VOLUME 5 NOMOR 1, APRIL 2016

ISSN 2089 - 1245

KILAT

JURNAL KAJIAN ILMU DAN TEKNOLOGI

ISSN 2089-1245

SEKOLAH TINGGI TEKNIK - PLN (STT-PLN)

KILAT	VOL.5	NO.1	HAL. 1 - 77	APRIL 2016	ISSN 2089 - 1245

IMPLEMENTASI ALGORITMA AES RIJNDAEL 128 PADA APLIKASI PENGAMANAN PENGIRIMAN SMS (*SHORT MESSAGE SERVICE*) BERBASIS DESKTOP

[1)]Mahmud Didi Nugraha, [2)]Safitri Juanita
[1)]Program Studi Teknik Informatika,Fakultas Teknologi Informasi, Universitas Budi Luhur
[2)]Program Studi Sistem Informasi,Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
e-mail : m.didinugraha94@gmail.com

ABSTRACT

Delivery secret information in a short message with SMS is not secure. This is case study research on UPT Pendidikan XII Kemang Bogor which is part of government intitution on education and culture of republic Indonesia which has responsibility for supervision business processes in public schools, one of the existing business processes in UPT are sending confidential information such as schedule unannounced inspections for supervisor ln public school without any security on the SMS, so easy to read by anyone. So, we need a security application in order for the SMS messages sent can be kept confidential. One way to secure the message is to use cryptographic, this technique wil encode message before sent (encrypt) and people who will receive message have to open message with key (decode). The algorithm used in this application is AES Rijndael algorithm 128. This application using system development life cycle Waterfall and using SMS Gateway features. Applications built using Java programming language and uses a MySQL database. Conclusion for this research is implementation AES Rijndael 128 algorithmto SMS security application can protect confidential information that is sent by operator to supervisor Education at UPT Kemang Bogor XIIwithout change message.

***Keywords** : UPT Pendidikan XII Kemang Bogor, SMS Security, Algoritma AES Rijndael 128, SMS Gateway.*

ABSTRAK

Pengiriman informasi rahasia menggunakan pesan singkat melalui media SMS terkendala dengan keamanan pesan rahasia tersebut. Pada penelitian ini dilakukan studi kasus padaUPT Pendidikan XII Kemang Bogor yang merupakan instansi pemerintah yang bergerak di bidang pengawasan terhadap sekolah-sekolah tingkat dasar di wilayah kecamatan Kemang Bogor, salah satu proses bisnis yang ada pada UPT ini adalah mengirimkan informasi rahasia seperti pelaksanaan waktu inspeksi mendadak kepada pengawas menggunakan aplikasi SMS tanpa adanya pengamanan pada SMS tersebut, sehingga mudah untuk dibaca oleh siapapun. Sehingga diperlukan aplikasi pengamanan SMS dengan tujuanagar pesan yang dikirimkan dapat terjaga kerahasiaannya. Salah satu cara mengamankan pesan tersebut adalah dengan menggunakan teknik kriptografi dimana pesan sebelum dikirim, disandikan terlebih dahulu atau dikenal dengan enkripsi dan dikembalikan lagi seperti semula atau dikenal dengan dekripsi oleh penerima pesan. Algoritma yang digunakan pada aplikasi ini adalah algoritma AES Rijndael 128. Aplikasi ini dibangun menggunakan metode pengembangan sistem Waterfalldan menggunakan SMS Gateway pada tahap pembangunannya.Aplikasi dibangun menggunakan bahasa pemrograman java serta menggunakan basis data MySQL. Aplikasi pengamanan SMS menggunakan algoritma AES Rijndael 128 maka pesan yang dikirimkan operator kepada pengawas UPT Pendidikan XII Kemang Bogor dapat terjaga kerahasiaannya, tanpa mengubah integritas dari pesan yang dikirimkan tersebut.

***Kata Kunci** : UPT Pendidikan XII Kemang Bogor,Pengamanan SMS, Algoritma AES Rijndael 128, SMS Gateway.*

1. PENDAHULUAN

1.1. Latar Belakang

UPT Pendidikan XII Kemang merupakan instansi pemerintah yang bergerak di bidang pengawasan terhadap sekolah-sekolah di wilayah kecamatan Kemang Bogor. Dalam melaksanakan kegiatannya, ada informasi rahasia mengenai waktu pelaksanaan SIDAK (Inspeksi Mendadak) yang harus di infokan oleh kepala UPT Pendidikan XII Kemang kepada jajarannya melalui fasilitas SMS (*Short Message Service*). Sehingga diperlukan suatu aplikasi pengamanan pengiriman SMS (*Short Message Service*), agar informasi rahasia tersebut tidak dapat dibaca terutama oleh sekolah-sekolah yang akan dikenakan SIDAK, sehingga tidak mengganggu pelaksanaan kegiatan dari UPT Pendidikan XII Kemang.Oleh karena itu, diperlukan sebuah aplikasi pengamanan pengiriman SMS (*Short Message Service*) dengan menggunakan Algoritma AES Rijndael 128 sehingga informasi penting dan rahasia dapat terkirim dengan aman kepada staf UPT Pendidikan XII Kemang.

1.2. Permasalahan

Bagaimana mengimplementasikan enkripsi dan dekripsi SMS pada Aplikasi Pengamanan Pengiriman Pesan SMS *Gateway* dengan menggunakan algoritma AES Rijndael 128, sehingga pesan yang dikirim dan diterima dapat di-enkripsi dan di-dekripsi tanpa merubah isi dari pesan yang asli ?

1.3. Tujuan Penulisan

Tujuan dari penelitian ini adalah untuk menghasilkan aplikasi yang dapat menyembunyikan informasi rahasia dari Kepala UPT ke jajarannya dan dapat diterapkan di semua *handphone* yang mendukung aplikasi SMS serta memberikan kontribusi ilmu pengetahuan di bidang teknologi informasi terutama topik Keamanan Data.

1.4. Batasan Permasalahan

Agar permasalahan menjadi terarah dan sesuai dengan sasaran yang ingin dicapai, maka penelitian ini dibatasi pada masalah yang akan dibahas, yaitu: cara membangun dan mengimplementasikan aplikasi pengamanan pengiriman pesan untuk mengamankan pesan rahasia pada UPT Pendidikan XII Kemang Bogor Bogor, mengirim dan menerima pesan, mengenkripsi dan mendekripsi pesan, dengan panjang karakter tiap SMS mencapai 160 karakter.

1.5 Studi Literatur Penelitian Sebelumnya

Melalui studi ini penulis memperoleh data atau informasi dengan mengumpulkan, mempelajari, dan membaca berbagai referensi baik itu dari buku-buku, jurnal, makalah, internet dan bebagai sumber lainnya sebagai berikut:

a. Menurut (Silva, 2013) dalam penelitian yang berjudul Aplikasi Enkipsi Dan Dekripsi *File* Dengan Menggunakan AES Rijndael Pada Sistem Operasi Android. *File* yang telah dienkripsi tidak dapat dibaca lagi dan *file* yang sudah didekripsi bisa dibaca lagi. Algoritma AES yang diterapkan secara Original kurang cocok untuk *file* yang berukuran diatas 300 kB[7].
b. Penelitian yang dilakukan oleh (Sianturi, 2013) yang berjudul Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advance Encryption Standard (AES) menghasilkan aplikasi yang menggunakan teknik pengamanan data teks dengan cara menerapkan metode AES kedalamnya yang bisa mengubah data teks asli ke dalam teks rahasia[8].
c. Menurut (Satria, 2009) dalam penelitiannya yang berjudul Studi Algoritma Rijndael Dalam Sistem Keamanan Data, Algoritma Rijndael sangat peka terhadap perubahan sekecil apapun pada data masukan ini didasarkan pada kenyataan bahwa perubahan kunci akan menyebabkan perubahan data pada saat dikembalikan pada bentuk semula dan algoritma Rijndael mempunyai kunci paling sedikit 128 bit,ini menyebabkan algoritma Rijndael tahan terhadap serangan *exhaustivekey search*[5].
d. Menurut(G. C. Gunawan, 2013)[6] dari hasil uji coba yang dilakukan terhadap program enkripsi dan dekripsi AES dengan menggunakan algoritma Rijndael. Kecepatan enkripsi AES dipengaruhi secara linier oleh besar data dan besar *cipher key* sehingga kompleksitas waktunya adalah (Nb*Nk). Dan penambahan *cipher key* lebih berefek terhadap waktu proses daripada penambahan data[2].
e. Menurut (Surian,2006) dalam penelitian yang berjudul Algoritma Kriptografi Aes Rijndael, Algoritma kriptografi AES Rijndael adalah algoritma kriptografi yang cukup handal hingga saat ini. Pada tahun 2006 *National Security Agency* (NSA) pernah menyatakan bahwa AES cukup aman digunakan untuk mengamankan data-data pemerintahan Amerika Serikat yang bukan tergolong sangat rahasia. Hingga tahun 2006 serangan terbaik terhadap algoritma Rijndael hanya berhasil menembus putaran ke -7 untuk kunci 128 bit[9].

Dari hasil studi literaturpenelitian sebelumnya, terdapat beberapa perbedaan fokus yang ingin penelitian ini capai, dimana dalam penelitian ini lebih berfokus pada keamanan dalam pengiriman pesan dengan memanfaatkan fasilitas SMS yang ada di *handphone.*

2. METODOLOGI PENELITIAN

2.1 Jenis Penelitian

Pada Penelitian ini digunakan jenis penelitian kualitatif. Penelitian kualitatif ini secara spesifik lebih diarahkan pada penggunaan metode studi kasus. Sebagaimana pendapat Lincoln dan Guba (Sayekti Pujosuwarno, 1992: 34) yang menyebutkan bahwa pendekatan kualitatif dapat juga disebut dengan case study ataupun qualitative, yaitu penelitian yang mendalam dan mendetail tentang segala sesuatu yang berhubungan dengan subjek penelitian [4].

2.2 Langkah-Langkah penelitian

Tahapan penelitian menurut (Moleong, 2000) [3] ada 4 tahapan dalam pelaksanaan penelitian, yaitu sebagai berikut :

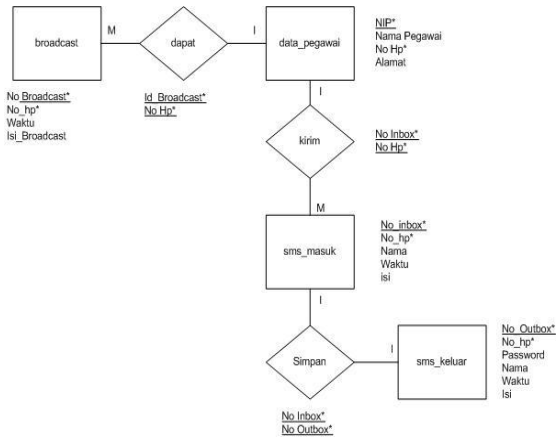
1. Tahap Pra Lapangan
   Pada tahap ini melakukan studi literatur topik kriptografi, mencari tempat sebagai lokasi studi kasus dan mencari subjek sebagai narasumber untuk mengetahui masalah yang bisa diselesaikan menggunakan topik kriptografi. Tahap ini dilakukan pada bulan oktober 2015.
2. Tahap Pekerjaan Lapangan
   Pada tahap ini dilakukan pengumpulan data dilakukan pada bulan November 2015.
3. Tahap Analisis Data
   Pada tahap ini analisa data dilakukan serangkaian proses analisa seperti membuat rancangan basis data, rancangan layar dan membuat desain rancangan layar dan pembuatan aplikasi menggunakan bahasa pemrograman java. Tahap ini dilakukan dari bulan November 2015 sampai bulan Desember 2015.

4. Tahap Evaluasi dan Pelaporan
   Pada tahap ini melakukan proses pengujian aplikasi dengan menguji aplikasi ke user. Tahap ini dilakukan pada bulan Januari 2016.

3. HASIL DAN ANALISA

3.1 Struktur Data yang Digunakan

Dalam pembuatan aplikasi ini digunakan sebuah basis data yang menyimpan semua data yang dibutuhkan untuk kelangsungan proses sistem. Dan dalam pembuatan basis data tersebut dibutuhkan beberapa rancangan. Berikut ini adalah beberapa rancangan yang dibuat.
ERD (*Entity Relationship Diagram*):

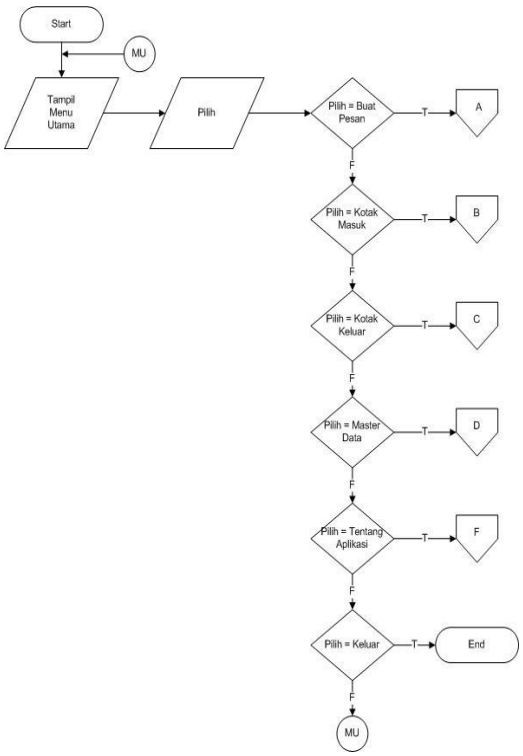


Gambar 1: ERD (Entity Relationship Diagram) Aplikasi

3.2 *Flowchart*

a. Flowchart Menu Utama

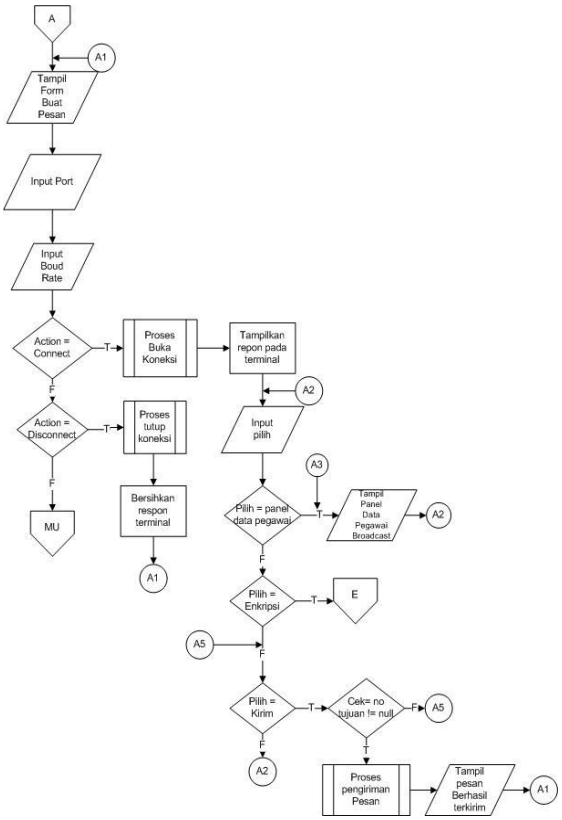
*Flowchart*ini menggambarkan proses pada Menu Utama.



Gambar 2 : Flowchart Menu Utama

b. *Flowchart* Buat Pesan

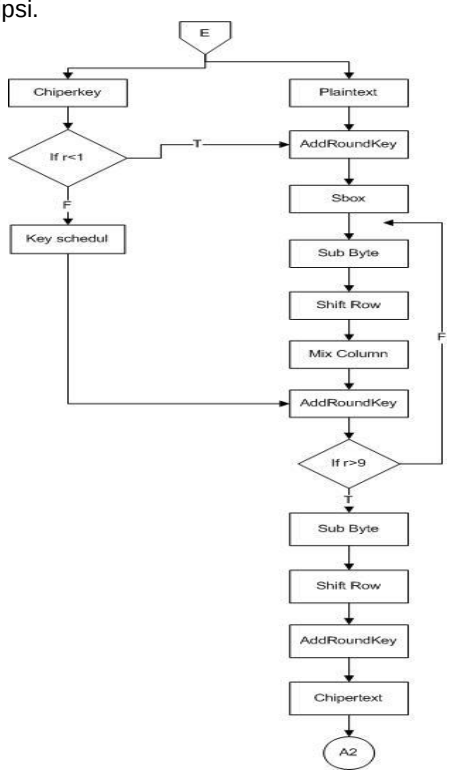
Flowchart ini menggambarkan urutan proses pada menu buat pesan.



Gambar 3: Flowchart Buat Pesan

b. *Flowchart* Proses Enkripsi

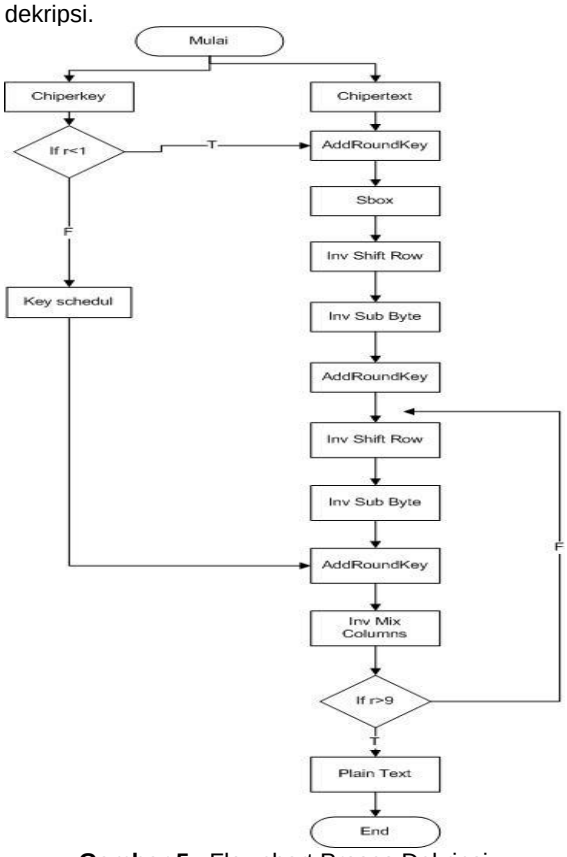
Flowchart dibawah ini menggambarkan proses enkripsi.



Gambar 4 : Flowchart Proses Enkripsi

c. *Flowchart* Proses Dekripsi

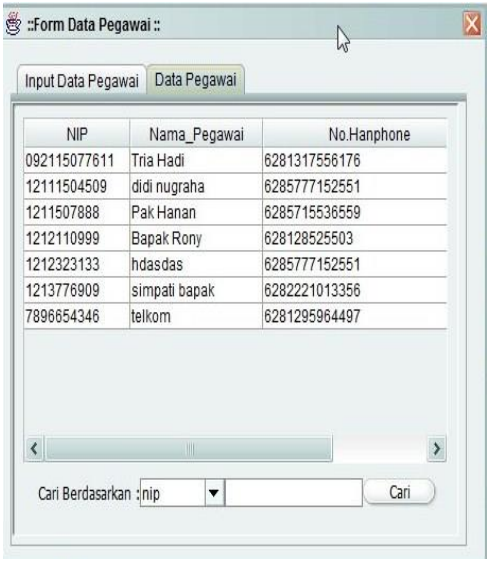
Flowchart dibawah ini menggambarkan proses dekripsi.



Gambar 5 : Flowchart Proses Dekripsi

3.3 **Tampilan Layar Data Pegawai**

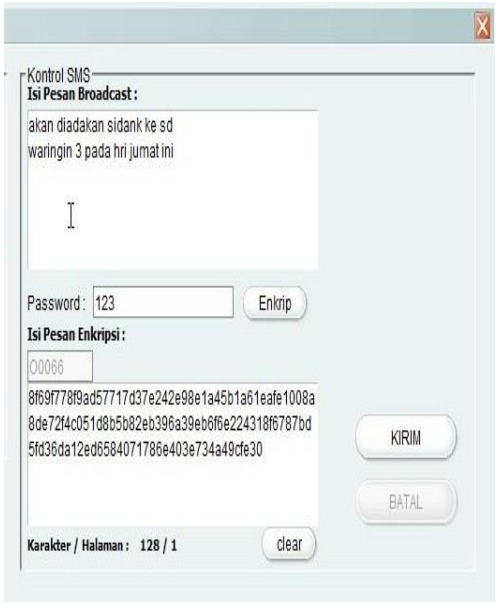
Gambar Berikut adalah tampilan layar *form* data pegawai, dimana *form* ini berisikan *list* pegawai.



Gambar 6: Tampilan Layar Form Data Pegawai

3.4 Tampilan Layar Form Buat Pesan

Gambar berikut adalah tampilan layar form Buat Pesan, dimana pesan asli di-enkripsi sebelum dikirimkan dengan memasukan password dan menekan tombol Enkrip.



Gambar 7: Tampilan Layar Form Buat Pesan

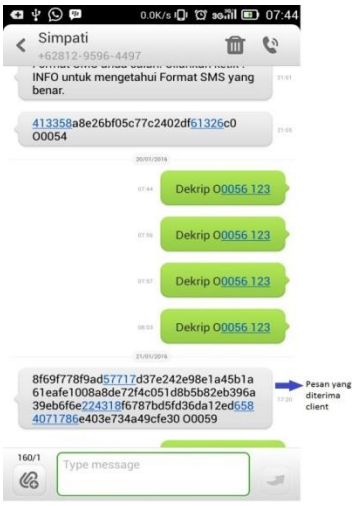
3.5 Tampilan Layar SMS Keluar

Gambar berikut adalah tampilan layar SMS keluar yang berisikan pesan-pesan yang keluar dari *server*.

Gambar 8: Tampilan Layar Form SMS Keluar

3.6 Tampilan Layar SMS Terenkripsi

Hasil SMS yang dikirimkan dalam bentuk *chippertext* atau terenkripsi terlihat seperti dibawah ini :



Gambar 9 : Tampilan Layar Hasil Enkripsi

3.7 Tampilan Layar Pesan Asli

Pesan rahasia atau pesan terenkripsi dapat dibaca dengan mengirimkan format pesan yang benar, berikut tampilan isi pesan asli:

Gambar 21: Tampilan Layar Pesan Asli

4. Kesimpulan

Dari hasil uji coba terhadap aplikasi yang dikembangkan dan perumusahan masalah yang diuraikan maka dapat ditarik kesimpulan bahwa enkripsi dan dekripsi dapat diimplementasikan pada aplikasi pengamanan pengiriman pesan SMS Gateway dengan menggunakan algoritma AES Rijndael 128 tanpa merubah isi dari pesan yang asli.

Adapun saran yang mungkin diperlukan untuk membuat aplikasi ini dapat berjalan lebih baik lagi antara lain, Program aplikasi dapat dikembangkan dengan memperbanyak fitur-fitur untuk memudahkan dalam pengiriman pesan seperti kompresi pesan dan program aplikasi dapat dikembangkan kemanannya dengan menambahkan algoritma yang sama namun metode yang berbeda yakni 192 bit dan 256 bit serta program tidak hanya dapat mengirimkan SMS tetapi juga file.

Daftar Pustaka

[1]. Douglas,Selent. (2010). Advanced Encryption Standard. Rivier Academic Journal 6 (2) : 1-14. Available at :https://www.rivier.edu/journal/ROAJ-Fall-2010/J455-Selent-AES.pdf. di akses : 6/10/2015.

[2]. Gunawan, G.C., A.Saikhu.,R.Soelaiman. (2013). Implementasi Algoritma Rijndael dengan menggunakan kunci enkripsi yang berukuran melebihi 256 Bit. Jurnal Teknik ITS 2(2). Available at : http://ejurnal.its.ac.id/index.php/teknik/article/view/3867. Tgl.akses:12/10/15.

[3]. Moleong, Lexy J. (2000). Metodologi Penelitian Kualitatif. Bandung : PT.Remaja Rosdakarya. ISBN:979-514-051-5.

[4]. Pujosuwarno, Sayekti. (1994). Bimbingan dan Konseling Keluarga. Yogyakarta: Menara Mas Offset.

[5]. Satria, Eko. (2009). Studi Algoritma Rijndael dalam Sistem Keamanan Data. [Skripsi] . Universitas Sumatera Utara. Available at : http://repository.usu.ac.id/bitstream/123456789/14093/1/09E01151.pdf. di akses : 7/10/2015.

[6]. Stallings, William. (2005). Cryptography and Network Security Principles and Practices.4th edition. Prentice Hall.

[7]. Silva P, L.D., Dessyanto, B.P., Heriyanto. (2013). Aplikasi Enkripsi dan Dekripsi File dengan menggunakan AES (*Advanced Encryption Standard*) Agoritma Rijndael pada Sistem Operasi Android. Telematika 10(1):33-42.

[8]. Sianturi, F.A. (2013). Perancangan Aplikasi Pengamanan Data dengan Kriptografi Advanced Encryption Standard (AES). Jurnal Pelita Informatika Budi Darma 4(1):42-46.

[9]. Surian, Didi. (2006). Algoritma Kriptografi AES Rijndael. Jurnal Teknik Elektro 8(2):97-101.