PERANCANGAN APLIKASI SMS (*SHORT MESSAGE SERVICE*) DENGAN ENKRIPSI TEKS MENGGUNAKAN ALGORITMA *BLOCK CIPHER* AES (*ADVANCED ENCRYPTION STANDARD*) BERBASIS *MOBILE* PADA *PLATFORM* ANDROID

Irwan

Program Studi Teknik Informatika
Fakultas Teknik Universitas Tanjungpura
silveriusirwan@gmail.com

Abstract - **In recent several years, there was a rapid development in mobile phone technology. One is the development of smart phone with many features and also complex operating system that similar to a computer. Although smart phones have many features that included in the operating system, but long or short messaging service known as SMS is still popular in use. SMS feature that still exist till today, bring out the question about the safety of information if someone wants to send a confidential information via SMS facility. The ease of exchanging information via SMS is misused by some people. Some people with a variety of ways to try to steal information that's illegal. Therefore, we need a way to secure the information that is confidential and important. Encryption process can be used to improve the SMS text message levels of information security. Currently, AES (Advanced Encryption Standard) is used as a standard for cryptographic algorithms. Therefore, it can be developed an SMS application with a text encryption using AES algorithm. Mobile-based applications built on the Android platform. The test results showed that the application can perform encryption of short messages with text to a particular destination number and can not decrypt the encrypted message. Application can help users to send short messages in a secure, fast, and easy.**

Keywords - SMS, encryption, decryption, AES, Android.

I. Pendahuluan

SMS (*Short Message Service*) mulai dikembangkan pada tahun 1991, dan sekarang SMS ini telah diterima secara global sebagai *wireless service* yang memungkinkan transmisi atau pengiriman pesan *alphanumeric* (teks) antar telepon selular. Meskipun SMS dibatasi hanya sampai 160 karakter saja, SMS ini adalah metode komunikasi *non-voice* yang tidak mahal.

Namun dengan fitur SMS yang telah ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Permasalahan keamanan data muncul disini mengingat beberapa fasilitas transaksi dilakukan menggunakan media ini. SMS pada awalnya dirancang untuk komunikasi tidak sinkron dimana konten yang dikirimkan adalah *plain text*. Bagaimanapun data *plain text* seperti ini dapat dicegat di jalan oleh siapa saja yang memiliki akses ke sistem SMS. Server SMS milik operator merupakan salah satu pihak yang dapat mengambil data ini, walaupun dalam setiap perjanjian terdapat klausul tentang kerahasiaan data, akan tetapi data *plain text* yang terkirim dan berkasnya tersimpan di berbagai tempat baik di server milik operator maupun milik *content provider* membawa satu potensi bahaya yang besar. Kelemahan itu dikarenakan SMS menggunakan standar pengkodingan yang universal, SMS dibangun dengan sistem bahasa program yang sejenis dengan bahasa program hardware seperti komputer dan telepon selular dapat menerjemahkan semua data dalam frekuensi tertentu yang terbuka (di udara) yang sangat rentan akan ancaman seperti penyadapan pihak yang tak bertanggung jawab. Kemudahan dalam bertukar informasi melalui SMS ini disalahgunakan oleh beberapa pihak. Beberapa orang dengan berbagai cara mencoba mencuri informasi yang bukan hak mereka. Hal ini tentunya akan sangat berbahaya untuk pengguna, terutama bagi mereka yang sering mengirimkan data dan informasi rahasia melalui SMS.

Karena itu, dibutuhkan suatu cara untuk mengamankan informasi yang sifatnya penting atau rahasia. Dengan melakukan enkripsi terhadap teks SMS, maka tingkat keamanan informasi dari pesan tersebut dapat ditingkatkan. Saat ini, AES (*Advanced Encryption Standard*) digunakan sebagai standar algoritma kriptografi terbaru. Dengan memanfaatkan algoritma AES ini, maka dapat dikembangkan suatu aplikasi SMS yang memungkinkan pengguna untuk mengirimkan pesan singkat dengan enkripsi teks dan dapat melakukan dekripsi terhadap pesan terenkripsi. Aplikasi SMS ini akan dibangun berbasis *mobile* pada *platform* Android.

I. Teori Dasar

1.1 SMS (*Short Message Service*) [1]

Layanan pesan singkat atau surat masa singkat (bahasa Inggris: *Short Message Service* disingkat SMS) adalah sebuah layanan yang dilaksanakan dengan sebuah telepon genggam untuk mengirim atau menerima pesan-pesan pendek (Gupta, 2000). Pada mulanya SMS dirancang sebagai bagian dari GSM, tetapi sekarang sudah didapatkan pada jaringan bergerak lainnya termasuk jaringan UMTS.

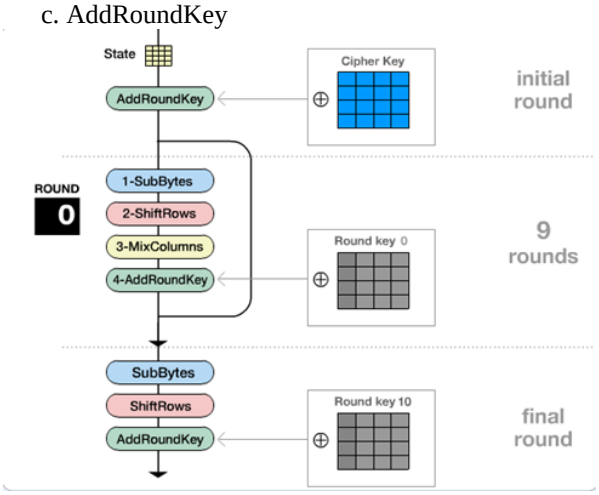
Sebuah pesan SMS maksimal terdiri dari 140 bytes, dengan kata lain sebuah pesan bisa memuat 140 karakter 8-bit, 160 karakter 7-bit atau 70 karakter 16-bit untuk bahasa Jepang, bahasa Mandarin dan bahasa Korea yang memakai Hanzi (Aksara Kanji / Hanja). Selain 140 bytes ini ada data-data lain yang termasuk. Adapula beberapa metode untuk mengirim pesan yang lebih dari 140 bytes, tetapi seorang pengguna harus membayar lebih dari sekali. SMS bisa pula untuk mengirim gambar, suara dan film. SMS bentuk ini disebut MMS.

1.2 *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) merupakan algoritma kriptografi yang dapat digunakan untuk mengamakan data. Menurut Ariyana (2011), Algoritma AES adalah blok *chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext*; sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES ini mengunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkripsi dan dekripsi data pada blok 128 bits. [2]

Algoritma ini berbeda dengan DES yang berorientasi bit, AES beroperasi dalam orientasi *byte*. Pada setiap putarannya digunakan kunci internal yang berbeda (disebut dengan *round key*). *Enchipering* melibatkan operasi subtitusi dan permutasi. Garis besar algoritma AES yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (di luar proses pembangkitan *round key*).

1. *AddRoundKey* : melakukan XOR antara state awal (plainteks) dengan *chiper key*. Tahap ini disebut juga *initial round*.
2. Putaran sebanyak *Nr* – 1 kali. Proses yang dilakukan pada setiap putaran adalah :
   a. *SubBytes* : subtitusi *byte* dengan menggunakan tabel subtitusi (*S-box*)
   b. *ShiftRows* : pergeseran baris-baris *array state* secara *wrapping*
   c. *MixColumns* : mengacak data di masing-masing kolom *array state*
   d. *AddRoundKey* : melakukan XOR antara state sekarang *round key*.
3. *Final round* : proses untuk putaran terakhir.
   a. *SubBytes*
   b. *ShiftRows*
   c. AddRoundKey



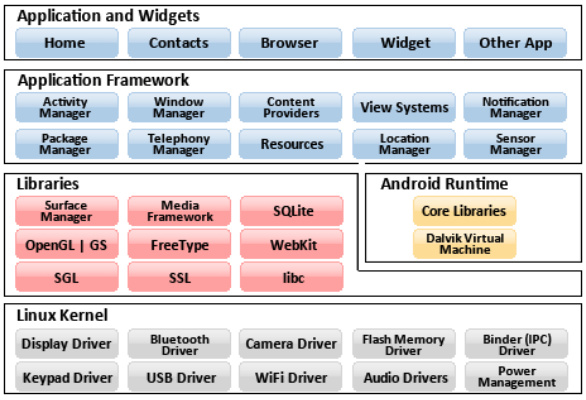
Gambar 1. Skema AES

1.3 Android[3]

Android adalah sistem operasi untuk telepon seluler yang berbasis Linux. Android menyediakan *platform* terbuka bagi para pengembang buat menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak. Awalnya, Google Inc. membeli Android Inc., pendatang baru yang membuat peranti lunak untuk ponsel (Murphy, 2010).

1.3.1 Android *Software Stack*

Google mengibaratkan Android sebagai sebuah *software stack*. Setiap lapisan dari susunan ini menghimpun beberapa program yang mendukung fungsi-fungsi spesifik dari sistem operasi. Android *software stack* digambarkan pada Gambar 2.4 sebagai berikut.



Gambar 2. Android *software stack*

2.3.2 Fitur Android

Fitur yang tersedia di Android adalah:

1. Kerangka aplikasi: itu memungkinkan penggunaan dan penghapusan komponen yang tersedia.
2. Dalvik mesin virtual: mesin virtual dioptimalkan untuk perangkat *mobile*.
3. Grafik: grafik di 2D dan grafis 3D berdasarkan pustaka OpenGL.
4. SQLite: untuk penyimpanan data.

5. Mendukung media: audio, video, dan berbagai format gambar (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)
6. GSM, Bluetooth, EDGE, 3G, dan WiFi (*hardware dependent*), kamera, *Global Positioning System* (GPS), kompas, dan *accelerometer* (tergantung hardware).

1.4 Eclipse IDE

Menurut Lyrac (2009), Eclipse adalah sebuah IDE untuk mengembangkan perangkat lunak dan dapat dijalankan di semua platform (*platform-independent*). Berikut ini adalah sifat dari Eclipse:

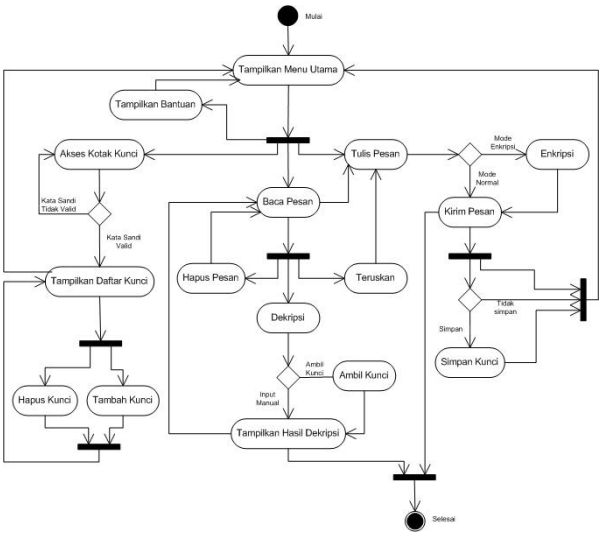
1. *Multi-platform*
   Target sistem operasi Eclipse adalah Microsoft Windows, Linux, Solaris, AIX, HP-UX dan Mac OS X.
2. *Multi-language*
   Eclipse dikembangkan dengan bahasa pemrograman Java, akan tetapi Eclipse mendukung pengembangan aplikasi berbasis bahasa pemrograman lainnya, seperti C/C++, Cobol, Python, Perl, PHP, dan lain sebagainya.
3. *Multi-role*
   Selain sebagai IDE untuk pengembangan aplikasi, Eclipse pun bisa digunakan untuk aktivitas dalam siklus pengembangan perangkat lunak, seperti dokumentasi, tes perangkat lunak, pengembangan *web*, dan lain sebagainya. [4]

II. Hasil Eksperimen

Aplikasi Android yang dibuat diberi nama AES SMS Plus. AES SMS Plus adalah aplikasi SMS dengan enkripsi teks yang menggunakan algoritma AES dalam proses enkripsi dan dekripsinya. Aplikasi yang dibuat memiliki spesifikasi dan fitur sebagai berikut :

1. Dijalankan di lingkungan sistem operasi Android 2.1 (éclair) ataupun versi di atasnya.
2. Penulisan pesan dalam modus normal atau modus enkripsi.
3. Enkripsi pesan dengan algoritma AES 128-bit.
4. Mendukung semua karakter UTF-8 (huruf Arab, Mandarin, Korea, Jepang, dll).
5. Dapat menggunakan kunci yang berbeda untuk setiap pesan.
6. Menggunakan MD5 untuk mengamankan kunci enkripsi.
7. Proses enkripsi dan dekripsi yang cepat.
8. Kotak kunci untuk menyimpan semua kunci enkripsi yang dilengkapi dengan pengamanan *password*.
9. Antar muka percakapan pesan berupa percakapan.
10. Laporan terkirim dan penerimaan pesan.

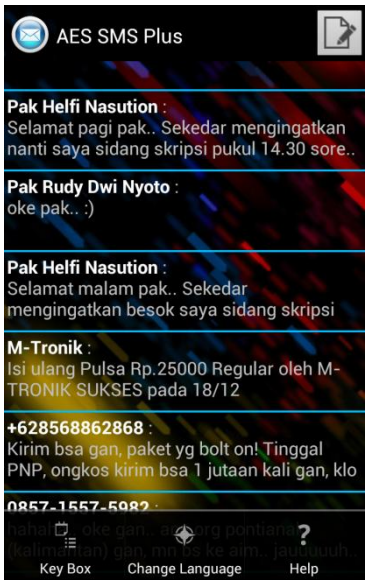
Secara garis besar, alur kerja aplikasi SMS dengan enkripsi teks menggunakan algoritma *block cipher* AES yang dirancang ditunjukkan dengan *activity diagram* pada Gambar 3.



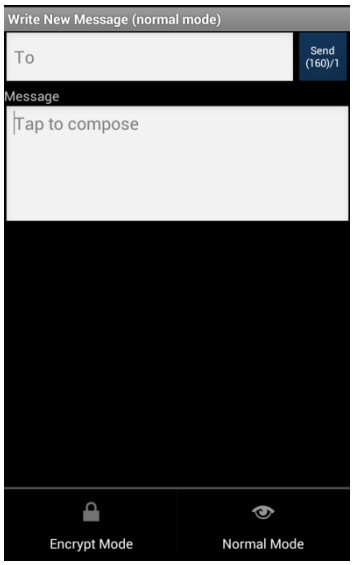
Gambar 3. *Activity diagram* aplikasi

Pengguna dapat melakukan aktivitas menulis pesan dan mengenkrip pesan tersebut sebelum dikirim dengan memasukkan kunci tertentu, atau dapat langsung mengirim pesan tanpa proses enkripsi. Jika pengguna menggunakan fitur enkripsi untuk mengirimkan pesan, maka pengguna dapat menyimpan kunci tersebut ke kotak kunci setelah pesan terkirim. Pengguna dapat membaca pesan langsung atau mendekrip pesan dengan memasukkan kunci secara langsung atau dengan mengakses kotak kunci. Pengguna dapat mengakses kotak kunci untuk melihat daftar kunci yang disimpan atau mendaftarkan kunci baru. Pengguna dapat mengakses bantuan yang berisi tentang deskipsi dan panduan penggunaan fitur aplikasi.

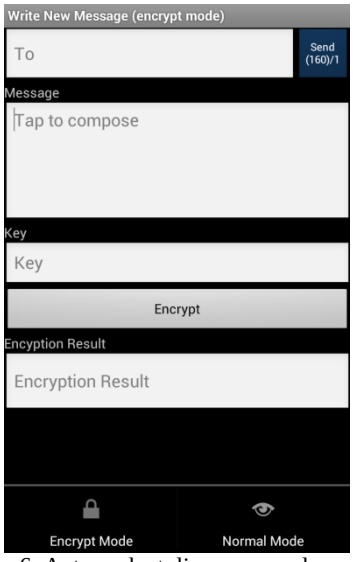
Berikut adalah antarmuka dari aplikasi AES SMS Plus beserta fiturnya.



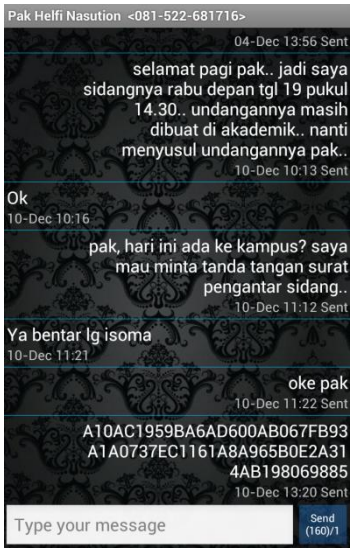
Gambar 4. Antarmuka menu utama



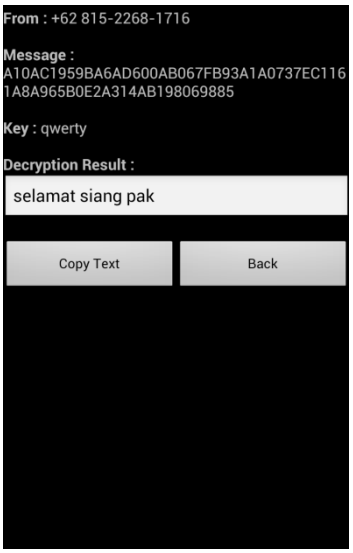
Gambar 5. Antarmuka tulis pesan



Gambar 6. Antarmuka tulis pesan modus enkripsi

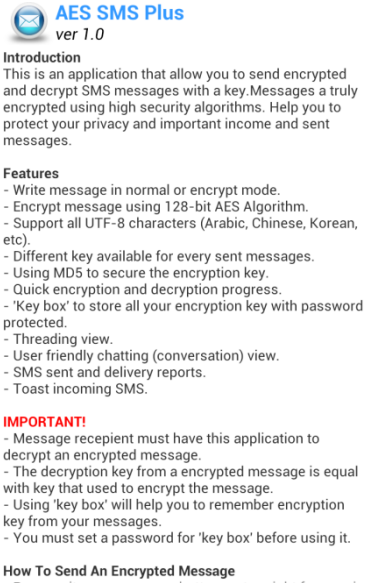


Gambar 7. Antarmuka percakapan pesan



Gambar 8. Antarmuka hasil dekripsi pesan

Gambar 9. Antarmuka kotak kunci



Gambar 10. Antarmuka bantuan

Pengujian dilakukan pada sistem menggunakan metode *Black Box* yang akan memeriksa apakah sistem dapat berjalan dengan benar sesuai dengan yang diharapkan. Adapun teknik ujicoba yang digunakan dalam pengujian *black box* pada aplikasi ini, yaitu menggunakan teknik *sample testing*. Pengujian ini dilakukan pada proses *input* data. Selain itu, akan dilakukan pengujian kompatibilitas aplikasi dengan melakukan pemasangan aplikasi pada *handset* tertentu. Pengujian juga dilakukan dengan metode UAT (*User Acceptance Test*) dimana pengujian dilakukan oleh pengguna secara langsung untuk memeriksa apakah sistem dapat berjalan dengan benar sesuai dengan yang diharapkan oleh pengguna. Pengujian ini melibatkan data real yang didapat secara langsung melalui kuesioner tanpa memperhatikan detail internal dari sistem.

Berikut ini adalah analisis hasil perancangan dan pengujian perangkat lunak Aplikasi SMS (*Short Messaging Service*) dengan enkripsi teks menggunakan algoritma *Block Cipher* AES (*Advanced Encryption Standard*) :

1. Pengguna dapat mengirimkan pesan singkat dengan atau tanpa enkripsi teks, dan dapat membaca rincian percakapan pesan singkat dengan pengguna lainnya.
2. Untuk membaca pesan terenkripsi, pada saat dekripsi pesan singkat pengguna harus menggunakan kunci yang sama dengan kunci yang digunakan saat enkripsi pesan.
3. Sistem akan menghalangi pengguna yang memasukkan *password* yang salah ketika proses *login key box* sehingga aktivitas *key box* hanya dapat diakses oleh pengguna yang memiliki hak akses.
4. Hasil pengujian menunjukkan saat dilakukan *input* data dengan menggunakan metode *black box*, *input* data dengan keseluruhan data kosong akan menimbulkan kesalahan pada program. Akan tetapi pada sistem ini, kemungkinan terjadinya kesalahan sudah ditangani pada kode program, sehingga hanya akan muncul pesan kesalahan atau instruksi pengisian data. Dengan kata lain, sistem dapat menangani data tersebut sesuai dengan apa yang diharapkan.
5. Hasil pengujian menunjukkan bahwa saat dilakukan *input* data dengan salah satu data yang benilai kosong akan menyebabkan kesalahan apabila data tersebut tidak diperbolehkan kosong didalam basis data. Pada sistem ini kemungkinan tersebut sudah ditangani pada kode program sehingga akan muncul pesan kesalahan jika ada salah satu data yang belum diisi.
6. Hasil pengujian kompabilitas menunjukkan bahwa aplikasi SMS dapat berjalan pada sebagian besar tipe dan merek perangkat Android, kecuali perangkat *tablet*/*phablet* merek Samsung dengan versi sistem operasi setara atau lebih dari 4.0.1 (Ice Cream Sandwich) dimana aplikasi gagal dieksekusi.
7. Hasil pengujian validitas kuesioner menunjukkan bahwa semua pertanyaan dalam kuesioner adalah valid untuk digunakan dalam pengumpulan data.
8. Hasil pengujian reliabilitas kuesioner menunjukkan bahwa kuesioner memiliki memiliki tingkat reliabilitas yang baik dan hasilnya dapat dipercaya.
9. Hasil perancangan dan pengujian menunjukkan bahwa aplikasi SMS ini dapat digunakan untuk mengirimkan pesan singkat dengan enkripsi teks kepada pengguna lainnya dan melakukan dekripsi terhadap pesan singkat yang diterima.
10. Berdasarkan hasil kuesioner, dapat disimpulkan bahwa perangkat lunak yang dirancang dinilai berhasil.

VI. Kesimpulan

Berdasarkan hasil analisis dan pengujian terhadap aplikasi SMS (*Short Message Service*) dengan enkripsi teks menggunakan algoritma *Block Cipher* AES (*Advanced Encryption Standard*) ini maka dapat disimpulkan bahwa:

1. Aplikasi dapat digunakan oleh pengguna untuk mengirimkan pesan singkat dengan enkripsi teks ke nomor tujuan tertentu.
2. Aplikasi dapat melakukan dekripsi terhadap pesan terenkripsi dengan masukan kunci yang sama dengan yang digunakan pada saat proses enkripsi.
3. Berdasarkan hasil pengujian kompatibilitas, aplikasi dapat berjalan dengan baik pada sebagian besar perangkat Android, kecuali *phablet* / *tablet* merek Samsung dengan versi sistem operasi setara atau diatas 4.0.1.
4. Berdasarkan hasil penilaian oleh responden melalui kuesioner, aplikasi yang dibuat dinilai berhasil untuk membantu pengguna dalam mengirimkan pesan singkat secara aman, cepat, dan mudah.

Referensi

[1] Gupta, Punet. 2000. *Short Message Service: What, How and Where.* Februari, 20,2009. http://www.wirelessdevnet.com/channels/sms/features/sms.html

[2] *Ariyana, Yoki. 2011. Advanced Encryption Standard (AES). Bandung : PPPPTK IPA Bandung*

[3] Murphy, Mark L. 2010. *Beginning Android 2*. New York: Apress.

[4] Lyracc. 2009. *Eclipse IDE*. Januari, 7, 2012. http://java.lyracc.com/belajar/java-untuk-pemula/eclipse-ide

Biografi

Irwan lahir di Pontianak, 8 April 1990. Ia menerima gelar ST dari Fakultas Teknik Universitas Tanjungpura pada tahun 2012.