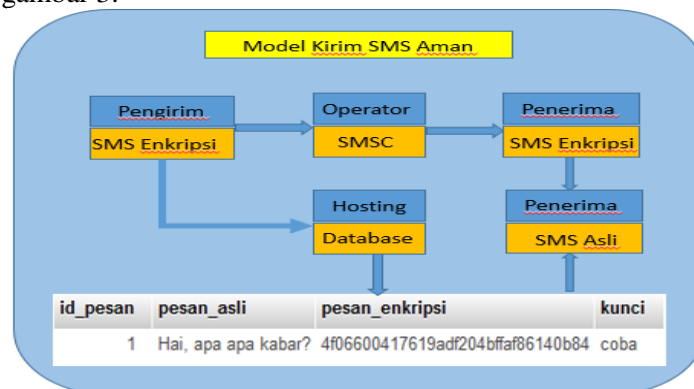
2.1 Model Kirim SMS

Terdapat dua model kirim SMS. Pertama adalah model kirim SMS tidak aman yang sering digunakan oleh masyarakat umum, karena masyarakat tidak mengerti akan bahayanya SMS yang terkirim bisa dibaca oleh operator. Model kirim SMS ini dapat dilihat pada gambar 2.



Gambar 2. Model Kirim SMS Tidak Aman

Kedua adalah model kirim SMS aman. Model kirim SMS Aman ini digunakan untuk mengamankan pesan yang dikirim. Pesan sebelum dikirim dienkripsi terlebih dahulu menggunakan Enkripsi MD5. Enkripsi MD5 tidak mempunyai dekripsi karena algoritma MD5 hanyalah enkripsi satu arah. Untuk membandingkan pesan terkirim dengan pesan yang diterima sama, maka dilakukan suatu metode *query select()*. Jika pesan yang diterima tidak sama dengan hasil metode *query select()* yang ada di tabel, maka pesan asli tidak bisa ditampilkan dan sebaliknya. Lihat gambar 3.



Gambar 3. Model Kirim SMS Aman

2.2 Desain Aplikasi

Untuk merancang perangkat lunak aplikasi pengirim SMS yang aman digunakan Unified Modeling Language (UML). UML [9][10] adalah bahasa visual untuk pemodelan dan komunikasi tentang sistem atau aplikasi dengan menggunakan diagram dan teks pendukung. UML hanya bekerja untuk pemodelan. Jadi penggunaan UML tidak terbatas pada metodologi spesifik [1][11]. Desain yang dibuat adalah *Usecase Diagram*, *Sequence Diagram*, *Activity Diagram* untuk menulis dan membaca SMS dan *Class Diagram*.

Aplikasi yang bagus memerlukan mesin status untuk menggambarkan adanya suatu objek. Mesin status aplikasi tulis dan baca pesan aman menggunakan Algoritma MD5 ini, menggambarkan siklus hidup suatu objek yang terdapat dalam aplikasi.

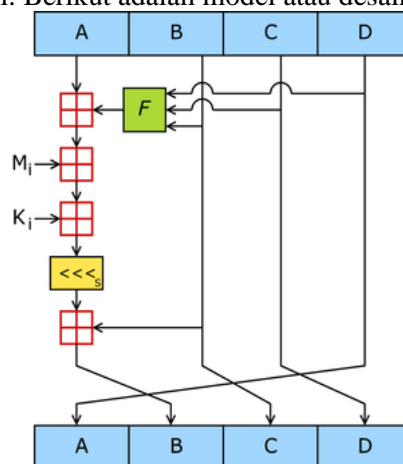
Penelitian ini juga menggunakan sebuah database server sehingga perlu dirancang sebuah database dan sebuah tabel. Tabel terdiri dari empat *field*, digunakan untuk menampung *id_pesan*, *pesan_asli*, *pesan_enkripsi* dan *kunci*.

Dan untuk melengkapi aplikasi perancangan, aplikasi tersebut harus menggunakan Graphical User Interface (GUI). Antarmuka pengguna grafis (GUI), adalah jenis antarmuka pengguna yang memungkinkan pengguna berinteraksi dengan perangkat elektronik melalui ikon grafis dan indikator visual seperti notasi sekunder, alih-alih antarmuka pengguna berbasis teks, label perintah yang diketik atau navigasi teks. GUI digunakan di banyak perangkat genggam seperti pemutar MP3, pemutar media portabel, perangkat game, smartphone dan kontrol rumah tangga, kantor dan industri yang lebih kecil. Desain GUI dalam aplikasi sangat penting karena dengan pengguna GUI dapat dengan mudah mengenali ikon dan cara menggunakannya.

2.3 Algoritma MD5

Algoritma MD5 merupakan sebuah algoritma yang sangat kuat. Algoritma ini tidak mempunyai kunci simetris, karena algoritma ini merupakan algoritma satu arah yang berarti hanya ada proses enkripsi. Supaya pengiriman pesan menjadi aman, maka dipilihlah algoritma MD5. Dalam membangun aplikasi perangkat lunak telepon seluler diperlukan sebuah teknik kriptografi untuk menangani persoalan kerahasiaan pesan, integritas data, keaslian data dan pesan yang tak terbantahkan. Metode yang digunakan adalah algoritma message digest 5 (MD5) menggunakan fungsi hash kriptografi yang banyak digunakan sebagai alat untuk menjamin atau memberi garansi bahwa pesan yang dikirimkan akan sama dengan pesan yang diterima dengan cara membandingkan 'sidik jari' kedua pesan tersebut. MD5 memproses teks masukkan ke dalam blok-blok bit (binary digit) sebanyak 512 bit, kemudian dibagi ke dalam 32 bit sub blok sebanyak 16 blok. Keluaran dari MD5 berupa empat (4) buah blok yang masing-masing 32 bit yang mana semuanya berjumlah 128 bit dan disebut sebagai nilai fungsi hash.

Satu operasi MD5 terdiri dari 64 operasi, dikelompokkan dalam empat putaran dari 16 operasi. F adalah sebuah fungsi nonlinear. Satu fungsi digunakan pada tiap-tiap putaran. M_i menunjukkan blok 32 bit dari masukkan pesan dan K_i menunjukkan konstanta 32 bit yang berbeda untuk tiap-tiap operasi. Berikut adalah model atau desain Algoritma MD5.

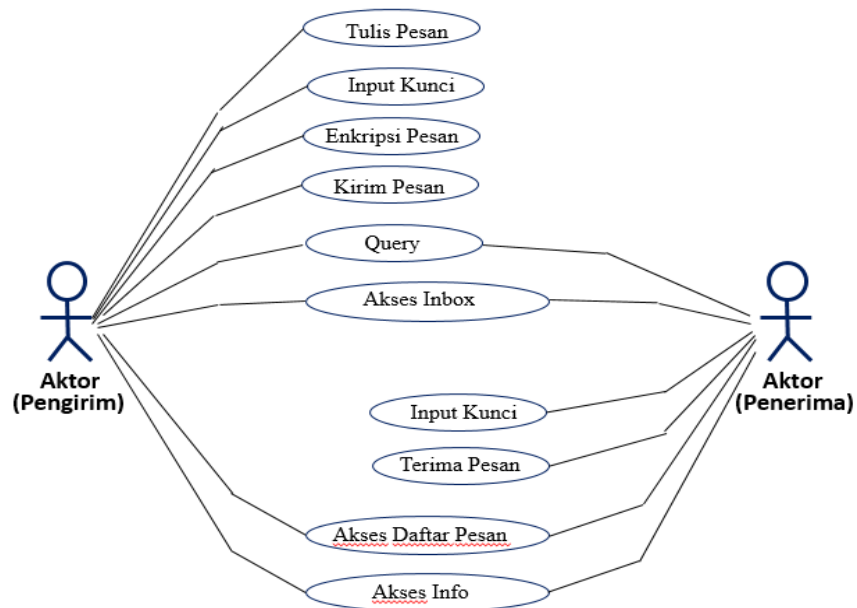


Gambar 3. Desain Algoritma MD5

3. Hasil dan Pembahasan

Untuk membuat sebuah aplikasi yang utuh diperlukan sebuah rancangan yang matang yang mampu membuat aplikasi yang dibangun berjalan ringan dan mulus. Perancangan aplikasi untuk mengirim SMS yang aman berdasarkan Algoritma MD5 tidak seperti rancangan umum untuk mengirim SMS, karena pada rancangan mengirim dan menerima SMS yang aman membutuhkan sebuah kunci yang nantinya digunakan baik oleh pengirim maupun oleh penerima SMS.

3.1 Usecase Diagram



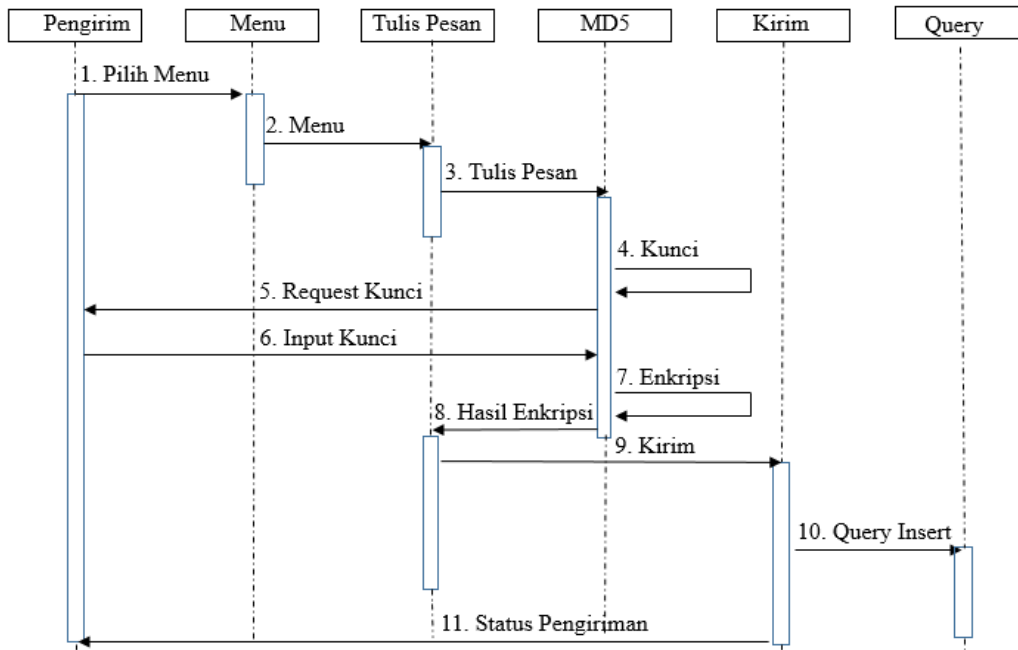
Gambar 4. Usecase Diagram Tulis dan Baca SMS

Pada *usecase* diagram tulis dan baca pesan, aktor (pengirim) dapat melakukan tulis pesan, menginput kunci pesan, mengenkripsi pesan berdasarkan kunci pesan, mengirim pesan dan melakukan metode insert menggunakan query. Sedangkan aktor (penerima) pesan dapat melakukan terima pesan, akses kotak pesan (inbox), menginput kunci dan melakukan metode select menggunakan query. Baik pengirim maupun penerima pesan dapat mengakses info.

3.2 Sequence Diagram Tulis Pesan

Sequence diagram menggambarkan kelakuan objek pada *usecase* dengan mendeskripsikan waktu hidup objek dan pesan yang dikirim dan diterima antar objek. Karena dalam penelitian ini terdapat dua objek utama yaitu, tulis pesan (pengirim pesan) dan baca pesan (penerima pesan), maka objek-objek diagramnya dapat diambil dari objek-objek yang ada pada *usecase* diagram disertai metode-metode yang dimiliki kelas yang diinisiasi menjadi objek.

Berikut adalah *sequence* diagram untuk tulis pesan yang nantinya dienkripsi menggunakan sebuah kunci dan hasil enkripsi akan dikirim ke hosting dan SMSC.

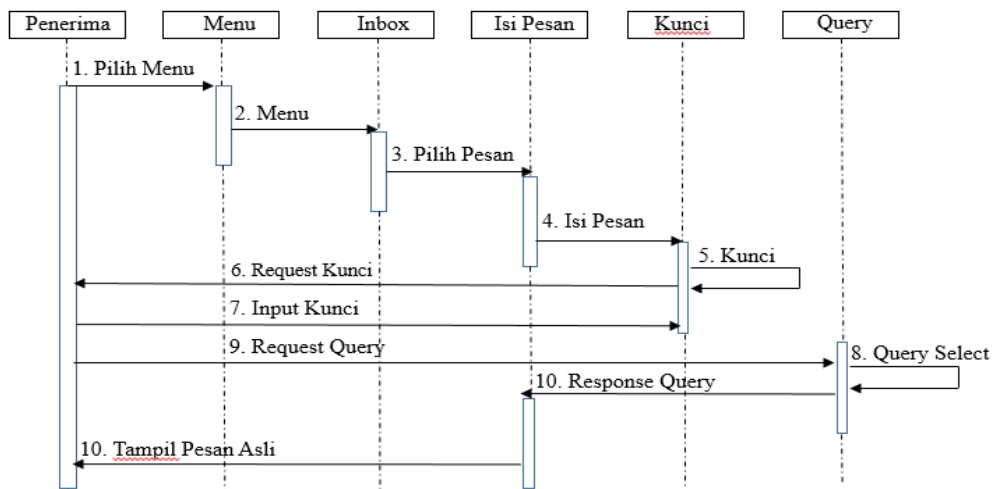


Gambar 5. Sequence Diagram Tulis Pesan

Pada diagram gambar 5 terlihat bahwa pengirim memilih menu Tulis Pesan. Setelah menulis pesan dipilih, kemudian sistem memanggil fungsi tulis pesan dan pesan selesai ditulis. Proses selanjutnya adalah aktor diminta untuk memasukkan kunci enkripsi pada fungsi MD5 dan mengenkripsi pesan yang ditulis berdasarkan kunci. Kemudian pesan selesai dienkripsi, maka hasil enkripsi akan ditampilkan pada fungsi tulis pesan. Setelah selesai, pesan dikirim ke hosting dan SMSC dan pengirim mendapatkan status pengiriman pesan SMS berhasil atau gagal.

3.3 Sequence Diagram Baca Pesan

Pada gambar 6 dapat dilihat *sequence* diagram proses baca SMS yang diterima oleh penerima melalui media SMS berbasis Android Mobile berdasarkan Algoritma MD5.



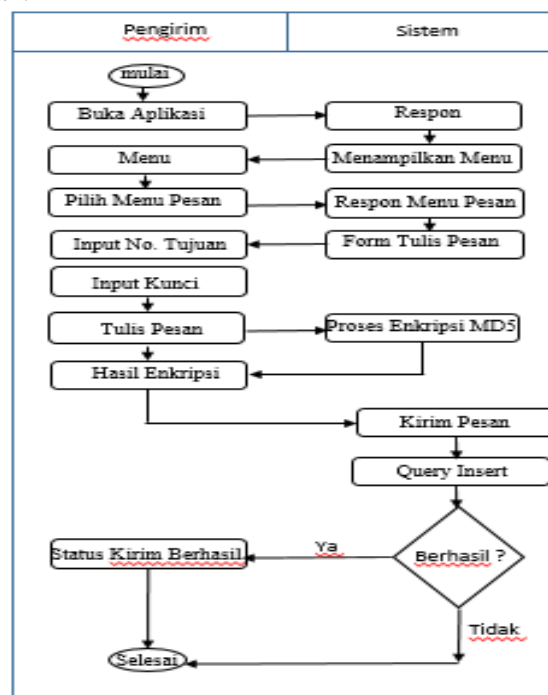
Gambar 6. Sequence Diagram Baca Pesan

Pada gambar 6 dapat dilihat *sequence* diagram proses baca SMS yang diterima oleh penerima melalui media SMS berbasis Android Mobile berdasarkan Algoritma MD5. Awalnya penerima memilih pesan masuk melalui inbox, kemudian penerima melihat isi pesan dalam bentuk pesan yang terenkripsi. Selanjutnya penerima pesan memasukan kunci pesan dan melakukan query select untuk memilih pesan yang ada berdasarkan kunci pesan dan isi pesan terenkripsi. Jika query select berhasil, maka pesan asli bisa ditampilkan.

3.4 Activity Diagram Tulis Pesan dan Baca Pesan

Activity diagram banyak digunakan untuk mendeskripsikan hal-hal yang berhubungan dengan rancangan proses bisnis, urutan atau pengelompokkan tampilan yang diberikan oleh sistem serta rancangan pengujian sebuah sistem.

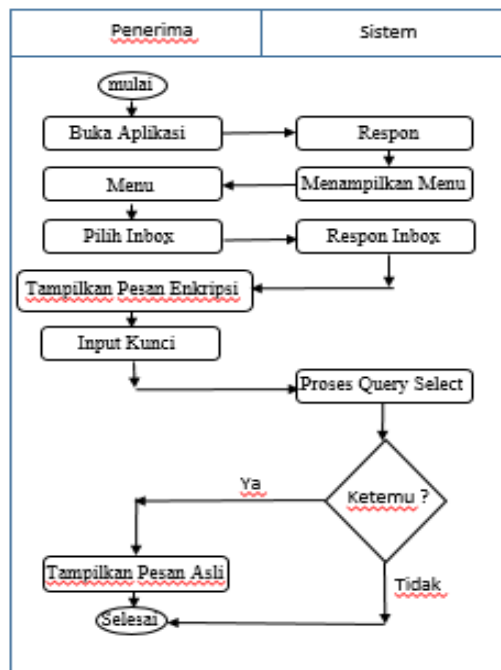
Secara prinsip sistem atau aplikasi ini terdiri dari dua *activity*, yaitu activity diagram tulis pesan dan *activity* diagram baca pesan. Pada gambar 3.4 dapat dilihat proses bisnis *activity* diagram untuk tulis pesan.



Gambar 7. Activity Diagram Tulis Pesan

Activity diagram untuk baca pesan SMS yang diterima oleh penerima merupakan kebalikan dari *activity* diagram tulis pesan. Gambar 8 merupakan *activity* diagram untuk baca pesan SMS.

Saat pesan masuk, pengguna membuka inbox, pengguna hanya bisa melihat pesan dalam bentuk teks yang sudah dienkripsi, kemudian pengguna memasukan sebuah kunci yang sama dengan kunci untuk kirim pesan. Setelah kunci diinput kemudian pengguna menekan tombol dekrip yang seolah-olah pesan didekrip. Sebenarnya pesan diambil dari tabel yang berada di hosting melalui query data manipulation language. Sistem memproses menggunakan Algoritma MD5 dan hasilnya ditampilkan dilayar pengguna, sehingga pengguna dapat membaca isi pesan yang sebenarnya.



Gambar 8. Activity Diagram Baca Pesan

3.5 Class Diagram

Database sangat diperlukan untuk menyimpan data yang dikirim kepada penerima pesan dalam bentuk teks yang sudah dienkripsi melalui SMSC. Saat pesan dikirim, pesan juga terkirim ke hosting dengan metode *query insert()* dengan bantuan sebuah file PHP, sehingga pesan yang ada dalam tabel adalah pesan asli dan pesan hasil enkripsi. Apabila penerima membuka pesan terlihat pesan masih dalam bentuk enkripsi. Kemudian, dengan memasukkan kunci yang sudah disepakati, penerima pesan menekan tombol kunci yang mengirimkan data pesan dan kunci ke hosting dan melakukan metode *query select()* dengan bantuan sebuah file PHP. Jika pesan yang diterima tidak sama dengan hasil query select yang ada di tabel, maka pesan asli tidak bisa ditampilkan dan sebaliknya. Dalam penelitian ini terdapat delapan class, yaitu : class MD5, class Menu, class Inbox, class Tulis_pesan, class Baca_pesan, class About dan class Sms dengan satu class Query sebagai class tambahan.

3.6 Database

Database sangat diperlukan untuk menyimpan data yang dikirim kepada penerima pesan dalam bentuk teks yang sudah dienkripsi melalui SMSC. Saat pesan dikirim, pesan juga terkirim ke hosting dengan *query insert*, sehingga pesan yang ada dalam tabel adalah pesan asli dan pesan hasil enkripsi.

id_pesan	pesan_asli	pesan_enkripsi	kunci
1	Hai, apa kabar?	43bd699ca53d25c87af3295612ad823f	123log

Gambar 10. Contoh isi tabel md5

Isi SMS adalah “Hai, apa kabar” tersimpan bersamaan dengan `id_pesan=1`, `pesan_enkripsi=` 43bd699ca53d25c87af3295612ad823f” dan `kunci=`”coba”. Penerima pesan memasukkan `kunci=`”123log” dan dengan metode `select` serta `kunci=`”123log” dan `pesan_enkripsi =`” 43bd699ca53d25c87af3295612ad823f” penerima pesan dapat menampilkan `pesan_asli=`”Hai, apa kabar?”

3.7 Rancangan Database

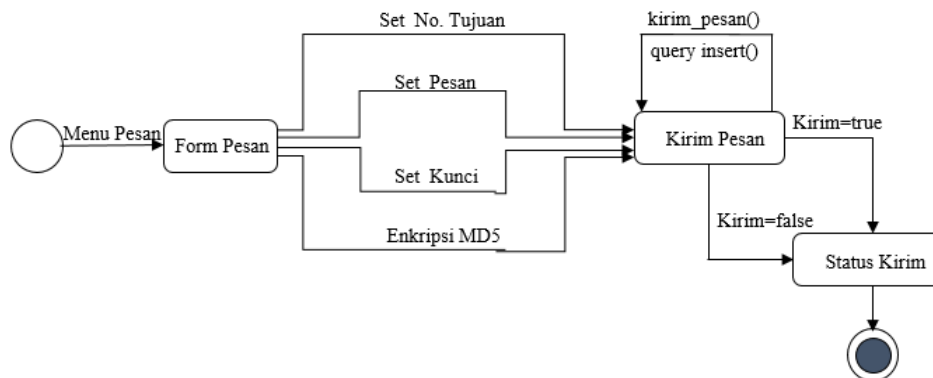
Rancangan database sangat diperlukan untuk mempermudah enkripsi pesan yang dikirim dengan sebuah kunci simetris(sama).

Tabel 1. Rancangan md5

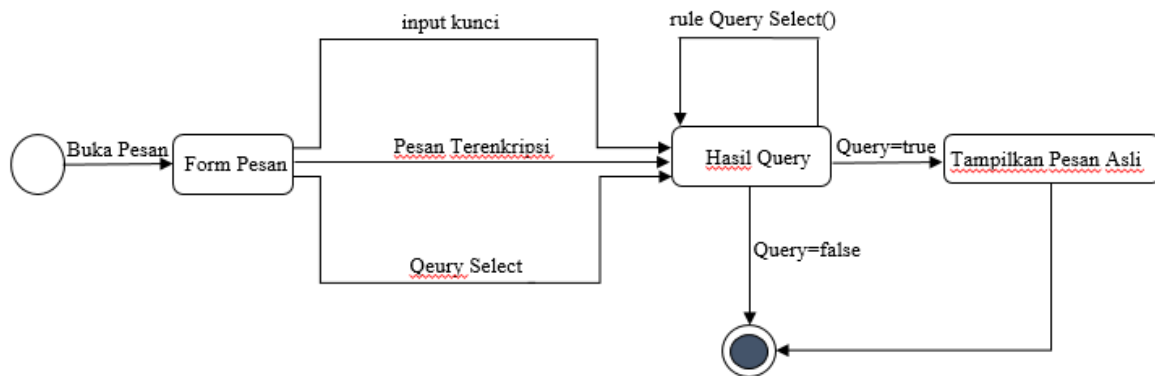
Nama Field	Type	Length	Primary Key	Decription
<code>id_pesan</code>	Int	10	Primary Key	auto_increment
<code>pesan_asli</code>	Text	-	-	Pesan
<code>pesan_enkripsi</code>	Text	-	-	Hasil enkripsi
<code>kunci</code>	Varchar	50	-	Kunci pesan

3.8 State Machine Tulis dan Baca Pesan

Untuk sebuah sistem yang baik diperlukan sebuah *state machine* yang menggambarkan keberadaan sebuah objek. Dalam *state machine* sistem pengiriman pesan yang aman menggunakan Algoritma MD5 ini, menggambarkan daur hidup suatu objek yang terdapat di dalam *state machine*. Karena di dalam pengiriman pesan yang aman ini diperlukan sebuah kunci, maka kunci ini memainkan peranan yang sangat penting di dalam pengiriman pesan. Dari menu pesan, pengirim pesan membuka form untuk mengirim pesan. Kemudian pengirim pesan memasukkan nomor penerima pesan, kunci pesan dan isi pesan. Setelah itu pesan dienkripsi menggunakan algoritma MD5 dan pesan siap dikirim. Mula-mula pesan terkirim ke SMSC dan juga ke hosting dengan metode `query insert` dengan bantuan sebuah file PHP. Selanjutnya status pesan akan tampil.



Gambar 12. State Machine Tulis Pesan



Gambar 13. State Machine Baca Pesan

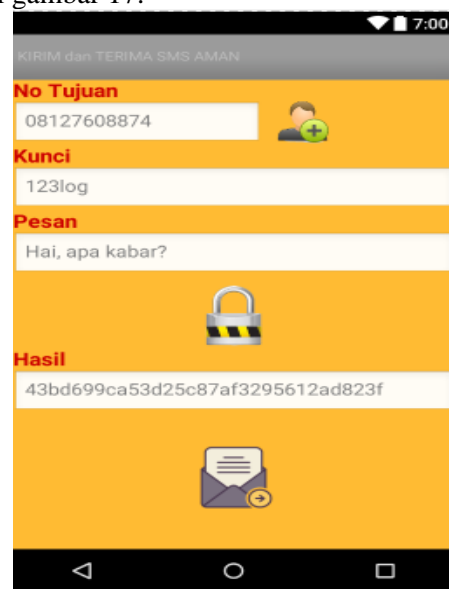
Penerima pesan mula-mula membuka pesan. Kemudian tampil form pesan yang berisikan nomor pengirim, pesan terenkripsi. Pengirim siap untuk memasukan kunci dan melakukan metode query select ke hosting dengan bantuan sebuah file PHP. Hasil query ini ditampilkan jika query berhasil dengan tampilan pesan asli.

3.9 Graphical User Interface

Berikut ini adalah hasil rancangan antar muka yang digunakan untuk mengirim dan menerima SMS aman menggunakan layout pada Android Studio 2.3.3 dan Gradle 3.3. Untuk desain antar muka ini banyak menggunakan layout terutama adalah LinearLayout dan RelativeLayout. Gambar 14 memperlihatkan satu icon Android dan satu buah teks nama aplikasi serta tiga buah tombol, tulis SMS yang ada gambar pensilnya, tombol inbox yang ada gambar panah ke bawah serta tombol info. Jika tombol tulis SMS di sentuh, maka akan tampil gambar 15. Jika tombol inbox disentuh maka akan tampil gambar 17.



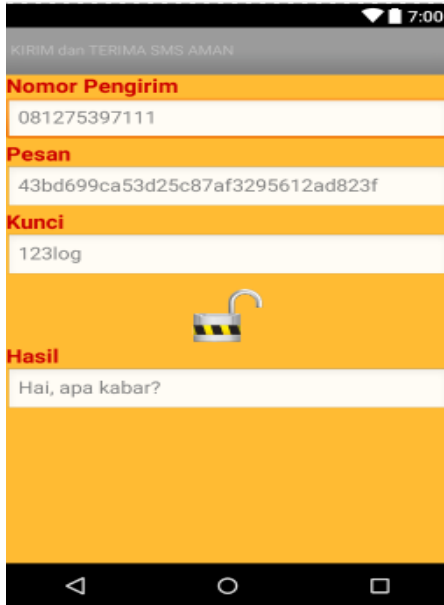
Gambar 14. Tampilan Awal Aplikasi



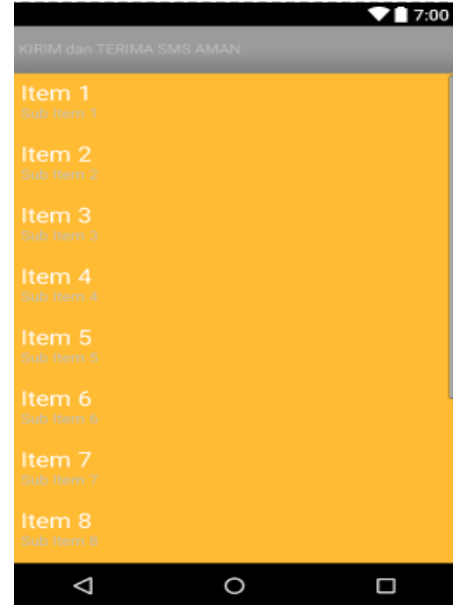
Gambar 15. Tampilan Tulis Pesan

Pada gambar 15 terdapat tiga buah tombol, yaitu tombol untuk mengambil nomor kontak (nomor tujuan) penerima pesan atau dengan menginputkan nomor tujuan. Setelah nomor tujuan terisi, selanjutnya menginputkan kunci pada kotak input kunci dan memuat pesan yang akan

dikirimkan. Tombol kunci berfungsi untuk mengubah pesan dengan algoritma md5, sehingga kotak input hasil berisi pesan yang terenkripsi. Pesan selanjutnya siap dikirimkan ke nomor tujuan melalui SMSC dan ke database yang ada di hosting dengan menyentuh tombol kirim yang bergambar panah ke kanan.



Gambar 16. Tampilan Baca Pesan



Gambar 17. Tampilan Inbox

Pada gambar 16 terdapat empat buah kotak input dengan fungsi masing-masing. Kotak input pertama dari atas adalah kotak nomor pengirim. Kedua adalah kotak pesan yang berisi pesan terenkripsi dengan algoritma MD5. Ketiga adalah kotak input kunci pesan. Apabila penerima membuka pesan terlihat pesan masih dalam bentuk enkripsi. Kemudian, dengan memasukkan kunci yang sudah disepakati dan penerima pesan menekan tombol kunci sehingga data pesan dan kunci dikirim ke hosting dan melakukan metode query select dengan bantuan sebuah file PHP. Jika pesan yang diterima tidak sama dengan hasil query select yang ada di tabel, maka pesan asli tidak bisa ditampilkan dan sebaliknya.

Gambar 17 merupakan daftar pesan yang masuk. Sedangkan gambar 17 berisikan info pembuat aplikasi dan pemberi dana penelitian.



Gambar 18. Tampilan Info

4. Kesimpulan

Rancangan yang dibangun merupakan rancangan berdasarkan model kirim SMS aman. Perancangan yang dibuat menggunakan UML ini merupakan perancangan yang cukup utuh untuk rancangan tulis dan baca SMS aman. Untuk melengkapi rancangan digunakan rancangan *graphical user interface* yang *user friendly* menggunakan Android 2.3.3 dan Gradle 3.3. Rancangan GUI ini sudah diujicoba dengan Compile Sdk Version: Android API 25 : Android 7.1.1 (Nougat) dengan Build Tools Version 26.0.1 dan berjalan dengan mulus tanpa ada kendala. Rancangan aplikasi atau aplikasi ini berjalan pada spesifikasi minimum Android API 15: Android 4.0.3 (Ice Cream Sandwich) dan maksimum Android API 25: Android 7.1.1 (Nougat). Sedangkan rancangan aplikasi seutuhnya belum bisa diterapkan dalam membuat aplikasi Android menggunakan Algoritma MD5, menunggu pendanaan selanjutnya.

Disarankan kepada peneliti untuk perancangan sebuah aplikasi yang diterapkan untuk membangun sebuah aplikasi berbasis Android sebaiknya menggunakan Android Studio dengan versi terbaru yang lebih stabil. Disarankan juga kepada peneliti untuk dapat membuat rancangan dan implementasi suatu aplikasi menggunakan algoritma lainnya. Terima kasih kepada DRPM Ristekdikti yang telah membiayai penelitian ini untuk tahap pertama di tahun 2017. Semoga penelitian ini bisa berlanjut pada tahap kedua di tahun 2018 yaitu implementasi dari desain yang telah dibangun.

Daftar Pustaka

- [1] Safaat, Nazruddin, Aplikasi Berbasis Android, Berbagai Implementasi dan Pengembangan Aplikasi Mobile Berbasis Android, Informatika Bandung 2013
- [2] Rusdianto, Qoshlim dan Akhmad, Implementasi Algoritma MD5 Untuk Keamanan Dokumen, *Jurnal Ilmiah Ilmu Komputer*, Vol. 2, No. 2, September 2016

- [3] Sulianto, Perancangan Aplikasi Untuk Memeriksa Keaslian Data Yang Telah Didownload Menggunakan Algoritma Message Digest 5 (MD5), *Pelita Informatika Budi Darma*, Vol. VIII, Nomor: 3, Desember 2014, halaman 172-177.
 - [4] Kurniawan, Ferlhi, et. al, Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost, *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Juni 2017, Vol. 1 No. 9, halaman 803-812.
 - [5] Apridiansyah, Yovi dan Rifqo, M. Husni, Aplikasi Keamanan Lembar Hasil Studi Menggunakan Algoritma MD5, Studi Kasus : Fakultas Teknik Universitas Muhammadiyah Bengkulu, September 2015, *Jurnal Pseudecode*, Vol. II No. 2, halaman 107-114.
 - [6] Robeth Muzaki, Achmed dan Utama, Ema, *Aplikasi Pengamanan Data dan Informasi Berlapis Dengan Metode Steganografi LSB, Kriptografi Open Sll dan MD5 Berbasis Web*, Seminar Nasional Teknologi Informasi dan Multimedia, STMIK AMIKOM Yogyakarta, 6-8 Februari 2015, halaman 57-62.
 - [7] Marisa, Fitri, Model dan Implementasi Metode enkripsi Kombinasi MD5 dan Skrip Pengolah String Pada Fitur Layanan PBM Online, *Jurnal Pengembangan Manajemen Informatika dan Komputer*, Volume 5, No.2 Juli 2014, halaman 155-162.
 - [8] Rosa dan Salahudin, *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*, Informatika Bandung, 2014.
 - [9] Rumpe, Bernhard, *Modeling with UML, Language, Concepts and Methods*, Springer International Publishing Switzerland 2016.
 - [10] Khairil dan Wira Ginta, Prama, Implementasi Pengamanan Database Menggunakan MD5, *Jurnal Media Infotama*, Vol. 8 No. 1, 2012, halaman 29-44
 - [11] Widodo, Joko Tri Susilo, *Implementasi Algoritma Kriptografi AES 128 Bit Sebagai Pengaman SMS Pada Smartphone Berbasis Android*, Yogyakarta, Sekolah Tinggi Manajemen Informatika Dan Komputer AMIKOM Yogyakarta, 2014
-