REKAYASA PERANGKAT LUNAK KRIPTOGRAFI MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) 128 BIT PADA SISTEM KEAMANAN *SHORT MESSAGE SERVICE* (SMS) BERBASIS ANDROID

Ahmad Arif [1)], Putri Mandarani[2)]
Mahasiswa Tenik Informatika[1]
Dosen Teknik Informatika[2]
Fakultas Teknologi Industri Institut Teknologi Padang

INTISARI

Layanan pesan singkat (SMS) merupakan salah satu media komunikasi pertukaran pesan yang populer digunakan, meskipun banyak aplikasi pertukaran pesan berbasis internet yang cenderung lebih hemat dan mudah, akan tetapi masih terhalang oleh jaringan tidak stabil. Android adalah sistem operasi dengan perkembangan yang paling maju saat ini, jumlah perangkat yang menawarkan sistem operasi ini meningkat tajam karena bertambahnya jumlah pengguna, kemudahan teknologi komunikasi disertai dengan keamanan yang meningkat, terutama keamanan dalam pertukaran informasi, salah satu cara untuk saling tukar informasi yang paling mudah dan yang paling populer adalah melalui layanan pesan singkat (SMS). Secara umum, sms di telepon genggam, android khususnya, rentan terhadap risiko pencurian informasi, karena sering pesan yang dikirimkan adalah pesan yang bersifat pribadi dan rahasia. Maka, dapat disimpulkan bahwa diperlukan sistem kriptografi yang diterapkan di android, guna mengamankan sms yang dikirim kepada penerima, tanpa rasa takut informasi akan bocor. Algoritma Edvanced Encryption Standard (AES) berjalan selama pengiriman pesan di android dapat menjadi satu jalan keluar untuk menyelesaikan masalah di atas , aplikasi ini memiliki tampilan yang sederhana dan menarik , karena itu aplikasi yang mudah digunakan dan tempat yang kokoh dalam solusi pertukaran informasi melalui sms.

Kata Kunci: SMS, Enkripsi, Dekripsi, Android, AES

ABSTRACT

Short message service (SMS) is one of the popularly used message exchange communication medias although many internet based message exchange application tend to be more thrifty and easy but still obstructed by unstable networks. Android is now the operating system with the most advanced developments, the number of devices that offer this operating system increasing rapidly due to the growing number of users, followed by ease of communication technology should be accompanied by increased security, especially security in the exchange of information, one of the easiest and most popular way to exchange information is through short message services (SMS). In general, SMS on mobile phones, especially Android, are particularly vulnerable to the risk of information theft, interception, and even the loss of important information, because frequently sent messages are personal and confidential. So, it can be concluded that it is necessary a cryptographic application in Android that important and confidential SMS delivery is expected can be safely delivered to the recipient, without fear of information leakage. Advanced encryption standard (AES) algorithm implementation for message delivery in Android could be one solution to the problem above, this application has a simple and attractive appearance, so the application is user friendly and can be a secure solution in exchange of information through SMS.

Keywords: SMS, Encryption, Decryption, Android, AES

1. Pendahuluan

Penggunaan teknologi telepon genggam (*handphone*) sebagai alat telekomunikasi pada saat ini telah mengubah cara pandang masyarakat dalam berkomunikasi. Telepon genggam mempunyai beberapa fungsi komunikasi yang dapat digunakan antara lain, *video Call*, SMS, MMS, *Chatting*, *Internet*, dan lain-lain. Berkembangnya teknologi telepon genggam dapat dilihat dengan munculnya berbagai sistem operasi yang lengkap layaknya komputer, diantaranya adalah Android. Android adalah sebuah sistem operasi untuk perangkat telepon yang berbasis linux yang mencakup sistem operasi, *middleware*, aplikasi dan menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka.

Meskipun Android memiliki fitur yang lengkap, namun layanan SMS (Short Message

Service) sebagai layanan pertukaran informasi atau pesan pendek menjadi komunikasi favorit karena saat ini semua telepon genggam memiliki layanan ini dan yang paling penting adalah biaya SMS relatif murah. Dari fasilitas pengiriman pesan yang didapatkan, pengguna sering mengabaikan tentang keamanan pesan dari pihak ketiga. Dan salah satunya yang harus benar-benar dijaga keamanan dan kerahasiaannya adalah pesan yang bersifat rahasia, pribadi ataupun pesan kenegaraan karena jika pesan itu diketahui oleh pihak ketiga dan tersebar luas maka akan mengancam keamanan pengirim, penerima ataupun persatuan dan kesatuan negara.

Ada berbagai macam pengamanan pesan, salah satunya dengan kriptografi. Kriptografi adalah proses untuk mengamankan informasi dengan menggunakan teknik penyandian. Proses penyandian informasi asli (*plaintext*) yang menghasilkan informasi yang tersandikan (*ciphertext*) disebut enkripsi, sedangkan proses menguraikan ciphertext menjadi informasi asli disebut dekripsi. Saat ini telah banyak metode kriptografi yang muncul, salah satunya adalah algoritma AES (*Advanced Encryption Standard*). Algoritma AES merupakan blok kode simetris untuk menggantikan Algoritma DES (Data Encryption Standard). AES mendukung berbagai variasi ukuran blok dan kunci yang tetap sebesar 128, 192 dan 256 bit, Pemilihan blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi.

Dari latar belakang tersebut maka penulis tertarik untuk membuat sebuah penelitian mengenai perancangan dengan mengaplikasian algoritma kriptogafi AES 128 bit pada suatu sistem keamanan pesan, penulispun mencoba membuat sebuah aplikasi yang dapat membantu menangani masalah tersebut dengan judul penelitian **"REKAYASA PERANGKAT LUNAK KRIPTOGRAFI MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) 128 BIT PADA SISTEM KEAMANAN SHORT MESSAGE SERVICE (SMS) BERBASIS ANDROID".**

2. Metodologi Penelitian

Penelitian ini merupakan penelitian eksperimen dengan merancang sebuah aplikasi perangkat lunak dan mengimplementasikan algoritma AES untuk proses enkripsi dan dekripsi *Short Massage Service* (SMS). Dari hasil perancangan sistem ini, penulis berharap agar dapat diimplementasikan dan bermanfaat bagi penggunan *mobile* untuk keperluan keamanan pesan berupa teks.

2.1. Short Message Service (SMS)

SMS adalah suatu fasilitas untuk mengirim dan menerima suatu pesan singkat berupa teks melalui perangkat nirkabel, yaitu perangkat komunikasi telepon selular, dalam hal ini perangkat nirkabel yang digunakan adalah telepon selular. Salah satu kelebihan dari SMS adalah biaya yang murah.

SMS pertama kali muncul di belahan Eropa pada tahun 1991 bersama sebuah teknologi komunikasi wireless yang saat ini cukup banyak penggunanya, yaitu *Global Sistem for Mobile Communication* (GSM). Dipercaya bahwa pesan pertama yang dikirim menggunakan SMS dialakukan pada bulan Desember 1992, dikirim dari sebuah *Personal Computer* (PC) ke telepon *mobile* dalam jaringan GSM milik *Vodafone* Inggris. Perkembagan kemudian merambah ke benua Amerika, dipelopori oleh beberapa operator komunikasi bergerak berbasis digital seperti *Bell Sputh Mobility, PrimeCo, Nextel*, dan beberapa operator lain. Teknologi digital yang digunakan sangat bervariasi dari yang berbasis GSM, *Time Division Multiple Access* (TDMA), hingga *Code Division Multiple Access* (CDMA).

2.2. Kriptografi

Salah satu cara yang dapat dilakukan untuk dapat mengamankan sistem informasi adalah kriptografi. Kata kriptografi berasal dari bahasa Yunani, yaitu Kryptos (tersembunyi, rahasia) dan Graphein (tulisan). Jadi kriptografi didefenisikan sebagai ilmu seni untuk menjaga kerahasiaan pesan dengan cara menyandikan kebentuk yang tidak dapat dimengerti (*Random*). Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi (*encrypt*) maupun dekripsi (*decrypt*) pesan. Teknik ini digunakan untuk mengubah pesan kedalam kode-kode tertentu sehingga informasi yang disimpan atau ditransmisikan melalui jaringan yang tidak aman (misalnya saja internet) tidak dapat dibaca oleh pihak manapun kecuali orang-orang yang berhak. Algoritma dari enkripsi adalah fungsi-fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika. Berdasarkan cara memproses teks (*plaintext*), *cipher* dapat dikategorikan menjadi dua jenis:

blok cipher dan stream cipher. Blok *cipher* bekerja dengan memproses data secara blok, dimana beberapa karakter / data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. Sementara itu stream cipher bekerja memproses masukan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan.

Kriptografi bertujuan untuk memberi layanan keamanan yang juga dinamakan sebagai aspek-aspek keamanan, yaitu sebagai berikut :

a. Kerahasiaan (*confidentiality*)
b. Keutuhan (*integrity*)
c. Jaminan atas identitas dan keabsahan (*authenticaticity*)
d. Nirpenyangkalan (*non-repuditation*)

2.3. Algoritma AES

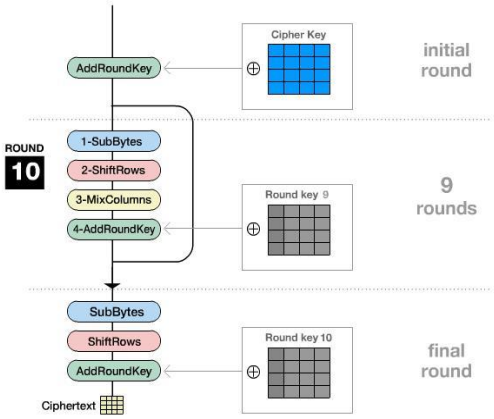
AES atau *Advanced Encryption Standard* merupakan standar enkripsi kunci simetri yang pada awalnya diterbitkan dengan algoritma Rijndael. Algoritma ini dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. *Advanced Encryption Standard* (AES) dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001. AES merupakan blok kode simetris untuk menggantikan DES (*Data Encryption Standard*). Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe : AES-128, AES-192, dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap putaran.

Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

a. Addroundkey
b. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: SubBytes , ShiftRows , MixColumns , dan AddRoundKey .
c. Final Round , adalah proses putaran untuk putaran terakhir yang meliputi SubBytes , ShiftRows , MixColumns , dan AddRoundKey .

Sedangkan pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

a. AddRoundKey
b. Putaran sebanyak a-1 kali, dimana pada setiap putaran dilakukan proses: InverseShiftRows, InverseSubBytes, AddRoundKey, dan InverseMixColumns.
c. Final Round adalah proses untuk putaran terakhir yang meliputi InverseShiftRows , InverseSubBytes , dan AddRoundKey .

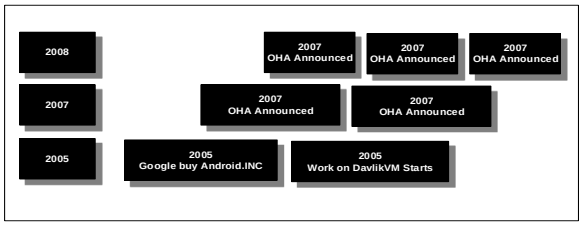


Gambar 1. Skema Kerja AES-128

2.4. Android

Android adalah sebuah sistem operasi untuk perangkat mobile berbasis linux yang mencakup sistem operasi, middleware dan aplikasi. Aplikasi Android yang dikembangkan menggunakan Java dan mudah menyesuaikan ke platform baru . Android terdiri dari satu tumpukan yang lengkap, mulai dari boot loader, device driver, dan fungsi-fungsi pustaka, hingga perangkat lunak API (*Application Programming Interface*), termasuk aplikasi SDK (*Software Development Kit*). Android bukanlah satu perangkat tertentu, melainkan sebuah platform yang dapat digunakan dan diadaptasikan untuk mendukung berbagai konfigurasi perangkat keras. Sistem operasi yang mendasari Android merupakan lisensi di bawah naungan GNU, General Public License Versi 2(GPLv2), yang biasa dikenal dengan istilah Copyleft. Istilah *copyleft* ini merupakan lisensi yang setiap perbaikan oleh pihak ketiga harus terus jatuh di bawah terms.Distribusi Android berada di bawah lisensi Apache Software (ASL/Apache2), yang memungkin untuk distribusi kedua atau seterusnya. Pengembang aplikasi Android diperbolehkan untuk mendistribusikan aplikasi mereka di bawah skema lisensi apapun yang mereka inginkan. Aplikasi Android dapat dikembangkan pada berbagai sistem operasi, diantaranya adalah:

a. Windows XP/Vista/7
b. Mac OS X (Mac OS X 10.48 atau yang lebih baru)
c. Linux



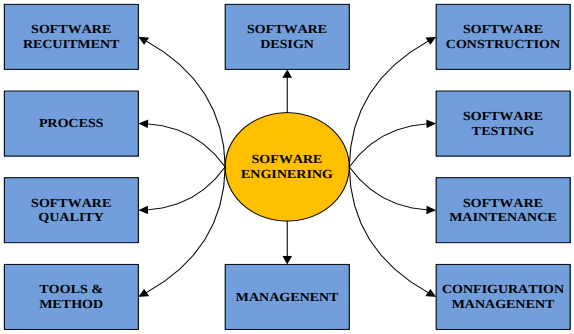
Gambar 2. Pengembangan platform android

2.5. Teori Rekayasa Perangkat Lunak

Istilah Rekayasa Perangkat Lunak (RPL) secara umum disepakati sebagai terjemahan dari istilah *Software engineering*. Istilah *Software Engineering* mulai dipopulerkan pada tahun 1968 pada *software engineering Conference* yang diselenggarakan oleh NATO. Sebagian orang mengartikan RPL hanya sebatas pada bagaimana membuat program komputer. Padahal ada perbedaan yang mendasar antara perangkat lunak (*software*) dan program komputer.

Perangkat lunak adalah seluruh perintah yang digunakan untuk memproses informasi. Perangkat lunak dapat berupa program atau prosedur. Program adalah kumpulan perintah yang dimengerti oleh komputer sedangkan prosedur adalah perintah yang dibutuhkan oleh pengguna dalam memproses informasi (O'Brien, 1999).

Pengertian RPL sendiri adalah suatu disiplin ilmu yang membahas semua aspek produksi perangkat lunak, mulai dari tahap awal yaitu analisa kebutuhan pengguna, menentukan spesifikasi dari kebutuhan pengguna, Desain, pengkodean, pengujian sampai pemeliharaan sistem setelah digunakan. Dari pengertian ini jelaslah bahwa RPL tidak hanya berhubungan dengan cara pembuatan program komputer. Pernyataan "semua aspek produksi" pada pengertian di atas, mempunyai arti semnua hal yang berhubungan dengan proses produksi seperti manajemen proyek, penentuan personil, anggaran biaya, metode, jadwal, kualitas sampai dengan pelatihan pengguna merupakan bagian dari RPL.



Gambar 3. Ruang lingkup RPL

2.6. Waktu dan Lokasi Penelitian

Penelitian ini dilakukan mulai Juni 2015 sampai dengan Oktober 2015 di kampus Institut Teknologi Padang.

2.7. Alat dan Bahan

Alat dan bahan yang digunakan dalam merancang aplikasi kriptografi menggunakan algoritma AES berbasis Android ini adalah sebagai berikut :

1. Perangkat Keras (*Hardware*)
   a. Processor AMD A8-6410 APU with AMD Radeon R5 Graphics (4 CPUs), ~2.0GHz
   b. Memory 4096MB RAM
   c. 500GB (SATA) HDD
   d. Monitor Generic Pnp Monitor 4073MB display 1366 x 768 32bit 60Hz

2. Perangkat Lunak (*Software*)
   a. Sistem Operasi Windows 8.1 Pro 64bit
   b. Open JDK Java8 Runtime
   c. Editor : Android Studio
   d. Emulator : Genymotion
   e. Gimp : Pengolah Citra Pembuatan *Image*

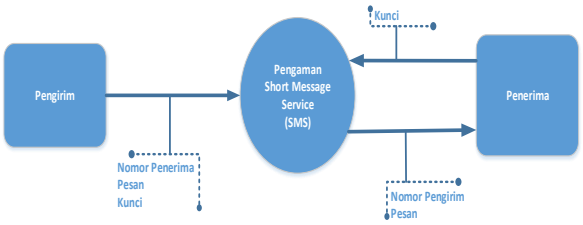
Selain perangkat di atas, pada pengujian aplikasi yang dibangun juga menggunakan dua perangkat mobile yang berbeda untuk mendapatkan hasil analisa dari aplikasi yang dibangun, diantaranya :

1. Perangkat 1
   Spesifikasi *Hardware* dan Sistem Operasi
   a. Processor Dual-core 1 GHz Cortex-A7
   b. Memory 1024 MB RAM
   c. Internal 4 GB
   d. Sistem Operasi Android v4.4.2 (KitKat)

2. Perangkat 2
   a. Processor Qualcomm MSM7225A, 1 MHz Cortex-A5
   b. Memory 512 MB RAM
   c. Internal 3 GB
   d. Sistem Operasi Android v2.3 (Gingerbread)

2.8. *Context* Diagram

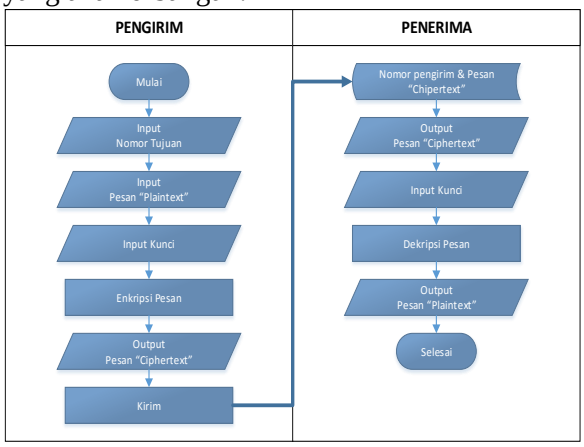
Context diagram digunakan sebagai alat bantu dalam merancang sistem secara global dengan memperlihatkan sistem secara umum. Berikut context diagram penelitian untuk aplikasi kriptografi algoritma AES berbasis Android:



Gambar 4. Context Diagram

2.9. Tahapam Merancang Antar Muka Sistem

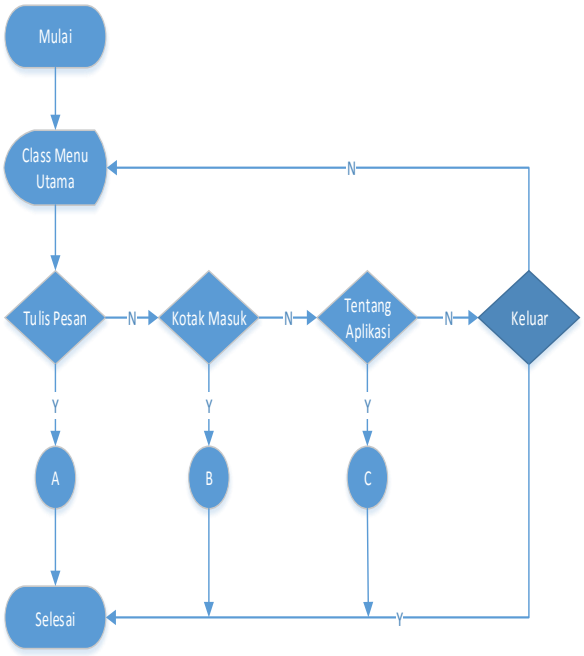
Perancangan antarmuka berisi pemaparan user interface yang digunakan dalam perancangan aplikasi. Dengan perancangan antar muka ini diharapkan dapat memudahkan pengguna dalam mengoperasikan aplikasi. Gambar 5 berikut rancangan *flowchart* program yang akan dibangun.



Gambar 5. *Flowchart* Sistem

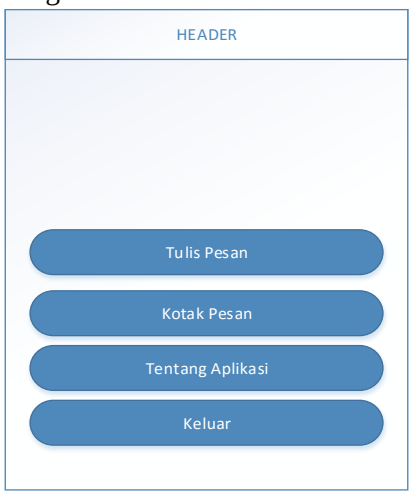
2.10. Tampilan Antar Muka Utama

Rancangan tampilan program aplikasi yang akan dibangun terdiri dari beberapa content yang dirancang seinteraktif mungkin sehingga memungkinkan pengguna dapat mengoperasikan aplikasi secara optimal. Berikut *flowchart* menu utama program yang akan dibangun:



Gambar 6. *Flowchart* Menu Utama Program

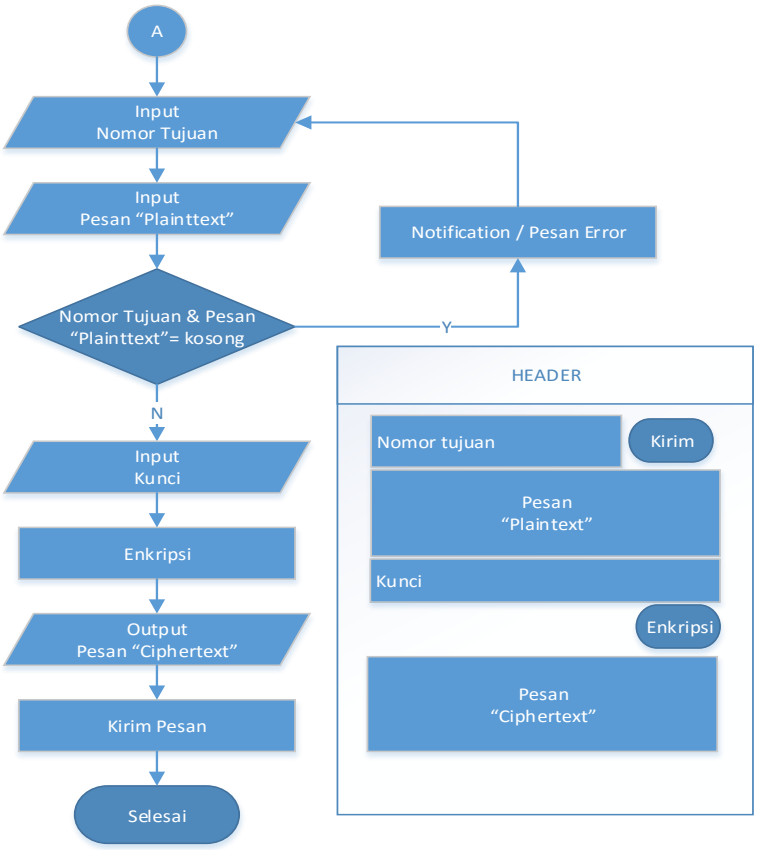
Dari rancangan *flowchart* diatas, penulis menvisualisasikannya dalam bentuk rancangan tampilan antar muka aplikasi, berikut rancangan tampilan aplikasi program kriptografi AES yang akan dibangun :



Gambar 7. Tampilan Menu Utama

2.11. Tampilan *Class* Tulis Pesan

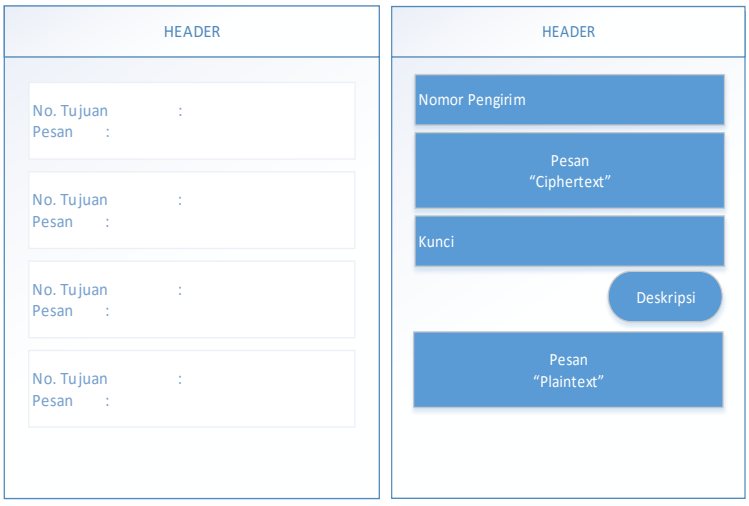
Class tulis pesan merupakan class yang digunakan untuk melakukan proses pembuatan pesan singkat atau SMS yang akan dienkripsi, pada class ini disediakan *interface* nomor tujuan, pesan, kunci, enkripsi, kirim serta hasil dari pesan yang dienkripsi. Berikut *flowchart* dan rancangan visualnya dari proses pembuatan pesan yang akan dienkripsi sebagai berikut:



Gambar 8. Flowchart dan Rancangan Pada Class Tulis Pesan

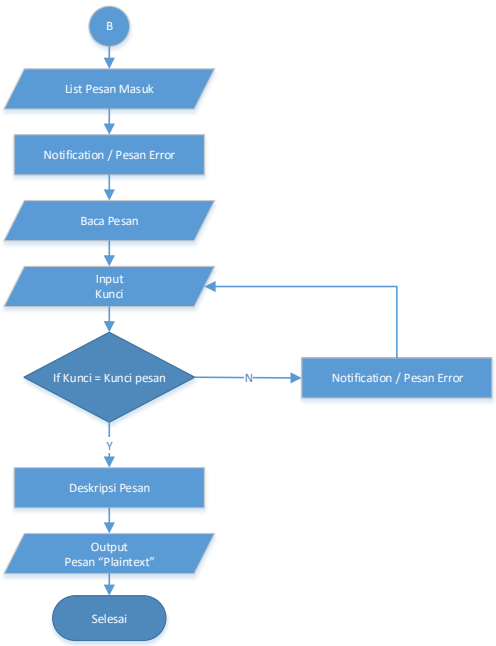
2.12. Tampilan *Class* Kotak Masuk

Tampilan ini mempunyai fungsi menampilkan list pesan yang diterima, dimana nantinya akan digunakan untuk melakukan proses dekripsi pesan. Adapun rancangan desain dari *class* kotak masuk seperti berikut:



Gambar 9. *List* Pesan Masuk dan Tampilan Baca Pesan

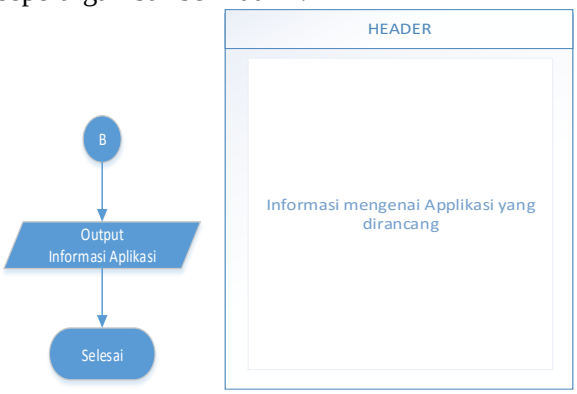
Setelah tampilan dari list pesan masuk kemudian akan ditambahkan juga tampilan baca pesan pada class menu kotak masuk, dimana proses ini hanya akan berjalan jika pengguna memilih dan membuka pesan yang akan dibaca pada tampilan class list pesan. Dari rancangan kedua tampilan pada class menu kotak masuk diatas, dapat dirancang *flowchart* proses yang terjadi pada class kotak masuk seperti berikut:



Gambar 10. *Flowchart class* kotak masuk

2.13. Tampilan Class Tentang Aplikasi

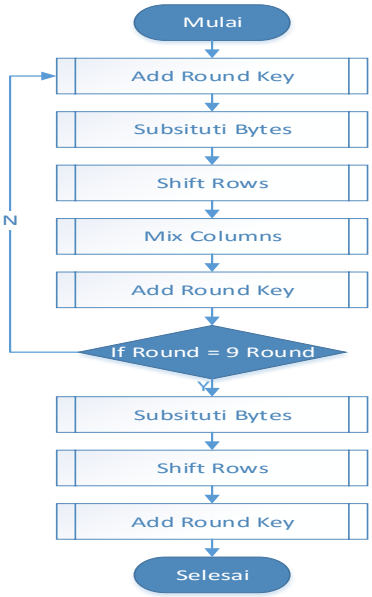
Class ini memiliki fungsi yang sangat sederhana yaitu menampilkan deskripsi atau informasi tentang aplikasi yang dirancang. Adapun rancangan visualnya dan flowchartnya seperti gambar berikut ini:



Gambar 11. Tampilan class tentang aplikasi

2.14. Proses Kriptografi AES

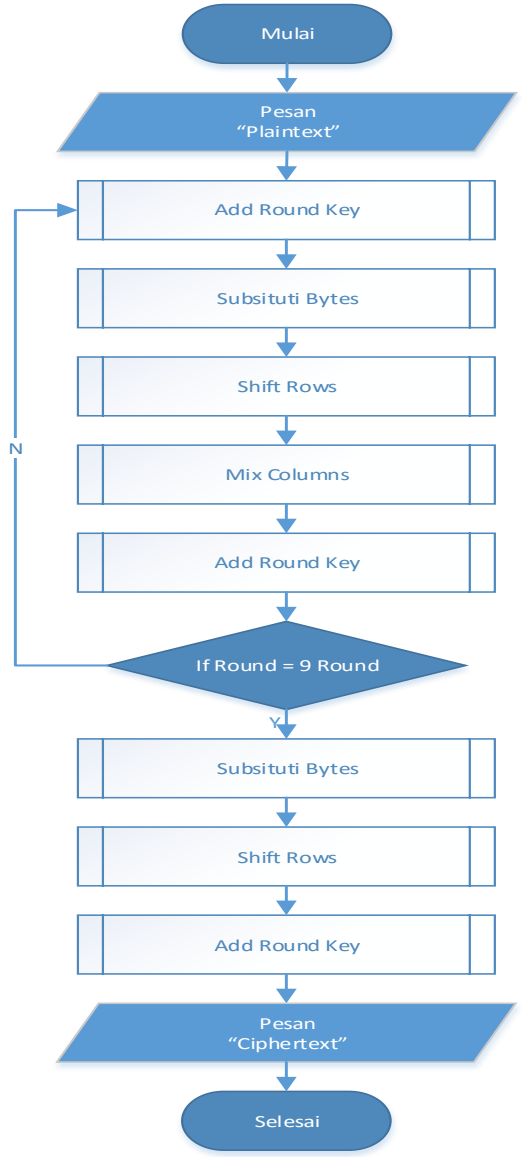
Pada proses kriptografi dengan mengunakan AES sebagai algoritmanya, ada beberapa tahapan yang harus dilalui pengirim sebelum mendapatkan hasil pesan yang telah disandikan, berikut *flowchart* dari proses yang terjadi:



Gambar 12. *Flowchart* AES

2.15. Proses Enkripsi

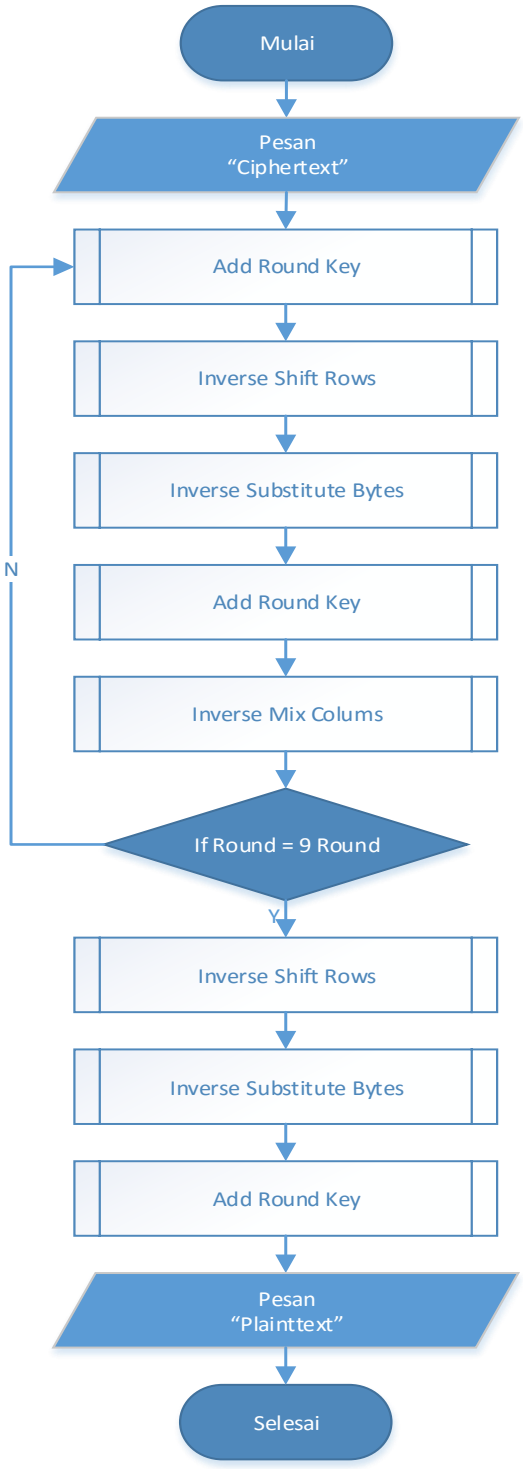
Pada proses enkripsi ada beberapa tahapan yang harus dilalui pengirim sebelum mendapatkan hasil pesan yang telah dienkripsi. Berikut *flowchart* untuk melakukan proses enkripsi:



Gambar 13. *Flowchart* proses enkripsi pesan

2.16. Proses Dekripsi

Pada proses dekripsi ada beberapa tahapan yang harus dilalui penerima sebelum mendapatkan hasil pesan yang telah didekripsi, berikut *flowchart* yang harus dilalui:



Gambar 14. *Flowchart* proses dekripsi

3. Pembahasan

3.1. Percobaan Aplikasi Mengamankan Pesan

Sistem keamanan pesan dengan algoritma *Advanced Encryption Standard* (AES) pada tugas akhir ini merupakan salah satu perkembangan implementasi kriptografi dalam bidang telekomunikasi. Manfaat kriptografi telah

banyak digunakan dalam teknologi informasi, dari beberapa sumber artikel yang penulis ketahui, salah satu aplikasi yang memanfaatkan kriptografi sebagai metode keamanan dalam pertukaran informasi adalah Skype, dalam artikel tersebut disebutkan bahwa Skype menggunakan algoritma RC5 sebagai metode keamanan pesan.

Gambar 15. Halaman Utama Aplikasi

Penggunaan karakter dalam aplikasi ini terbatas dengan jankauan nilai ASCII (hex) karna pada impementasinya, algoritma ini mengunakan konversi bilangan ke heksadesimal. Pesan dan kunci yang dikonversikan ke heksadesimal selanjutnya akan memalui proses secara bertahap seperti pada teori-nya. Untuk lebih jelas penulis akan melakukan beberapa percobaan untuk membuktikan kinerja dari aplikasi yang telah dibuat. Berikut adalah langkah-langkah percobaan yang dilakukan.

3.2. Kirim Pesan

Sebelum mengirimkan pesan tersandi atau terenkripsi, terlebih dahulu pengirim pesan untuk memasukkan nomor tujuan, pesan yang akan disandikan dan kunci. Untuk lebih jelasnya lihat pada Gambar 16.

Gambar 16. Halaman kirim pesan

Penulis akan melakukan percobaan fungsi kirim pesan ke nomor tujuan '082388966670' dengan isi pesan 'Ahmad Arif – Teknik Informatika' yang kemudian pesan akan dienkripsi dengan kunci '2011610178', selanjutnya meng-klik / tab tombol enkripsi untuk dapat menghasilkan pesan yang tersandikan. Setelah mendapatkan pesan yang tersadikan, tahap selanjutnya adalah mengirim pesan yang tersandikan dengan cara meng-klik atau tab tombol kirim, Seperti Gambar 17.

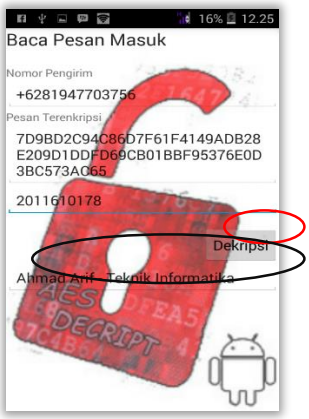
Gambar 17. Percobaan kirim pesan

3.3. Baca Pesan

Ada beberapa persyaratan yang harus dipenuhi oleh penerima pesan untuk dapat membaca pesan yang tersandikan antara lain adalah pesan yang akan didekripsi atau diterjemahkan adalah pesan yang telah disandikan dan dikirim oleh pengirim dengan bantuan aplikasi ini tentunya. Kemudian syarat yang juga harus dipenuhi ialah kunci untuk membuka pesan yang tersandikan, dengan meminta kunci kepada pengirim pesan melalui media komunikasi yang lain. Untuk lebih jelasnya dapat dilihat Gambar 18.

Gambar 18. *List* Pesan Masuk

Pada Gambar 18 penulis akan melakukan percobaan fungsi baca pesan dengan nomor pengirim '+6281947703756' dengan isi pesan yang tidak dapat dibaca atau tersandikan, selanjutnya meng-klik / tab pesan yang akan dibaca pada halaman list pesan masuk yang selanjutnya aplikasi akan membuka halaman baca pesan, seperti Gambar 19. Untuk dapat menghasilkan pesan yang dapat dimengerti langkah pertama dengan memasukkan kunci yang sama dengan kunci yang digunakan oleh pengirim pesan untuk membuat pesan yang disandikan. Selanjutnya dengan meng-klik / tab tombol dekripsi untuk menghasilkan pesan yang dapat dimengerti oleh penerima pesan.



Gambar 19. Baca pesan

4. Penutup

4.1. Kesimpulan

Berdasarkan hasil dan pembahasan dapat ditarik kesimpulan sebagai berikut :

a. Algoritma AES 128 dapat diimplementasikan pada telepon seluler berbasis Android, sebagai sistem keamanan pesan.
b. Aplikasi yang dibuat oleh penulis mampu melakukan dekripsi dengan baik untuk semua bentuk karakter ASCII.
c. Aplikasi dapat melakukan dekripsi terhadap pesan terenkripsi dengan memasukan kunci yang sama dengan kunci yang digunakan pada saat proses enkripsi.

4.2. Saran

Saran yang dapat disampaikan penulis yang bertujuan membantu pengembangan aplikasi ini adalah :

a. Menyempurnakan aplikasi ini agar dapat beroperasi dengan baik pada sistem android pada versi yang lebih tinggi.
b. Menambahkan fitur scrollview dan antar muka percakapan pada aplikasi agar dapat memudahkan pengguna aplikasi dalam melakukan penulisan, pengiriman atau membaca pesan.
c. Tampilan aplikasi masih monoton sehingga masih perlu banyak tambahan.

DAFTAR PUSTAKA

Ariyana, Yoki (2011). Advanced Encryption Standard (AES). Bandung Penerbit : PPPPTK IPA Bandung

Ariyus, Dony (2008). Pengantar Ilmu Kriptografi: Teori, Analisa, dan Implementasi. Yogyakarta. Penerbit : Andi Offset

Enterprise. Jubilee (2013). Memahami pemrograman android secara cepat dan mudah. Jakarta. Penerbit : Elex Media Komputindo

Irawan, Arif Fajar (2013). Sistem Keamanan Pesan Pada Android Gingerbread (2.3.4) Dengan Algoritma LUC. Penerbit : Universitas Jember

Putra, Novernus Ayundha (2014). Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma RSA Pada Sistem Keamanan File Berbasis Java. Penerbit : Institut Teknologi Padang

Suarga (2009). Dasar Pemrograman Komputer Dalam Bahasa Java. Makasar. Penerbit : Andi Offset