APLIKASI PENGAMAN SMS DENGAN METODE KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) 128 BERBASIS ANDROID

Awang H. Kridalaksana[1)], Eka Arriyanti [2)], Wahyu Widodo[3)]

[1,2,3]Teknik Informatika, STMIK Widya Cipta Dharma
[1,2,3] Jl. Prof. M. Yamin No. 25, Samarinda, 75123
E-mail : awangkid@gmail.com[1)], ivaneka@gmail.com[2)], wahyudjadoel@gmail.com [3)]

ABSTRAK

Beberapa tahun belakangan ini telah terjadi perkembangan pesat dalam teknologi telepon seluler. Salah satunya adalah perkembangan dari telepon pintar dengan banyak fitur dan juga sistem operasi yang kompleks serupa dengan sebuah komputer. Walaupun telepon pintar memiliki banyak fitur yang termasuk di dalamnya sistem operasi, tetapi SMS tetap populer untuk digunakan. Fitur SMS yang masih digunakan hingga saat ini, memunculkan pertanyaan tentang keamanan informasi jika seseorang ingin mengirimkan informasi rahasia melalui fasilitas SMS. Kemudahan pertukaran informasi melalui SMS disalahgunakan oleh beberapa orang.

Beberapa orang dengan berbagai cara mencoba untuk mencuri informasi secara ilegal. Oleh karena itu, kita membutuhkan suatu cara untuk mengamankan informasi yang bersifat rahasia dan penting. Proses enkripsi dapat digunakan untuk meningkatkan tingkat keamanan informasi dan teks pesan SMS. Sekarang, AES (Advanced Encryption Standard) digunakan sebagai standar untuk algoritma kriptografi. Oleh karena itu, ini dapat digunakan untuk mengembangkan aplikasi SMS dengan enkripsi teks menggunakan algoritma AES. Aplikasi berbasis mobile dibangun pada platform android. Hasil uji menunjukkan bahwa aplikasi dapat menjalankan enkripsi sebuah pesan teks pendek kepada nomor tujuan tertentu dan tidak dapat mendekripsi pesan yang terenkripsi. aplikasi dapat membantu pengguna untuk mengirim pesan singkat dengan aman, cepat, dan mudah.

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

1. PENDAHULUAN

Dewasa ini perkembangan teknologi seluler sangat pesat. Android adalah sistem operasi *open source smartphone* layar sentuh seperti iOS iPhone dan OS BlackBerry. Ada beberapa *open source* seperti linux, symbian, windows mobile dan sebagainya. Dengan munculnya Android yang dapat dijalankan pada ponsel, membuat banyak produsen ponsel berlomba mengunakan *open source* ini.

Android dikembangkan dari Kernel Linux yang adalah Open Source, sehingga perkembangannya sangat pesat. Bahkan menurut data terbaru dari perusahaan riset pasar GfK Ritel dan Teknologi pada tahun 2011, penjualan ponsel berbasis Android meroket, mencapai peningkatan 350 persen. Dan ada ratusan ribu aplikasi yang siap di *download* dalam Android *Market*. Ini merupakan perkembangan yang sangat pesat, karena Android terus berkembang baik dari aplikasi maupun pengembangannya.

Pasar Android di Indonesia akan berkembang seiring dari banyaknya operator selular dan produsen *smartphone* yang gencar menyuarakan *open source* Android. Pangsa pasar *smartphone* Indonesia yang besar, memungkinkan *smartphone* yang murah dan mempunyai fitur yang lengkap sesuai dengan karateristik dari masyarakat Indonesia.

Persaingan di *open source* ini sangat terbuka. Android datang untuk menjadi pesaing dari iPhone dan Blackberry untuk pangsa *smartphone*. Kedua *smartphone* tersebut sudah mendominasi pasar dunia, dengan kehadiran Android dipastikan mereka sudah mulai terancam dominasinya. Produsen smartphone yang sudah memasukkan *open source* Android antara lain: HTC, Sharp, Motorola, Toshiba, Samsung, Sony Erricson, dll.

Saat ini siapa yang tidak mengenal teknologi nirkabel, dimana industri telekomunikasi dari tahun ke tahun mengalami pertumbuhan yang cukup fantastik dan jumlah pengguna telepon genggam atau *handphone* semakin meningkat. Salah satu layanan favorit yang sering digunakan yaitu SMS (*Short Message Service*), dimana hampir setiap detik orang menggunakan layanan tersebut saat ini. Penggunaan pesan 160 karakter (dalam satu pengiriman pesan) untuk komunikasi *person-to-person* sudah menjadi kebutuhan utama setiap pengguna ponsel.

Faktor psikologis yang mendukung stabilnya penggunaan SMS saat ini antara lain, biaya yang terkesan murah, skema tarif yang sangat sederhana dan mudah dimengerti oleh konsumen, serta tidak mengenal biaya roaming nasional layaknya *voice call*/panggilan telepon.

Berbagai keunggulan diatas belum dimiliki oleh MMS (*Multimedia Messaging Service*) sehingga layanan pesan multimedia tersebut belum bisa menggantikan peranan pesan singkat SMS. SMS semakin berdaya guna ketika dapat digunakan untuk beragam aplikasi baik untuk keperluan pribadi, korporasi maupun publik.

Disisi lain, dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Di luar negeri pemanfaatan SMS untuk mengirim pesan rahasia telah lebih dulu dikembangkan. Misalnya di Inggris sebuah perusahaan operator telepon selular, staellium UK, mengeluarkan layanan bernama "s*tealth 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 *self-destruct text message*. Ada juga pengamanan sms dengan menggunakan kriptografi sms yang memanfaatkan kunci untuk medekripsikan sms yang telah di enkripsi.

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.

Oleh karena itu, penulis akan mencoba membuat sebuah aplikasi pengamanan sms dengan metode kriptografi *Advaced Encryption Standard* (AES)128 untuk mengenkripsi data yang berjalan pada system operasi android sehingga pemilih *handphone* yang berbasis android dapat melakukan pertukaran data (sms) dengan lebih aman dan nyaman.

2. RUANG LINGKUP PENELITIAN

1. Rumusan Masalah

Sesuai dengan latar belakang masalah yang dijabarkan diatas, maka penulis membuat perumusan masalah, yaitu sebagai berikut : "Bagaimana membuat aplikasi pengaman SMS pada ponsel berbasis android dengan metode kriptografi *Advaced Encryption Standard* (AES)".

2. Batasan Masalah

Adapun Batasan masalah dari aplikasi ini adalah untuk menghindari analisis yang berkepanjangan dan mengingat luasnya ruang lingkup permasalahan yang ada, Batasan masalah di sini adalah :

1. Perangkat lunak yang di bangun hanya dapat di jalankan pada ponsel yang memiliki sistem operasi android versi *gingerbread*.
2. Dua belah pihak pengguna harus sama-sama menggunakan aplikasi ini.
3. Aplikasi pengaman SMS menggunakan *Kriptografi Advanced Encryption Standard* (AES) 128 untuk proses enkripsi dan dekripsinya.

3. BAHAN DAN METODE

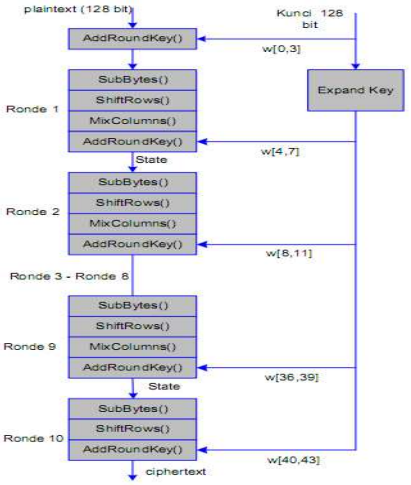
3.1 Penjelasan Bahan

Aplikasi menurut Sudarmo (2006), aplikasi adalah jenis tugas atau pekerjaan yang dilakukan suatu program atau sistem komputer misalnya perancangan teknik, sistem pemesanan tiket pesawat terbang, administrasi keuangan dan lain sebagainya.

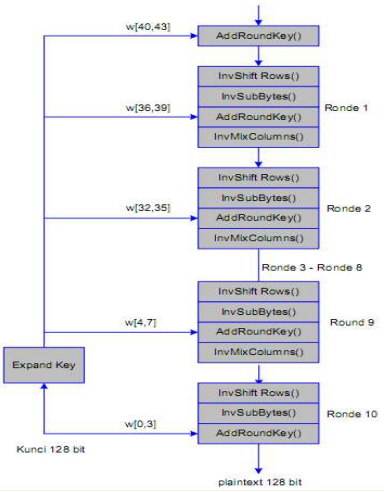
Menurut Talib (2005), aplikasi adalah program yang dibuat untuk tujuan tertentu misalnya untuk penjualan disupermarket, untuk mengelola data pasien di rumah sakit, untuk mencetak kuitansi dan sebagainya.

SMS menurut Rosidi (2004), Short Message Service (SMS) merupakan sebuah layanan yang banyak diaplikasikan pada sistem komunikasi tanpa kabel, memungkinkan dilakukannya pengiriman pesan dalam bentuk alphanumeric antara terminal pelanggan atau antara terminal pelanggan dengan sistem eksternal seperti email, paging, voice mail, dan lain-lain.

Advanced Encryption Standard (AES) merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data. Menurut Ariyana (2011), Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi.



Gambar 1 Enkripsi AES



Gambar 2. Dekrispi AES

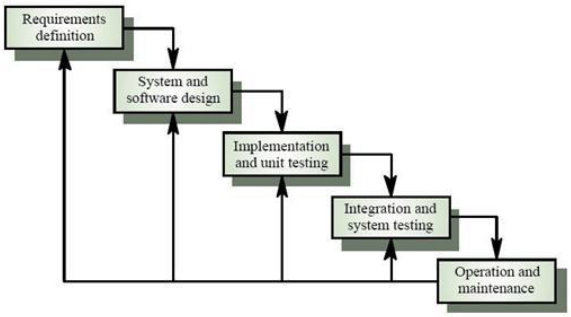
Menurut Hermawan (2011), Android merupakan sistem operasi untuk telepon seluler yang berbasis Linux.

Menurut Hermawan (2011), Java merupakan dasar pemrograman untuk membangun aplikasi pada Sistem Operasi Android. Oleh karena itu, untuk membangun aplikasi pada sistem operasi ini diperlukan dasar tentang pemrograman Java. Java merupakan pemrograman berorientasi objek. Oleh karena itu, setiap konsep yang diimplementasikan dalam Java berbentuk dalam kelas.

Kelas ini mendefinisikan objek-objek yang memerikan kesamaan prilaku dan keadaan.

3.2 Metode Air Terjun

Menurut Sommerville (2003) model ini adalah model klasik yang bersifat sistematis, berurutan dalam membangun software. Berikut ini adalah dua gambaran dari waterfall model sekalipun keduanya menggunakan nama-nama fase yang berbeda, namun sama dalam intinya. Yang pertama adalah fase-fase dalam metode waterfall menurut referensi Pressman dan yang kedua menurut referensi Sommerville.

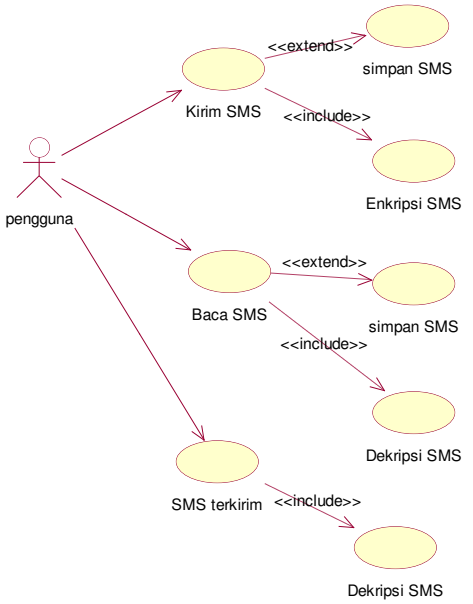


Gambar 3. Metode Air Terjun

Model air terjun (waterfall) adalah model satu arah yang dimulai dari tahap persiapan sampai perawatan, dan model inilah yang dipakai oleh penulis dalam menganalisa sistem yang akan dikerjakan (Pressman, 2002).

2. RANCANGAN SISTEM/APLIKASI

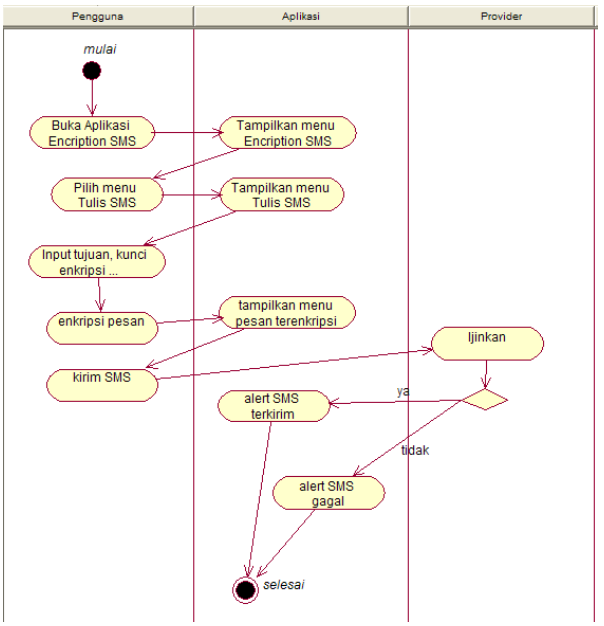
Use Case diagram dari aplikasi yang dibuat ini dapat dilihat pada gambar berikut :



Gambar 4. Use Case Diagram.

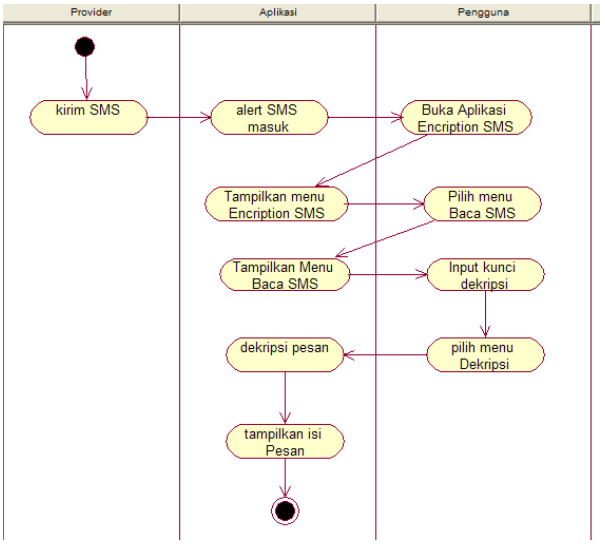
Use Case diatas menggambarkan menu utama yang terdapat pada aplikasi Encription SMS yang dibuat. Terdapat menu Kirim SMS, Baca SMS dan SMS terkirim. Pengguna dapat memilih menu Kirim SMS untuk mengirimkan pesan yang terenkripsi, memilih menu Baca SMS untuk membaca pesan yang terenkripsi lalu mendekripsi pesan sebelum dapat membaca pesan asli, dan pengguna juga dapat memilih menu SMS Terkirim untuk membaca pesan yang telah pengguna kirimkan ke pengguna lain.

Activity Diagram kirim SMS memperlihatkan segala aktifivitas yang dilakukan oleh pengguna yang menggunakan aplikasi Encription SMS. Berikut adalah perancangan Activity kirim SMS nya:



Gambar 5. Activity Diagram Kirim SMS

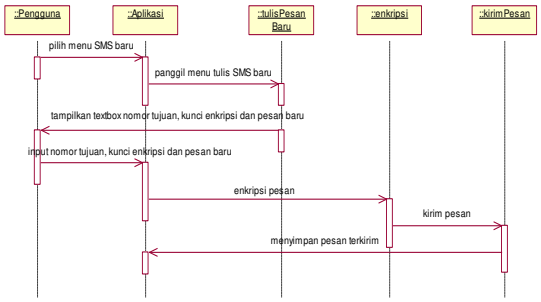
Activity Diagram baca SMS memperlihatkan segala aktifivitas yang dilakukan oleh pengguna yang menggunakan aplikasi Encription SMS. Berikut adalah perancangan Activity baca SMS nya:



Gambar 6. Activity Diagram Baca SMS

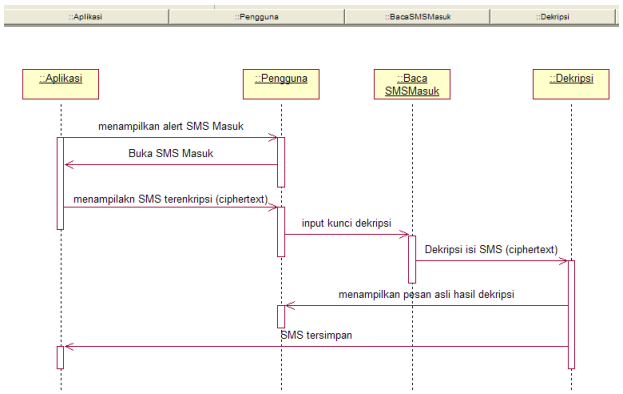
Sequence Diagram biasa digunakan untuk menggambarkan skenario atau rangkaian langkah-langkah yang dilakukan sebagai respons dari sebuah event untuk menghasilkan output tertentu. Diagram ini

menunjukan sejumlah contoh obyek dan message yang di letakkan di antara objek-objek di dalam use case. Komponen utama sequence diagram terdiri dari objek yang di gambarkan dengan kotak segi empat bernama. Message di wakili oleh garis dengan tanda panah dan waktu yang di tunjukkan dengan progress vertical. Diawali dari apa yang mentrigger aktivitas tersebut, proses dan perubahan apa saja yang terjadi secara internal dan output apa yang dihasilkan.



Gambar 7. Sequence Diagram kirim SMS

Gambar diatas merupakan Sequence Diagram kirim SMS yang menggambarkan proses Penulisan SMS sebelum dikirimkan. Prosesnya dimulai dengan pengguna membuka aplikasi lalu memilih menu Tulis SMS kemudian pengguna menginputkan nomor tujuan, kunci enkripsi dan pesan asli sebelum dikirimkan ke pengguna lain. Setelah semua diinputkan pengguna memilih menu enkripsi pesan yang kemudian diteruskan kepada kirim pesan untuk mengirimkan pesan ke pengguna lainnya.



Gambar 8. Sequence Diagram Baca SMS

Gambar diatas merupakan Sequence Diagram baca SMS yang menggambarkan proses baca SMS yang masuk yang dikirimkan oleh pengguna lain. Prosesnya dimulai dengan aplikasi menampilkan alert pesan masuk lalu pengguna membuka aplikasi kemudian pengguna memasukkan kunci dekripsi sebelum dapat membaca pesan yang telah di enkripsi. Sebelumnya kedua pengguna telah menetapkan kunci yang sama antara kunci enkripsi dan kunci dekripsinya.

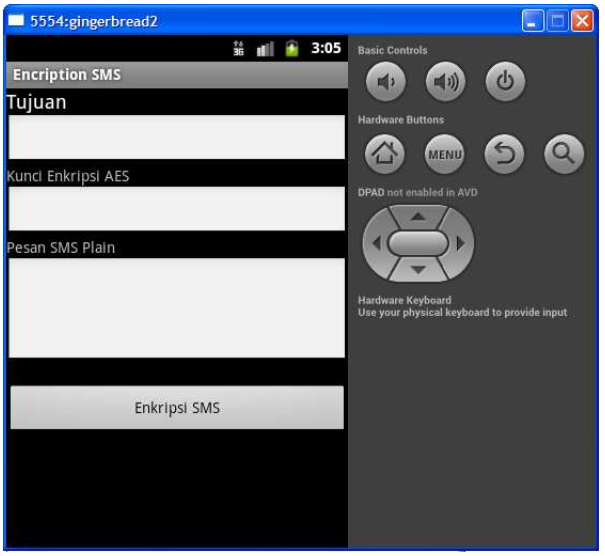
5. IMPLEMENTASI

Tampilan Halaman Utama

Gambar 9. Halaman Utama

Layar ini merupakan tampilan awal pada aplikasi Encription SMS, dimana terdapat beberapa menu yaitu Tulis SMS, Baca SMS dan SMS terkirim.

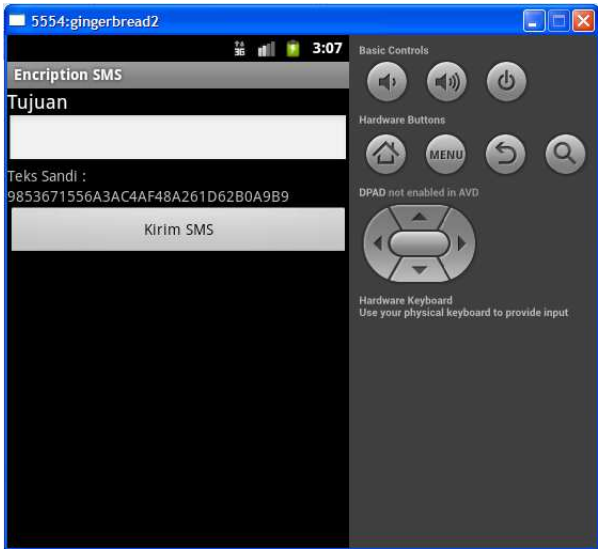
Tampilan Tulis SMS



Gambar 10. Tampilan Menu Tulis SMS

Layar ini merupakan tampilan menu Tulis SMS. Pada menu ini terdapat inputan berupa tujuan berupa nomor tujuan, kunci enkripsi AES yang merupakan kunci yang telah disepakati oleh kedua belah pihak pengguna aplikasi Encription SMS dan Pesan SMS Plain yang merupakan isi pesan yang akan dikirimkan kepada pengguna lainnya. Dan juga ada menu Enkripsi SMS untuk mengenkripsi pesan sebelum dikirimkan ke pengguna lain tersebut.

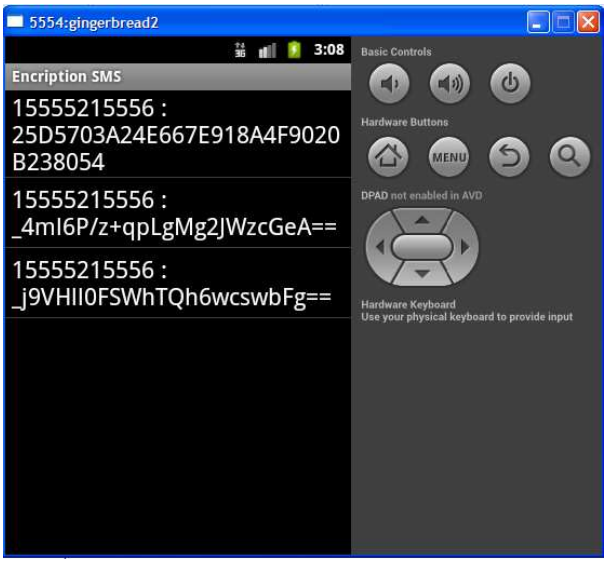
Tampilan Enkripsi SMS



Gambar 11. Tampilan Menu Enkripsi SMS

Layar ini merupakan tampilan hasil menu Enkripsi SMS. Terdapat input tujuan bila pada saat tulis SMS belum menginputkan nomor tujuan, lalu terdapat teks sandi yang merupakan hasil dari pesan yang telah di enkripsi. Kemudian menu Kirim SMS untuk mengirimkan pesan sandi (ciphertext) ke pengguna lainnya.

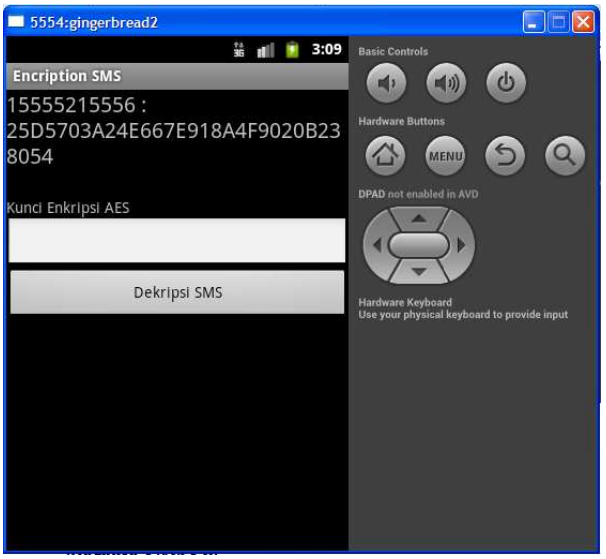
Tampilan Baca SMS



Gambar 12. Tampilan Menu Baca SMS

Layar ini merupakan tampilan seluruh pesan masuk. Pilih salah satu pesan masuk untuk membaca isi pesan yang telah dikirim oleh pengguna lain.

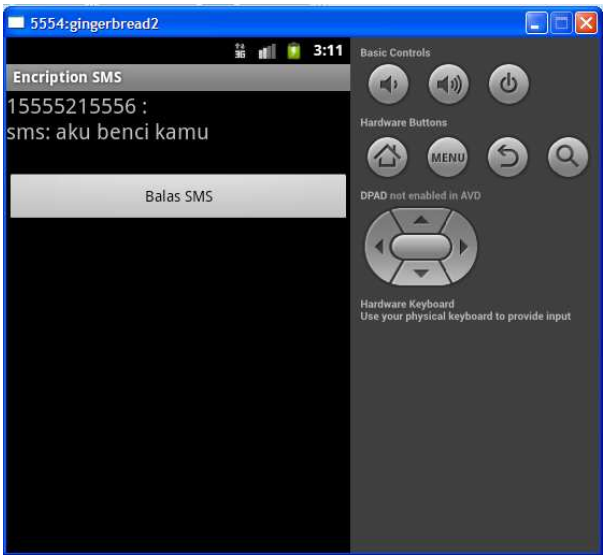
Tampilan Isi Menu Baca SMS



Gambar 13. Tampilan Isi menu Baca SMS

Layar ini merupakan tampilan isi pesan masuk yang dikirimkan oleh pengguna lain kepada anda. Pada menu ini pesan masih berupa kode sandi atau *ciphertext*. Inputkan kunci enkripsi aes yang telah disepakati sebelumnya untuk dapat melihat isi dari pesan yang telah diterima. Pilih menu dekripsi untuk melihat isi dari pesan berupa text asli.

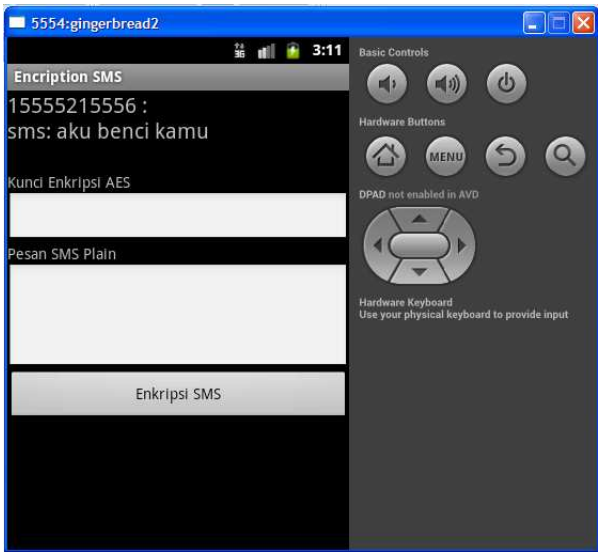
Tampilan Isi Dekripsi



Gambar 14. Tampilan hasil dekripsi

Layar ini merupakan tampilan isi dari pesan asli yang telah dienkripsi sebelumnya. Pilih menu Balas SMS untuk membalas isi pesan kepada pengguna yang telah mengirimkan pesan kepada anda.

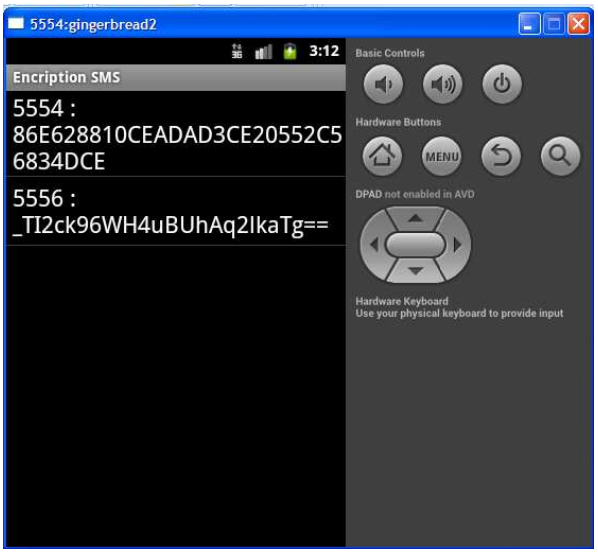
Tampilan Balas SMS



Gambar 15. Tampilan Balas SMS

Layar ini merupakan tampilan isi balas SMS. Sama seperti pada menu sebelumnya Tulis SMS, yang membedakan hanya pada menu Balas SMS pengguna tidak perlu lagi menginputkan nomor tujuan.

Tampilan SMS Terkirim



Gambar 16. Tampilan SMS Terkirim

Layar ini merupakan tampilan seluruh SMS terkirim berupa text sandi atau *ciphertext*. Pilih salah satu pesan terkirim untuk membaca isi pesan yang telah dikirimkan.

Pengujian Black Box

Metode *black box* adalah cara pengujian hanya dilakukan dengan menjalankan atau mengeksekusi unit atau modul, kemudian diamati apakah hasil dari unit itu sesuai dengan hasil yang diinginkan. Pengujian terhadap aplikasi pengaman sms dengan metode kriptografi *Advanced Encryption Standard* (AES) 128 berbasis Android dilakukan terhadap enkripsi, dekripsi, mengirim dan menerima pesan yang dilakukan untuk menguji fungsi-fungsi khusus dari aplikasi perangkat lunak yang dirancang. Seperti yang terlihat pada tabel 1 dibawah ini :

Tabel 1. Daftar Pengujian Black Box

No.	Kasus/diuji	Skenario uji	Hasil yang diharapkan	Hasil pengujian
1.	Tampilan Awal	Memilih icon louncher Encryption SMS	Ketika icon disentuh maka aplikasi berjalan dan masuk ke tampilan awal	berhasil
2.	Pilih tulis SMS	Memilih menu tulis SMS	Ketika memilih menu ini akan tampil input tujuan, kunci enkripsi aes, pesan SMS dan tombol enkripsi SMS	berhasil
3.	Pilih enkripsi SMS	Memilih tombol enkripsi SMS	Ketika tombol dipilih maka akan tampil tujuan, teks sandi dan tombol kirim SMS	berhasil
4.	Pilih kirim SMS	Memilih tombol kirim SMS	Ketika tombol kirim SMS dipilih maka pesan akan dikirim.	Berhasil
5.	Pilih baca SMS	Memilih menu baca SMS	Ketika tombol menu SMS dipilih maka pesan akan terbuka	Berhasil
6.	Pilih dekripsi SMS	Memilih tombol dekripsi SMS	Ketika tombol menu dekripsi dipilih maka ciphertext akan di dekripsi menjadi text pesan yang akan dibaca	Berhasil

Pengujian Beta Testing

Beta testing merupakan pengujian yang dilakukan secara objektif, pengujian ini dilakukan oleh user yang akan menggunakan aplikasi yang dibangun. Pengujian dilakukan terhadap 10 orang yang akan berhubungan dengan aplikasi yang dibangun. Dari hasil kuesioner tersebut akan dilakukan perhitungan untuk

dapat diambil kesimpulannya terhadap penilaian aplikasi yang dibangun.

Berikut adalah pertanyaan dan hasil kuesioner yang telah dibagikan dengan menggunakan rumus:

$$Y = P / Q * 100\%$$

Keterangan :
Y = Nilai prosentase
P = Banyaknya jawaban responden tiap soal
Q = Jumlah responden

Hasil pengujian *beta* adalah sebagai berikut :

1. Bagaimana tampilan menu aplikasi Encription SMS ?
   ☐ ya ☐ cukup ☐ tidak
2. Bagaimana keamanan pesan sandi aplikasi Encription SMS ?
   ☐ ya ☐ cukup ☐ tidak
3. Bagaimana kecepatan enkripsi dan dekripsi aplikasi Encription SMS ?
   ☐ ya ☐ cukup ☐ tidak
4. Bagaimana kemudahan penggunaan aplikasi Encription SMS?
   ☐ ya ☐ cukup ☐ tidak
5. Apakah anda berminat menggunakan aplikasi Encription SMS ?
   ☐ ya ☐ cukup ☐ tidak

Kesimpulan Pengujian *Beta Testing*

Dari hasil pengujian yang dilakukan menggunakan beta testing didapatkan sebuah kesimpulan yang merujuk pada perkembangan sebuah aplikasi yang dibangun. Untuk mengetahui hasil pengujian dibuatlah kuisioner dengan beberapa pilihan jawaban yang disediakan adalah sebagai berikut :

- Ya
- Cukup
- Tidak

Dari hasil yang diujikan terdapat beberapa poin penilaian seperti yang sudah diujikan yaitu tampilan, keamanan, kecepatan, kemudahan dan minat. Maka didapat hasil jawaban pada tabel 2 yaitu :

Tabel 2. Hasil Jawaban Pengujian Beta Testing

Soal	Jawaban Ya	Jawaban Cukup	Jawaban Tidak	Jumlah Koresponden
1	-	10	-	10
2	8	2	-	10
3	10	-	-	10
4	2	8	-	10
5	4	6	-	10
Jumlah	**24**	**26**	**-**	**50**

Tabel merupakan jumlah jawaban dari hasil kuesioner uji responden yang diisi oleh 10 orang. Hasil tersebut dibuat dengan penjelasan seperti berikut:

1. Jawaban ya : 24 dari 50 (24/50 x 100% = **48%**)
2. Jawaban Cukup : 26 dari 50 (26/50 x 100% = **52%**)
3. Jawaban Tidak : 0 dari 50 (0/50 x 100% = **0%**)

6. KESIMPULAN

Berikut adalah kesimpulan yang diperoleh selama pelaksanaan skripsi ini:

1. Sebuah aplikasi enkripsi SMS yang mengimplementasikan algorima kriptografi simetri telah berhasil dibangun.
2. Aplikasi enkripsi SMS telah berhasil meningkatkan keamanan pengiriman pesan SMS melalui telepon seluler sebesar 85%.
3. Algoritma AES dapat diimplementasikan dengan baik sebesar 80% untuk melakukan enkripsi SMS yang bekerja pada jaringan GSM dengan mengirim dan menerima pesan dalam bentuk *ciphertext*.

7. SARAN

Untuk perbaikan dan pengembangan aplikasi enkripsi SMS lebih lanjut, disarankan perbaikan sebagai berikut:

1. Pengembangan aplikasi enkripsi SMS ini menggunakan satu jenis algoritma yaitu AES, guna meningkatkan keamanan yang lebih, aplikasi dapat ditambahkan beberapa algoritma kriptografi lainnya.
2. Aplikasi ini dapat mengengkripsikan pesan karakter standar ASCII, untuk pengembangan lebih lanjut diharapkan aplikasi dapat mengenkripsikan karakter *Arabic* dan *Chines*.

8. DAFTAR PUSTAKA

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

Hermawan, Stephanus, 2011. Mudah Membuat Apliaksi Android, Yogyakarta : Andi.

Kurniawan, Yusuf, 2004. Kriptografi Keamanan Internet dan Jaringan Komunikasi, Bandung : Informatika.

Munir, Rinaldi, 2004. Advanced Encryption Standard (AES), Institut Teknologi Bandung.

Pressman, Roger, 2002, Rekayasa Perangkat Lunak Praktisi (Buku I), Yogyakarta : Penerbit Andi & McGraw-Hill Book Co.

Rosidi, R,. I.2004, Membuat Sendiri SMS Gateway (ESME) Berbasis Protokol SMPP. Yogyakarta : ANDI

Sudarmo, Padji M, 2006. Kamus Istilah Komputer, Teknologi Informasi, Jakarta : Yrama Widya.

Talib, Hear, 2005. Panduan Praktis Belajar Komputer, Jakarta : Elek Media Komputindo.