APLIKASI ENKRIPSI DAN DEKRIPSI FILE DENGAN MENGGUNAKAN AES (*ADVANCED ENCRYPTION STANDARD*) ALGORITMA RIJNDAEL PADA SISTEM OPERASI ANDROID

[1] Langit Da Silva P., [2] Dessyanto B.P., [3] Heriyanto
[1,2,3] Prodi. Teknik Informatika
Universitas Pembangunan Nasional "Veteran" Yogyakarta
Tambakbayan 2 Babarsari, Yogyakarta
email : dess95@gmail.com

Abstract

Rijndael algorithm is an algorithm that won the contest organized by NIST to replace DES algorithm known weaknesses . After winning the contest Rijndael algorithm , Rijndael lagoitma then serve as the AES (Advanced Encryption Standard) . This algorithm has been widely used in the encryption problem both for text , files , and databases . While Android is an open source operating system developed by Google . Currently Android operating system has become the operating system most widely used on smartphoanes . Smartphones now prevalent and had also been owned by many people because of its reliability. In this final project has been able to be made to solve the problem of software security file on the device that uses the Android operating system using AES (Advanced Encryption Standard) Rijndael algorithm . The method used in the design and manufacture of this software is the method GRAPPLE (Guideliness for Rapid Application Engineering) . The programming language used is Java . In the application can generate an encrypted file that can not be opened . To open the file , then the application can perform the decryption process . The parameters used in the analysis of this algorithm when used for encryption and decryption .

Keywords : Encrypsi, Rijndael, AES, Android

Algoritma Rijndael merupakan algoritma yang memenangkan sayembara yang diselenggarakan oleh NIST untuk menggantikan algoritma DES yang telah diketahui kelemahannya. Setelah algoritma rijndael memenangkan sayembara tersebut, maka lagoitma Rijndael dijadikan sebagai AES (*Advanced Encryption Standard*). Algoritma ini telah banyak digunakan dalam masalah enkripsi baik itu untuk teks, file, maupun database. Sedangkan Android merupakan sistem operasi sumber terbuka yang dikembangkan oleh Google. Saat ini sistem operasi Android telah menjadi sistem operasi yang paling banyak digunakan pada *smartphone*. *Smartphone* sekarang pun juga sudah mewabah dan dimiliki oleh banyak orang karena kehandalannya. Pada tugas akhir ini telah dapat dibuat perangkat lunak untuk menyelesaikan masalah pengamanan file pada perangkat yang menggunakan sistem operasi Android dengan menggunakan AES (*Advanced Encryption Standard*) algoritma Rijndael. Metode yang digunakan dalam perancangan dan pembuatan perangkat lunak ini adalah metode GRAPPLE (*Guideliness for Rapid Application Engineering*). Bahasa pemrograman yang digunakan adalah java. Dalam aplikasi dapat menghasilkan file yang terenkripsi agar tidak dapat dibuka. Untuk membuka kembali file tersebut, maka aplikasi ini dapat melakukan proses dekripsi. Parameter yang digunakan dalam analisis algoritma ini waktu yang digunakan untuk proses enkripsi dan dekripsi.

Kata Kunci : Enkripsi, Rijndael, AES, Android

1. PENDAHULUAN

Perkembangan dunia digital dan teknologi infomasi terutama di bidang perkembangan telepon seluler akhir-akhir ini sangatlah pesat. Perkembangan ini membuat para produsen telepon seluler berlomba-lomba untuk memasarkan produk mereka. Sistem operasi android pun hadir dengan lisensi *open source* dan gratis dan dapat digunakan maupun dimodifikasi oleh produsen teknologi. Hal ini mengakibatkan perang harga dan pada akhirnya banyak telepon seluler canggih dengan harga murah bertebaran di pasaran.

Kecanggihan perangkat dengan sistem operasi android sekarang sudah sangat maju. Perangkat bersistem operasi android sekarang dapat digunakan untuk mengambil foto, video, suara, membuat dokumen, menyimpan data, dan lain sebagainya. Kemampuan perangkat dengan sistem android dalam menyimpan data sekarang semakin baik dengan adanya media penyimpanan yang ukurannya semaikin besar. Bahkan kadang pengguna juga menyimpan data penting di dalam android. Hal ini dikhawatirkan apabila data penting yang tidak dilindungi akan dapat dengan mudah dibaca, atau bahkan disebarluaskan oleh orang yang tidak bertanggung jawab.

Oleh karena itu, dibutuhkan aplikasi yang dapat melindungi data agar tidak dapat dibaca oleh orang lain. Salah satunya adalah dengan metode enkripsi. Algoritma enkripsi yang digunakan adalah algoritma Rijndael, yaitu algoritma yang dirancang oleh Rijmen dan Joan Daemen. Algoritma ini memenangkan sayembara pembuatan AES (*Advanced Encryption Standard*) yang diadakan oleh NIST sehingga algoritma ini sudah teruji kehebatannya.

File yang telah dienkripsi isinya kan menjadi acak dan tidak dapat dimengerti isinya. File tersebut hanya bisa dibaca apabila sudah didekripsi terlebih dahulu dengan menggunakan kata kunci yang benar. Aplikasi enkripsi *file* ini akan membuat keberadaan *file* akan menjadi lebih aman.

Rumusan Masalah

Berdasarkan latar belakang masalah yang ada, maka dapat diambil rumusan masalah yaitu, bagaimana membangun aplikasi enkripsi dan dekripsi file dengan menggunakan AES (*Advanced Encryption Standard*) algoritma Rijndael pada sistem operasi android untuk membantu mengamankan file yang ada di dan membandingkan library yang terbaik untuk diimplemantasikan.

Tujuan Penelitian

Tujuan penulisan ini adalah menghasilkan aplikasi enkripsi dan dekripsi file dengan menggunakan AES (*Advanced Encryption Standard*) algoritma Rijndael pada sistem operasi android untuk membantu mengamankan file yang ada di perangkat dengan sistem operasi android.

2. LANDASAN TEORI

Berikut ini beberapa landasan teori yang digunakan untuk mengembangkan Aplikasi Enkripsi dan Dekripsi dengan Menggunakan AES (*Advanced Encryption Standard*) Algoritma Rijndael Pada Sistem Operasi Android.

Aplikasi

Aplikasi adalah program yang khusus dibuat untuk melakukan suatu pekerjaan atau proses tertentu (Kadir, 2002).

Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani : "*cryptos"* artinya "*secret"* (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi kriptografi berarti "*secret writing*" (tulisan rahasia) (Munir, 2006).

AES (*Advanced Encryption Standard*)

AES (*Advanced Encryption Standard)* menggunakan algoritma Rijndael yang telah memenangkan sayembara terbukan yang dilakukan oleh NIST (*National Institute of Standard and Technology*). Sayembara ini dilakukan untuk menemukan algoritma baru untuk menggantikan algoritma DES (*DataEncryption Standard)* yang dirasa sudah tidak aman lagi (Munir, 2006).

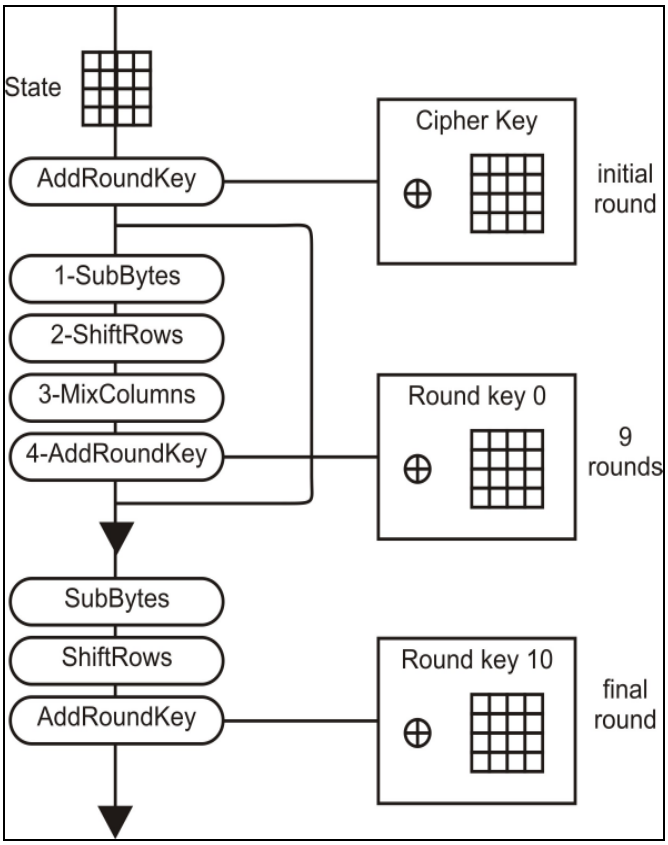
Algoritma Rijndael

Algoritma Rijndael menggunakan substitusi dan permutasi, dan sejumlah putaran (*cipher* berulang), setiap putaran menggunakan kunci internal yang berbeda (kunci setiap putaran disebut *round key*). Rijndael beroperasi dalam orientasi *byte*. Garis besar algoritma Rijndael yang beroperasi pada blok 128 bit dengan panjang kunci 128 bit adalah sebagai berikut (di luar proses pembangkitan *round key*) :

1. *AddRoundKey* : melakukan XOR antara *state* awal (*plintext*) dengan *cipher key*. Tahap ini disebut juga *initial round*.
2. Putaran sebanyak sembilan kali. Proses yang dilakukan pada setiap putaran adalah :
   a. *SubBytes* : substitusi *byte* dengan menggunakan tabel substitusi (*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 dengan *round key*.

3. *Final round* : proses untuk putaran terakhir :
   a. *SubBytes*
   b. *ShiftRows*
   c. *AddRoundKey* (Munir, 2006)



Gambar 1. Diagram Proses Enkripsi AES-128

Android

Android merupakan sistem operasi untuk *mobile* berbasis linux yang mencakup sistem operasi, *middleware*, dan aplikasi. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka. Awalnya Google Inc. membeli Android Inc. yang merupakan pendatang baru yang membuat peranti lunak untuk ponsel/*smartphone.* Kemudian untuk mengembangkan Android makan dibentuklah *Open Handset Alliance,* konsorsium dari perusahaan pembuat peranti keras, peranti lunak, dan telekomunikasi termasuk Google, HTC, Intel, Motorola, Qualcomm, T-Mobile, dan Nvidia (Safaat, 2012).

Diagram *Unified Modeling Language* (UML)

Unified Modeling Language (UML) merupakan system arsitektur yang bekerja dalam OOAD *(Object-Oriented Analysis Design*) dengan satu bahasa yang konsisten untuk menentukan, visualisasi, mengkontruksi dan mendokumentasi *artifact* (sepotong informasi yang digunakan atau dihasilkan dalam suatu proses rekayasa software (Suhendar, 2002).

Eclipse

Aplikasi Android ditulis dan dibangun dengan menggunakan Java, dengan begitu ada beberapa pilihan *Aplication Building Tools*. Baik dengan memakai IDE (*Integrated Development Environment*) atau dengan CLI (*Command Line Interface*). Akan tetapi pada saat ini OHA (*Open Handset Alliance*) dan Google sangat mendukung Eclipse sebagai IDE Java untuk membangun aplikasi android dibandingkan dengan IDE lain. Salah satu bukti adalah dirilisnya plugin ADT (*Android Development Tools*) untuk Eclipse.

Bahasa Pemrgraman Java

Java merupakan bahasa pemrograman yang berorientasi objek, dibuat pertama kali pada tahun 1991oleh James Gosling dan dibantu oleh rekan rekannya di sebuah perusahaan perangkat lunak yang bernama Sun Microsystem. Bahasa pemrograman java selain digunakan untuk *enterprise (*J2EE), dan untuk *desktop* (J2SE), juga dapat digunakan untuk membuat aplikasi pada perangkat *mobile* seperti telepon seluler. Java yang digunakan untuk perangkat *mobile,* sering disebut J2ME (Charibaldi dan Aribowo, 2007).

Pengembangan Sistem

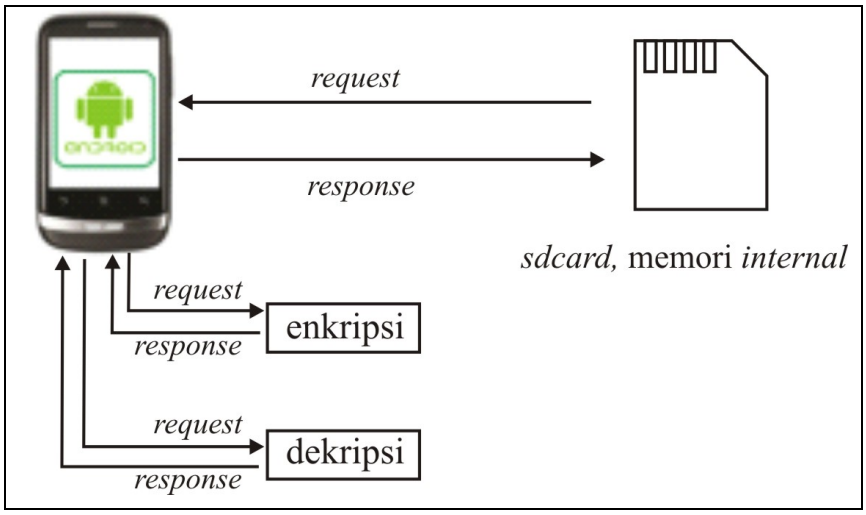
Dalam membangun aplikasi ini, akan digunakan metodologi GRAPPLE (*Guideliness for Rapid Application Engineering*) karena biasanya metodologi ini digunakan untuk mengembangkan aplikasi yang berbasis objek. Metode ini terdiri dari perencanaan kebutuhan, analisis, desain, pengembangan dan implementasi, dan penyebaran. Pada penelitian ini hanya membahas sampai pada tahap pengembangan dan implementasi.

3. ANALISIS DAN PERANCANGAN

Analisis sistem dalam penelitian aplikasi enkripsi ini memaparkan permasalahan yang muncul pada keamanan *file* dan solusi yang diharapkan dapat menyelesaikan masalah tersebut.

Identifikasi Sistem

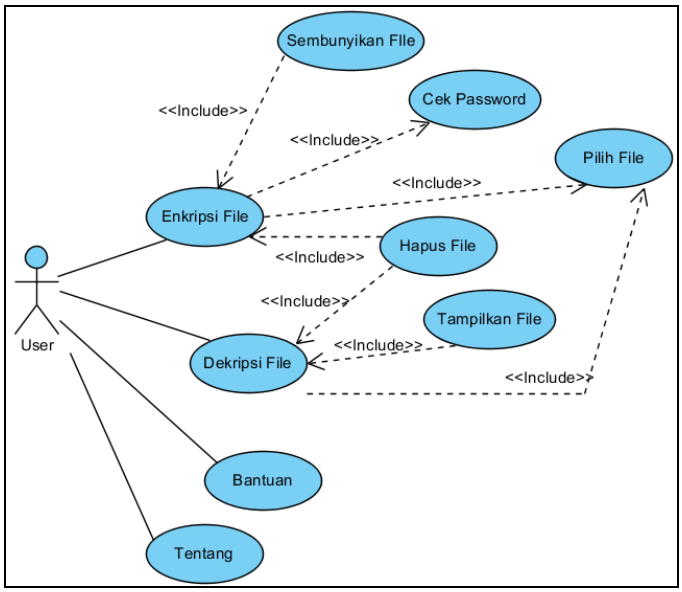
Pada aplikasi ini perangkat keras yang digunakan adalah *smartphone* dengan sistem operasi android versi 2.3 *(*Gingerbread*)* untuk sarana penerapan aplikasi enkripsi dan dekripsi file dengan menggunakan AES (*Advanced Encryption Standard*) algoritma Rijndael berbasis android. Dari identifikasi diatas, maka dapat dilihat arsitektur sistem aplikasi pada gambar di bawah ini.



Gambar 2. Arsitektur Sistem

Analisis Kebutuhan Sistem (Diagram *Use Case*)

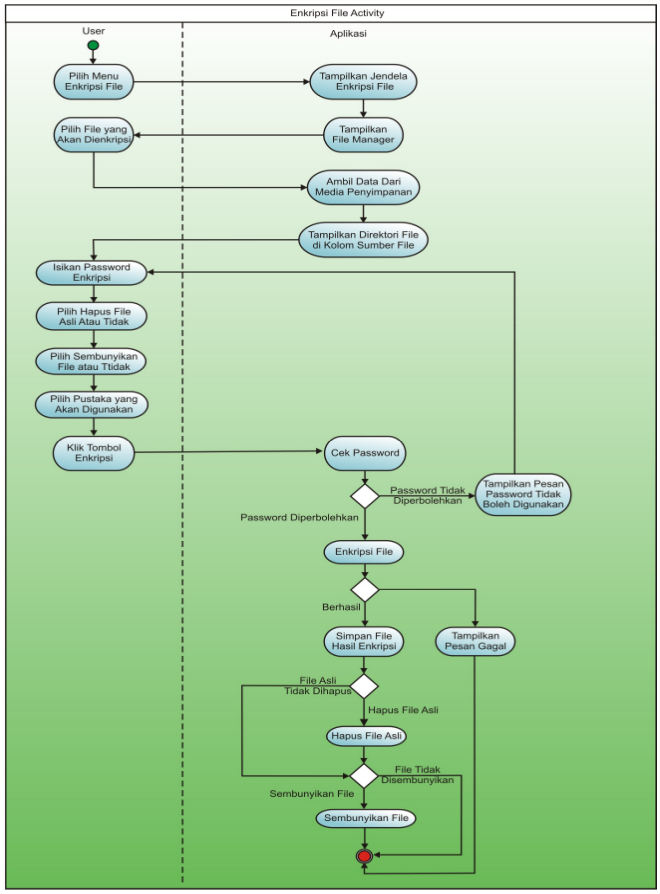
Dalam analisis kebutuhan sistem terdapat satu *user* yaitu *user* dan sembilan *usecase*. User tersebut dapat melakukan enkripsi dan dekripsi file serta dapat juga melihat bantuan dan halaman tentang. Sebelum melakukan proses enkripsi dan dekripsi, *user* harus memilih *file* terlebih dahulu. User juga dapat menghapus *file* asli atau menyembunyikan *file* hasil enkripsi. *Usecase* pada penjelasan diatas dapat dilihat pada gambar 3.



Gambar 3. Diagram *Usecase*

Diagram *Activity* Enkripsi *File*

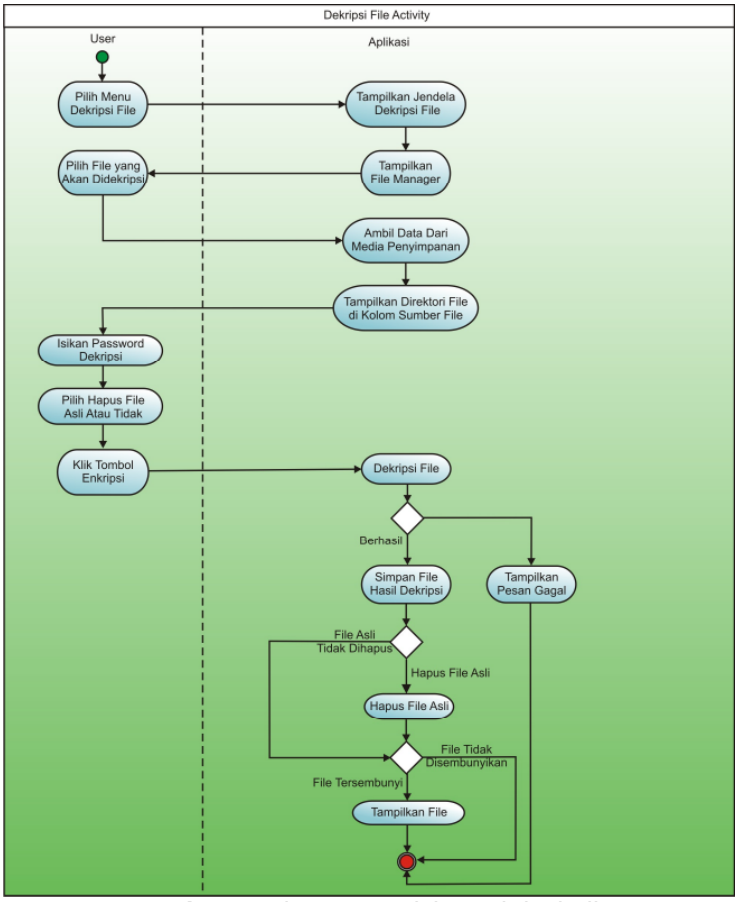
Diagram *activity enkripsi* file memiliki dua *partition* yaitu *user* dan aplikasi. Dalam sistem ini *user* memilih file yang terdapat pada media penympanan, memilih pilihan hapus file asli, sembunyikan file enkripsi dan memilih pustaka yang akan digunakan dan aplikasi akan memprosesnya. Diagram *activity* enkripsi *file* dapat dilihat pada gambar 4.



Gambar 4. Diagram *Activity* Enkripsi File

Diagram *Activity* Dekripsi *File*

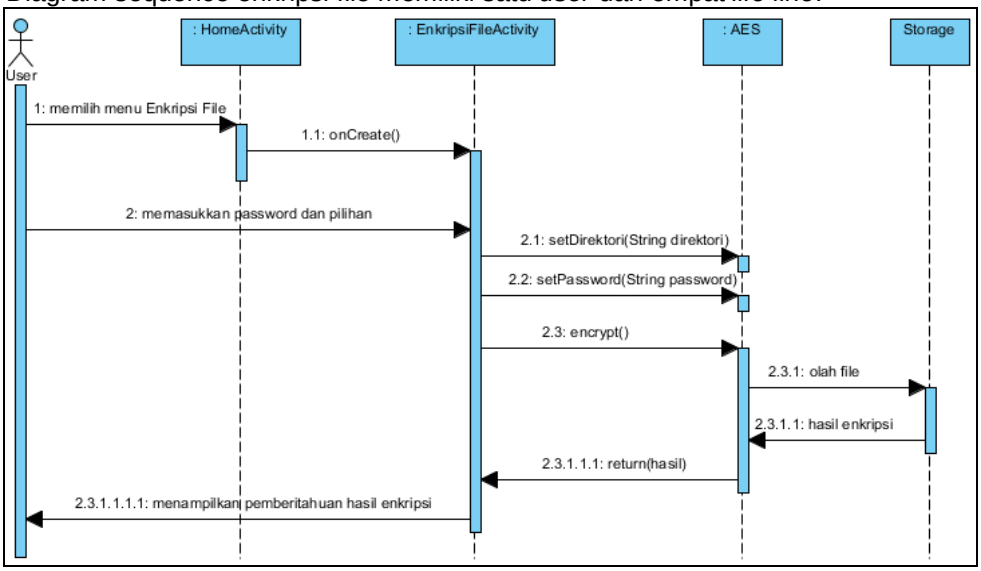
Diagram *activity enkripsi* file memiliki dua *partition* yaitu *user* dan aplikasi. Dalam sistem ini *user* memilih file yang terdapat pada media penympanan, lalu aplikasi akan melakukan proses dekripsi, selanjutnya aplikasi akan menampilkan pilihan penghapusan *file* yang terenkripsi, dan user tinggal meilih pilihan yang disediakan. Diagram *activity* dekripsi file dapat dilihat pada gambar 5.



Gambar 5. Diagram *Activity Dekripsi File*

Diagram Sequence Enkripsi *File*

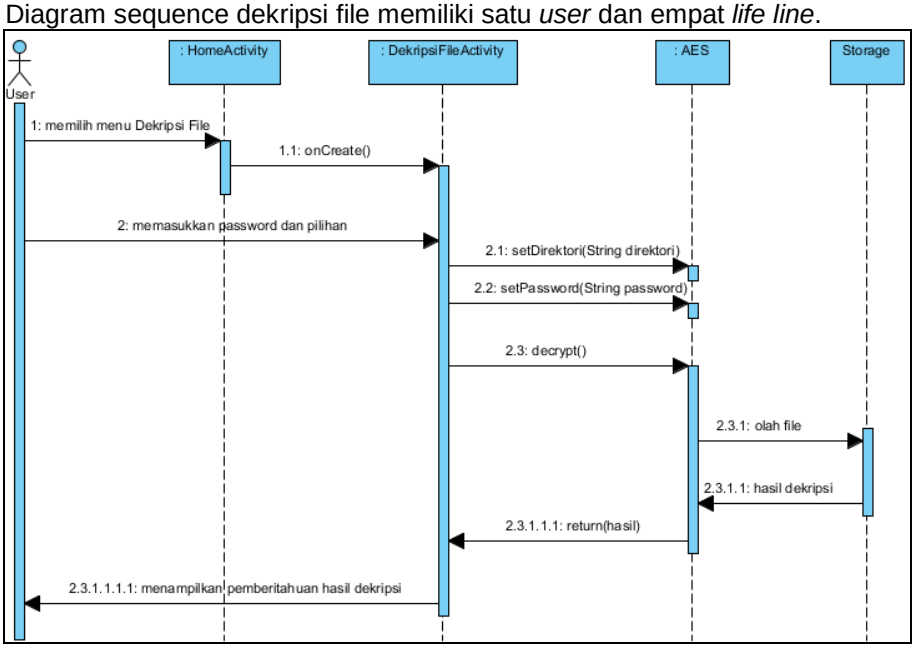
Diagram sequence enkripsi file memiliki satu *user* dan empat *life line*.



Gambar 6. Diagram *Sequence Enkripsi File*

Diagram Sequence Dekripsi *File*

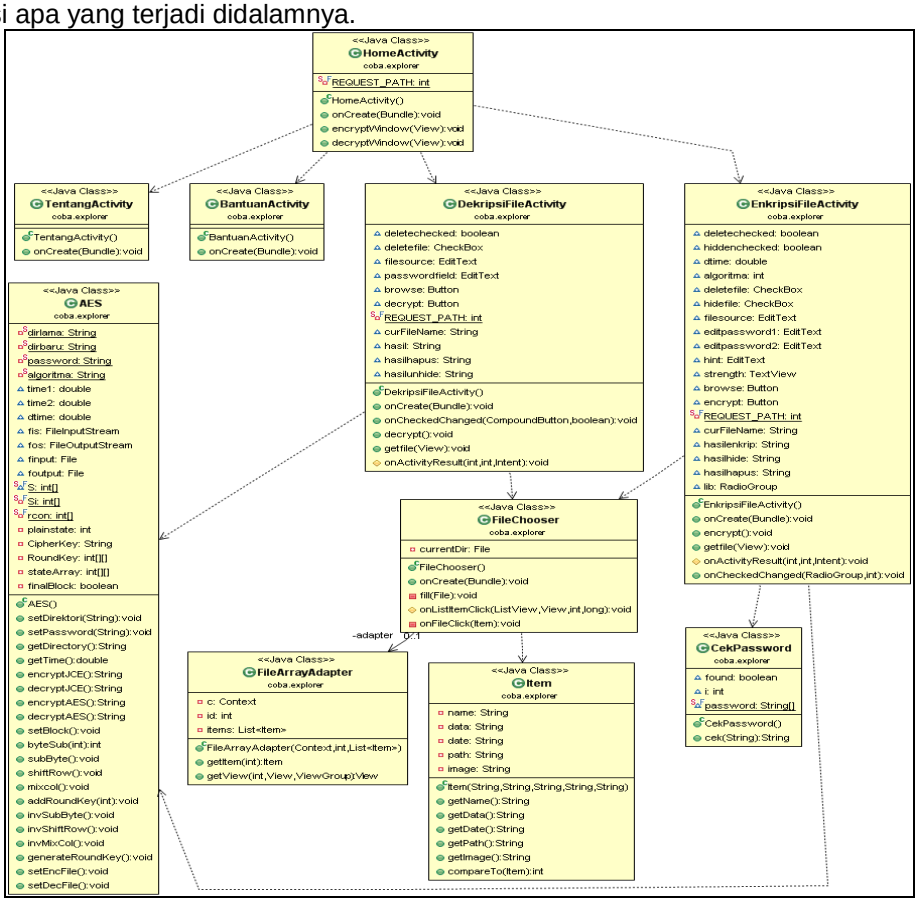
Diagram sequence dekripsi file memiliki satu *user* dan empat *life line*.



Gambar 7. Diagram *Sequence Enkripsi File*

Diagram *Class*

Diagram *class* menampilkan kelas – kelas yang digunakan didalam Aplikasi Enkripsi Dan Dekripsi File Dengan Menggunakan AES (*Advanced Encryption Standard*) Algoritma Rijndael Berbasis Android yang sedang dikembangkan, memberikan gambaran tentang sistem dan relasi apa yang terjadi didalamnya.



Gambar 8. Diagram *Class*

4. IMPLEMENTASI

Pada bab ini akan membahas implementasi dari analisis dan perancangan aplikasi enkripsi dan dekripsi file dengan menggunakan AES (*AdvancedEncryption Standard*) algoritma Rijndael pada sistem operasi android.

Perangkat Keras yang Digunakan

Perangkat keras yang digunakan dalam penerapan aplikasi ini adalah perangkat komputer dengan spesifikasi sebagai berikut :

1. Perangkat : Axioo M540SR
2. *Processor* : Intel Pentium Dual CPU T2330 @ 1,60 GHz (2 CPU)
3. Memori Utama : 894 MB RAM
4. *Hard disk* : 80 GB

Sedangkan perangkat *mobile* yang digunakan untuk menjalankan aplikasi ini adalah :

1. Perangkat : *Smartphone* ZTE Blade
2. *Processor* : 600 MHz ARM 11
3. Memori Utama : 168 MB RAM
4. SD Card : 8 GB *Class* 10

Perangkat Lunak yang Digunakan

Perangkat lunak yang digunakan pada komputer dalam penerapan aplikasi ini adalah sebagai berikut :

1. Sistem Operasi : Windows XP Professional SP2
2. IDE : Eclipse Galileo
3. Android SDK : Android SDK 2.3

Sedangkan perangkat lunak pada perangkat *mobile* yang digunakan untuk menjalankan aplikasi ini adalah sistem operasi Android Gingerbread 2.3.7

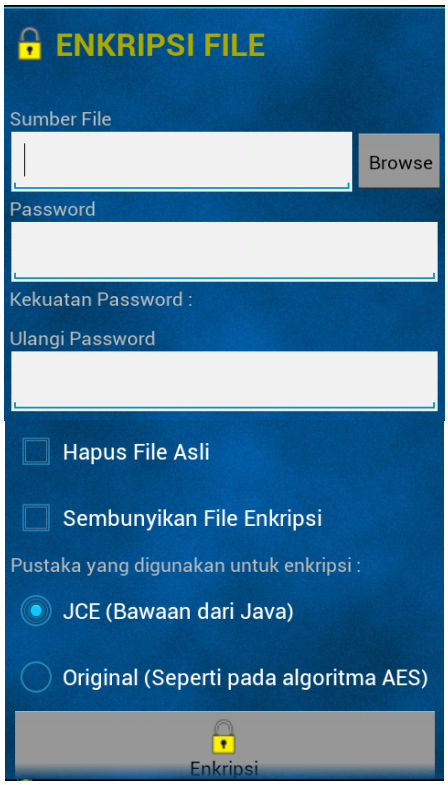
Halaman *Home*

Halaman *home* adalah halaman yang pertama kali ditampilkan saat aplikasi dijalankan.

Gambar 9. Tampilan Halaman *Home*

Halaman Enkripsi File

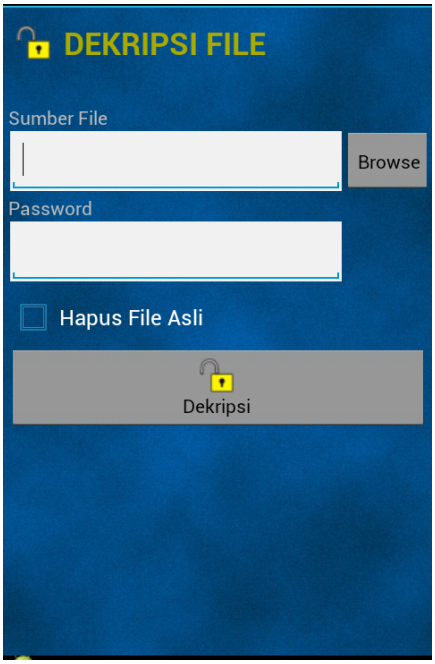
Halaman ini digunakan untuk melakukan proses enkripsi *file*. Halaman ini akan muncul setelah pengguna memilih menu enkripsi file pada halaman *home*.



Gambar 10. Tampilan Halaman Enkripsi File

Halaman Dekripsi File

Halaman ini digunakan untuk melakukan proses dekripsi *file*. Halaman ini akan muncul setelah pengguna memilih menu dekripsi file pada halaman *home*.



Gambar 11. Tampilan Halaman Enkripsi File

5. PENUTUP

Kesimpulan

Penelitian ini berhasil menghasilkan aplikasi enkripsi dan dekripsi file dengan menggunakan AES (*Advanced Encryption Standard*) Algroitma Rijndael pada sistem operasi android. *File* yang telah dienkripsi tidak dapat dibaca lagi. File yang sudah didekripsi kembali dapat dibaca kembali.

Berdasarkan perhitungan waktu, didapat kecepatan rata rata :

1. Proses enkripsi menggunakan library JCE adalah 164.219,185659 bytes per detik.
2. Proses dekripsi menggunakan library JCE adalah 170.583,006914 bytes per detik.
3. Proses enkripsi menggunakan Original adalah 5.421,132320 bytes per detik.
4. Proses dekripsi menggunakan Original adalah 6.923,396380 bytes per detik.

Proses enkripsi dan dekripsi dengan menggunakan metode *Original* memakan waktu yang jauh lebih banyak daripada dengan menggunakan pustaka bawaan dari Java, yaitu JCE (*Java Cryptography Extension*). Algoritma AES yang diterapkan secara Original kurang cocok untuk *file* yang berukuran di atas 300 kB karena waktu yang digunakan sudah di atas satu menit sehingga kurang cocok untuk diterapkan di perangkat *mobile* yang bersistem operasi android.

Saran

Aplikasi ini dapat dikembangan lebih lanjut lanjut lagi, misal dengan memperbaiki tampilan yang lebih bagus, fitur yang lebih banyak bahkan menambahkan fitur penyimpanan secara *cloud*.

DAFTAR PUSTAKA

Charibaldi, Novrido, dan Aribowo, Agus Sasmito, 2007, *Pemrograman Berorientasi Objek dengan Java,* Ardana Media, Yogyakarta.

Dharwiyanti, Sri, dan Wahono, Romi Satrio, 2003, *Pengantar Unified Modelling Language (UML)*, <http://setia.staff.gunadarma.ac.id/Downloads/files/6077/Modul_UML.pdf>, (diakses. 29 Juli 2013)

http://gladman.plushost.co.uk/oldsite/cryptography_technology/rijndael/aes.spec.v316.pdf (diakses 13 Agustus 2013)

Huda, Arif Akbarul, 2012, *24 Jam Pintar Pemrograman Android*, Penerbit Andi, Yogyakarta

Knudsen, Jonathan, 1998, *Java Cryptography,* O'Reilly & Associates, Inc., Sebastopool

Munir, Rinaldi, 2006, *Kriptografi,* Penerbit Informatika, Bandung.

Schmuller, Joseph. (1999). *Sams Teach Yourself UML in 24 Hours*. Sams Publishing, United States of America