Perancangan Aplikasi Enkripsi Menggunakan Algoritma AES Berbasis Android

Encryption Application Design Using Android-Based AES Algorithm

Ahyuna[1)], Suryadi Hozeng[2)]

Sekolah Tinggi Manajemen Informatika dan Komputer Dipanegara Makassar
Jl. Perintis Kemerdekaan km.9 Makassar, Telp/Fax: 0411-587194

Ahyuna@ dipanegara.ac.id[1)], Suryadi_hozeng@hotmail.com[2)]

Abstrak – Perkembangan teknologi telepon seluler saat ini sudah sangat pesat dan maju. Akhir-akhir ini sedang berkembang teknologi ponsel pintar (*smartphone*) yang membuat ponsel tidak hanya digunakan untuk menelpon atau mengirim pesan saja, namun masih ada beberapa kekurangan dari aplikasi tersebut. Jika digunakan secara optimal menggunakan teknologi *smartphone* khususnya *android* yang bersifat *open source*, kita bisa membuat berbagai macam aplikasi terutama pengekripsian pesan yang umumnya berbasis sms maka dalam penelitian ini kami membuat sebuah aplikasi pengengkripsian Pesan Email. Oleh karena itu, enkripsi pesan email berbasis *mobile* android sebagai jembatan keamanan data sudah mulai marak dikembangkan oleh beberapa programmer yang didukung fasilitas yang diberikan oleh android terutama kepada *user* yang tidak perlu lagi mengkhawatirkan keamanan datanya karena sebelum pengiriman data telah di enkripsi terlebih dahulu dengan menggunakan metode algoritma AES.

Kata Kunci : android, algoritma AES

Abstract – The development of cellular telephone technology at this time has been very rapid and advanced. Lately, smartphone technology (smartphone) is developing which makes cell phones not only used to call or send messages, but there are still some shortcomings of the application. If used optimally using smartphone technology, especially Android, which is open source, we can make a variety of applications, especially encrypting messages that are generally based on SMS, so in this study we created an Email Message encrypting application. Therefore, the encryption of e-mail messages based on Android mobile as a data security bridge has begun to be developed by several programmers supported by the facilities provided by Android, especially to users who no longer need to worry about data security because before sending data has been encrypted using the method AES algorithm.

***Keywords** : android, algorithm AES*

PENDAHULUAN

Pada awal perkembangannya, arus informasi yang semakin marak untuk menggunakan media digital, bagi pihak–pihak perusahaan institusi dan terutama menjaga keamanan data atau organisasi tersebut agar terhindar dari gangguan orang lain yang mempunyai pesan ataupun hal yang ingin disampaikan secara rahasia dan penting. Salah satu teknik untuk pengamanan data adalah dengan menggunakan algoritma penyandian data. Algoritma penyandian data saat ini semakin banyak jumlahnya, sejalan dengan berkembangnya ilmu yang mempelajari penyandian data tersebut, ilmu ini biasa di sebut Kriptografi.

Kriptografi adalah ilmu yang digunakan untuk menjaga keamanan dari pihak yang tidak memiliki hak akses terhadap suatu data, baik data berupa *e-mail*, dokumen, maupun berkas pribadi (Ariyus, 2008). Aplikasi keamanan data ditujukan untuk membantu mengatasi masalah keamanan pesan yang dikirimkan melalui email ataupun pesan password yang terenkripsi dari sebuah dokumen yang dikirimkan, sehingga orang lain tidak dapat mengetahui isi dari pesan – pesan ataupun pesan password dari sebuah file yang dikirimkan tersebut, oleh karena itu dilakukan proses penyandian (enkripsi dan dekripsi) terhadap pesan email yang dikirimkan. Enkripsi dilakukan pada saat sebelum pengiriman dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia. Enkripsi dapat diartikan sebagai kode atau *cipher*. Sebuah *cipher* menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (*stream*) bit dari suatu pesan asli (*plaintext*) menjadi *cryptogram* yang tidak dimengerti.

Email merupakan salah satu teknologi yang sangat bermanfaat baik sebagai media komunikasi ataupun pertukaran data dalam dunia maya dimana penggunaannya lebih mudah dan lebih cepat

dibandingkan mail pada dunia nyata. Email memberikan informasi yang sangat penting terhadap penggunaannya dan media yang dapat menjadi pertukaran data sehingga dibutuhkan suatu tingkat pengamanan data sehingga data tidak mudah disadap dan disusupi oleh pihak lain. Oleh sebab itu, keamanan pesan email yang bersifat rahasia sangat diperlukan, dan metode algoritma AES ini digunakan untuk pengamanan baik dalam proses enkripsi dan deskripsi dari pesan email yang dikirimakan dari smartphone.

Ada beberapa penelitian yang sebelumnya dilakukan mengenai Algoritma AES, dalam upaya mengembangkan dan menyempurnakan pengembangan Algoritma AES ini perlu dilakukan studi pustaka (*literature review*) sebagai salah satu dari penerapan metode penelitian yang dilakukan, diantaranya seperti Penelitian yang dijalankan oleh (Da Silva & Heriyanto, 2015) di TELEMATIKA Universitas Pembangunan Nasional "Veteran" Yogyakarta dengan judul "Aplikasi Enkripsi dan Dekripsi file Dengan Menggunakan AES (*Advanced Endryption Standard*) Algoritma Rijndael Pada Sistem Operasi Android" algoritma ini telah banyak digunakan dalam maslah enkripsi baik itu untuk teks, file maupun database. Metode yang digunakan dalam perancangan dan pembuatan perangkat lunak ini adalah metode GRAPPLE (Guideliness for Rapid Application Engineering). Adapun Penelitian lainnya dilakukan oleh (Zulham, Kurniawan, & Rahmad, 2017) di Seminar Nasional Informatika STMIK Potensi Utama dengan judul "Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6 Berbasis Android" Masalah pengiriman data email ataupun pesan telah menjadi masalah penting pada era teknologi informasi seperti saat ini. Kriptografi merupakan salah satu alat keamanan yang digunakan disegala bidang keamanan. Untuk itu perlunya sebuah keamanan dengan cara enkripsi dan dekripsi data email menggunakan algoritma kriptografi Rivest Code 6 (RC6). Selain penelitian diatas ada juga penelitian lainnya yang dilakukan oleh (Rosyadi, 2012) pada TRANSIENT Jurnal Ilmiah Teknik Elektro, dengan judul "Implementasi Algoritma Kriptografi AES untuk Enkripsi dan Dekripsi Email" Algoritma kriptografi AES digunakan untuk proses penyandian email. Pada apalikasi ini menggunakan bahasa pemrograman Java dan Netbeans 7.0 sebagai perangkat lunak. Server mail yang digunakan adalah google mail dan menggunakan port 465, kunci yang digunakan menggunakan kunci 128 bit sehingga hanya ada 10 putaran kunci.

METODOLOGI PENELITIAN

Pengumpulan data merupakan metode yang difungsikan untuk memperoleh informasi – informasi atau data-data terhadap kasus yang menjadi permasalahan dalam penelitian ini. Hal yang dibutuhkan oleh penulis adalah informasi – informasi mengenai metode yang digunakan dalam penelitian kasus ini. Ada dua pendekatan yang digunakan untuk memperoleh informasi – informasi ini, diantaranya adalah :

1. Studi literatur
   Berupa pencarian sumber – sumber bacaan yang dapat menunjang topik dan sebagai landasan teoritis yang lebih meyakinkan. Sumber bacaaan yang dapat menjadi sumber referensi tersebut berupa text book, tugas akhir, buku panduan belajar pemrograman, maupun sumber bacaan softcopy yang diperoleh dari media internet.
2. Percobaan dan pengamatan
   Melakukan percobaan pada aplikasi yang dibuat, mengamati perkembangan algoritma aes dari website, dan mencatat alur logika dari pembentukan algoritma AES.

Penelitian ini dilakukan dengan pengembangan sistem dimana tahap – tahap yang dilakukan dalam perancangan sistem sebagai berikut:

1. Pengumpulan Data : mengumpulkan informasi yang dilakukan secara langsung ketempat penelitian atau melalui studi literatur.
2. Analisis Sistem : penguraian dari suatu aplikasi yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan, kesempatan, hambatan yang terjadi dan kebutuhan yang diharapkan sehingga dapat diusulkan perbaikannya.
3. Perancangan Aplikasi : merupakan strategi untuk memecahkan masalah dan mengembangkan solusi terbaik bagi permasalahan serta coding aplikasi.
4. Pengujian Program : mengetahui cara kerja dari aplikasi yang dirancang secara terperinci sesuai spesifikasi dan menilai apakah setiap fungsi atau prosedur yang dirancang sudah bebas dari kesalahan logika.
5. Implementasi : tahap dimana aplikasi siap untuk diterapkan, maka pada kegiatan ini dilakukan pengetesan secara langsung dengan pemakai atau *user* pada priode tertentu, bila pada kegiatan ini

ternyata sistem sudah berjalan dengan baik, maka sistem baru dinyatakan dapat digunakan.

Spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam aplikasi ini adalah sebagai berikut :

A. Hardware, terdiri atas :
   1. Laptop HP G42 dengan spesifikasi :
      a. Processor Intel Core i3
      b. VGA Nvidia Geforce GT520M 1 GB
      c. Harddisk 500 GB
      d. Memori RAM DDR3 2 GB
   2. Smartphone Samsung Galaxy ACE 2 GTI8160 spesifikasi :
      a. *OS : Android Versi 2.3.6 GINGERBREAD.DXLF2*
      b. *Internal SD Card Sandisk 8 GB.*
      c. *Processor Cortex A5 900 Mhz.*

B. Software, terdiri atas :
   a Sistem O*perasi Windows Seven Ultimate x32 bit.*
   b. *Java Development Kit (JDK).*

HASIL DAN PEMBAHASAN

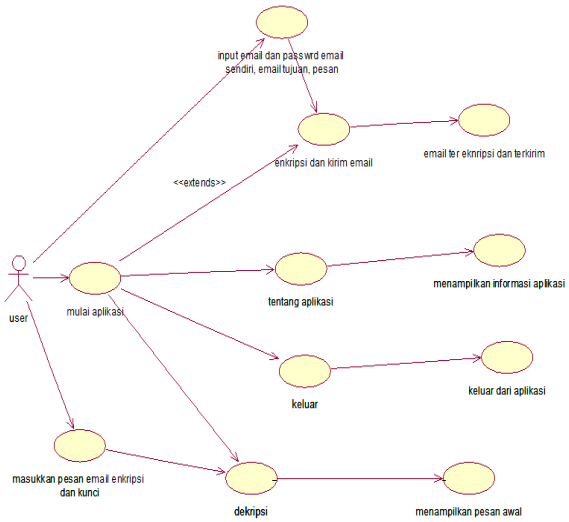
Analisis Sistem

Aplikasi enkripsi email ini adalah aplikasi yang menggunakan algoritma AES dimana algoritma aes menjadi metode untuk mengenkripsi pesan email kemudian di kirim menggunakan email service dan untuk mendekripsi kembali digunakan kunci yang disepakati dalam metode aes pula. Dalam perancangan aplikasi ini dibutuhkan dua unsur utama pada android adalah :

1. *Email Service*
   Menyediakan jasa layanan pengiriman email dalam bentuk mobile dimana aplikasi *mobile* memiliki akun tersendiri yang digunakan untuk mengirim pesan kepada user lainnya yang dituju dalam hal ini *email service* bisa berupa banyak hal antara lain Gmail, Yahoo mail, dan lainnya.
2. Metode AES
   Metode yang digunakan untuk mengenkripsi suatu pesan dimana pesan di enkripsi menggunakan beberapa perhitungan atau round dengan memanfaatkan kunci private yang disepakati oleh kedua pihak agar pesan yang telah di enkripsi tidak dapat dengan mudah di pecahkan oleh orang lain.

Use Case Diagram Aplikasi

Use Case yang dirancang untuk menggambarkan apa yang dilakukan sistem dan siapa saja aktor yang berinteraksi dengan sistem sehingga user dapat memahami tentang aplikasi yang akan dibuat ini.

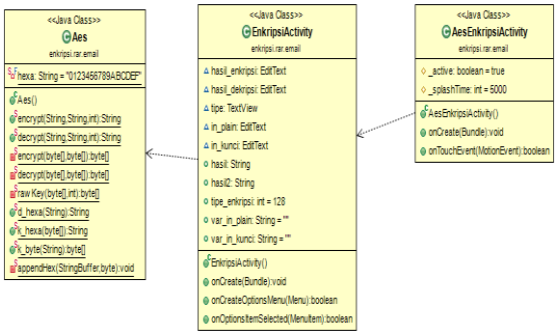


Gambar 1.Use Case diagram aplikasi secara umum

Pada gambar diatas User akan memulai aplikasi lalu memasukkan plain text, keyword lalu menkripsi, setelah kegiatan itu selesai maka dilakukan pengiriman email setelah itu dilakukan maka dapat dilakukan keluar dari aplikasi.

Class Diagram

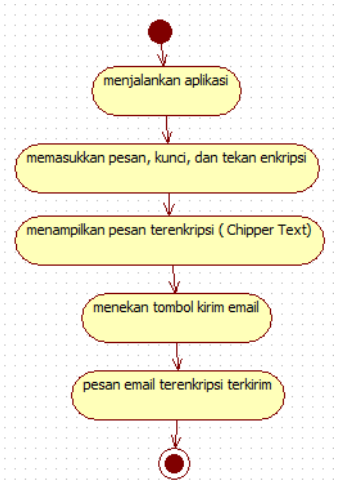
Class Diagram menunjukkan hubungan antarkelas dalam sistem yang sedang dibangun dan bagaimana mereka saling berkolaborasi sehingga membentuk suatu alur program yang ada.



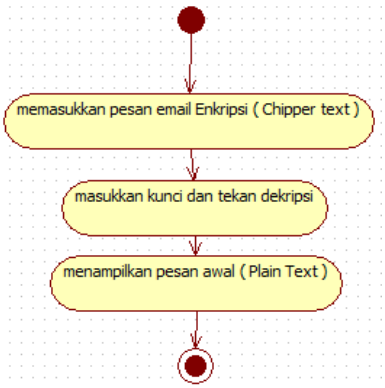
Gambar 2. *Class Diagram*

Activity Diagram

Activity diagram yang dirancang menggambarkan aliran *activity* atau proses dalam sistem yang dirancang. Dalam aplikasi ini dibuat diagram *activity* dimana *activity* adalah diagram untuk enkripsi, dekripsi dan pengiriman email.



Gambar 3. *Activity Diagram* untuk Enkripsi aplikasi Aes *mobile*



Gambar 4. *Activity Diagram* untuk deskripsi aplikasi Aes *mobile*

Rancangan Aplikasi

1. Rancangan Icon Aplikasi
   Gambar dibawah menampilkan aplikasi pada android yang dapat mengoperasikan enkripsi email.

Gambar 5.Rancangan Icon Aplikasi

2. Rancangan Interface index awal aplikasi

Untuk memulai aplikasi enkripsi email AES maka diberikan petunjuk melakukan "Tap untuk memulai "

Gambar 6. Rancangan Interface Awal

3. Rancangan Interface Menu Aplikasi

Gambar 7. Rancangan Interface menu

4. Rancangan Interface saat Enkripsi
   Pada gambar dibawah akan memasukkan plain text dan memasukkan keyword dan melakukan proses enkripsi.

Gambar 8. Rancangan Interface Saat Enkripsi

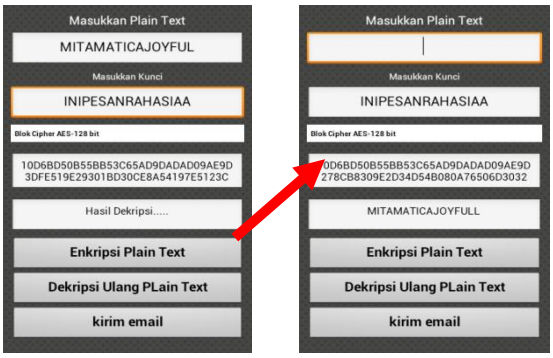
5. Rancangan *Interface* Saat Deskripsi
   Proses pada gambar dibawah memasukkan plain text yang akan dideskripsi dan memasukkan keywordnya lalu menekan deskripsi.

Gambar 9. Rancangan *Interface* Saat Deskripsi

6. Aplikasi melakukan enkripsi data

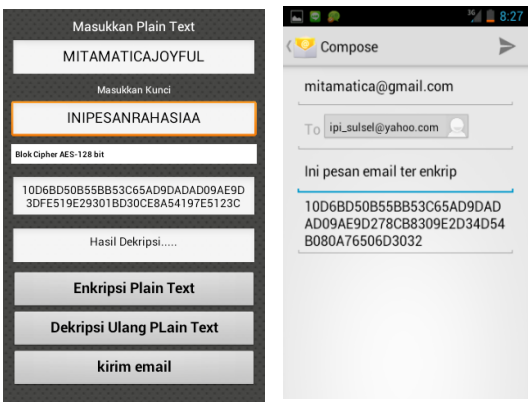
Pada proses enkripsi dapat dilihat dalam simulasi sebagai berikut :

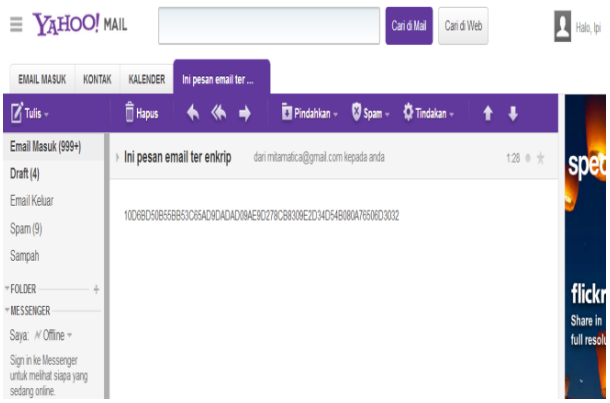
Plaintext : MITAMATICAJOYFULL
Kunci : INIPESANRAHASIAA
Ciphertext : 10D6BD50B55BB53C65AD 9DADAD09AE9D278CB8309E2D34D54B0 80A76506D3032



Gambar 10.Aplikasi melakukan enkripsi data

7. Pengujian Tombol Pengiriman





Gambar 11.Pengujian tombol dan pesan enkripsi

Pada gambar diatas terjadi proses enkripsi dan pengiriman email, lalu menampilkan email yang telah terenkripsi pada email penerima.

KESIMPULAN

Aplikasi yang memberikan layanan keamanan pengiriman pesan email dimana pesan email akan di enkripsi yang kemudian akan dikirimkan melalui *email service*. Maka yang dapat disimpulkan adalah sebagai berikut:

1. Dengan adanya fasilitas yang disediakan oleh Aplikasi ini, maka kami memberikan solusi keamanan pengiriman data dimana pesan email di enkripsi dengan metode AES sehigga data tidak dapat diketahui dengan mudah oleh orang lain karena pengirim dan penerima yang hanya mengetahui kunci pembangkit atau kunci untuk mendekripsi data yang di enkripsi karena menggunakan kedua kunci yang telah disepakati sebelumnya.
2. Pada pengujian sistem yang telah dibuat menggunakan teknik pengujian Black Box, telah diperoleh hasil yang menunjukkan tidak terdapatnya kesalahan pada fungsionalitas dari aplikasi dan dibuktikan dengan hasil yang didapatkan jika menggunakan perhitungan secara langsung atau dengan cara yang manual.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak yang terlibat pada penelitian ini dan kepada rekan-rekan dosen yang mendukung sehingga terselesainya penelitian ini.

DAFTAR PUSTAKA

Ariyus, D. (2008). *Pengantar ilmu kriptografi: Teori analisis & implementasi*. Penerbit Andi.

Da Silva, L., & Heriyanto, H. (2015). Aplikasi enkripsi dan dekripsi file dengan menggunakan AES (Advanced Encryption Standart) Algoritma Rijndael pada sistem operasi Android. *Telematika*, *10*(1).

Rosyadi, A. (2012). Implementasi Algoritma Kriptografi AES Untuk Enkripsi Dan Dekripsi Email. *TRANSIENT*, *1*(3), 63–67.

Zulham, M., Kurniawan, H., & Rahmad, I. F. (2017). *Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6 Berbasis Android*. *1*, 96–101.