

# APLIKASI SHORT MESSAGE SERVICE DENGAN ENKRIPSI TEKS MENGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD BERBASIS MOBILE PADA PLATFORM ANDROID

**Andi Harmin**

Program Studi Teknik Komputer  
STMIK Profesional Makassar  
andiharmin1976@gmail.com

## **Abstrak**

*Perangkat Android memiliki fitur yang lengkap seperti layanan SMS (Short Message Service) yang paling sering digunakan. SMS merupakan layanan telepon seluler untuk mengirim dan menerima pesan singkat yang sangat praktis, murah dan efisien sebagai bentuk pertukaran informasi melalui pesan pendek. Namun demikian SMS tidak menjamin integritas dan keamanan pesan yang disampaikan. Penerapan Algoritma AES (Advanced Encryption Standard) merupakan metode yang tepat terhadap permasalahan layanan sms yang mempunyai keunggulan dalam melakukan enkripsi dan dekripsi, dengan melakukan 10 kali putaran pada jaringan Feistel serta menggunakan operasi substitusi dan permutasi yang membuat tingkat pengacakan semakin rumit. Hasil yang diperoleh dengan penerapan Algoritma Enkripsi Advanced Encryption Standard akan mampu meningkatkan keamanan pengiriman dan penerimaan pesan singkat dengan cara enkripsi dan dekripsi isi pesan pada perangkat Android.*

**Kata kunci :** *Android, SMS, AES, Enkripsi dan Dekripsi.*

## **A. PENDAHULUAN**

Teknologi telepon genggam (*handphone*) sebagai alat telekomunikasi pada saat ini telah mengubah cara pandang masyarakat dalam berkomunikasi. Berkembangnya teknologi telepon genggam dapat dilihat dengan munculnya berbagai sistem operasi yang lengkap layaknya komputer, diantaranya adalah *Android*.

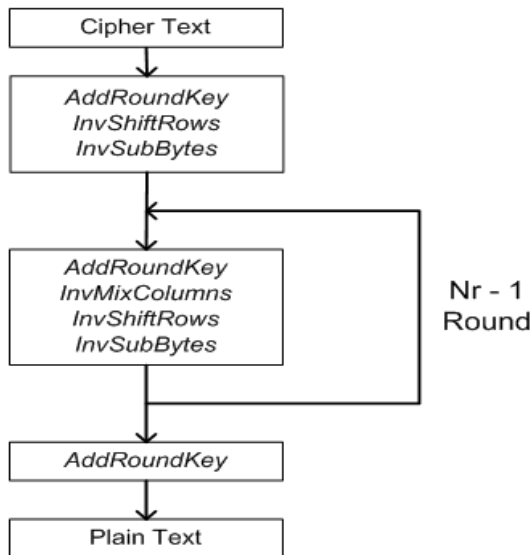
Meskipun *Android* memiliki fitur yang lengkap, layanan *SMS (Short Message Service)* sebagai layanan pertukaran informasi atau pesan pendek menjadi komunikasi yang paling sering digunakan. Namun demikian *SMS* tidak menjamin

integritas dan keamanan pesan yang disampaikan. Pesan yang bersifat personal atau rahasia tidak dijamin sampai ke penerima tanpa diketahui informasinya oleh pihak yang tidak bertanggung-jawab.

Dengan adanya beberapa masalah diatas maka dibutuhkan sebuah sistem keamanan pada layanan *SMS* yang mampu menjaga integritas dan keamanan isi pesan untuk menutupi celah keamanan. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga penyadap akan kesulitan untuk mengetahui isi informasi yang sebenarnya.



tentang deskripsi dan panduan penggunaan fitur aplikasi. Proses deskripsi pesan sms yang terenkripsi menggunakan algoritma AES dapat dilihat pada gambar 3 berikut ini :



**Gambar 3.** Algoritma deskripsi AES

### C. HASIL

Aplikasi *AES SMS Plus* terdiri dari beberapa fitur yang dapat digunakan oleh pengguna. Fitur Menu utama digunakan untuk mengakses pesan melalui kotak masuk dan kotak keluar seperti pada Gambar 4.



**Gambar 4.** Antarmuka menu utama

Untuk fitur kotak masuk digunakan untuk memeriksa pesan yang masuk dari pengirim pesan. Pada fitur ini informasi yang ditampilkan terdiri dari nomor kontak serta isi pesan yang terenkripsi maupun yang tidak terenkripsi. Antarmuka pada fitur ini bisa dilihat pada Gambar 5 berikut ini :



**Gambar 5.** Antarmuka kotak masuk SMS

Sedangkan fitur untuk menulis pesan dapat dilihat pada Gambar 6 berikut ini :



**Gambar 6.** Antarmuka tulis pesan

Aplikasi ini juga dilengkapi dengan fitur kotak keluar untuk menampilkan informasi pesan yang pernah ditulis dan dikirim oleh pengirim pesan dengan menampilkan nomor kontak dan isi pesan yang terenkripsi seperti terlihat pada Gambar 7 dibawah ini :



**Gambar 7.** Antarmuka Pesan keluar

#### **D. PEMBAHASAN**

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 bernilai 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 komparabilitas 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.

## E. 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:

- a. Aplikasi dapat digunakan oleh pengguna untuk mengirimkan pesan singkat dengan enkripsi teks ke nomor tujuan tertentu.
- b. Aplikasi dapat melakukan dekripsi terhadap pesan terenkripsi dengan

- masukan kunci yang sama dengan yang digunakan pada saat proses enkripsi.
- c. 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.
  - d. Berdasarkan hasil penilaian oleh responden melalui kuesioner, aplikasi yang dibuat dinilai berhasil untuk membantu pengguna dalam mengirimkan pesan singkat secara aman, cepat, dan mudah.

## DAFTAR PUSTAKA

- [1] Ariyana, Yoki. 2011. *Advanced Encryption Standard (AES)*. PPPPTK IPA Bandung. Bandung.
- [2] Gupta, Punet. 2000. *Short Message Service: What, How and Where*. <http://www.wirelessdevnet.com/channels/sms/features/sms.html>. Diakses 20 Februari 2009
- [3] Lyracc. 2009. *Eclipse IDE*. <http://java.lyracc.com/belajar/java-untuk-pemula/eclipse-ide>. Diakses 7 Januari 2012.
- [4] Murphy, Mark L. 2010. *Beginning Android 2*. Apress. New York.