BAB III

ANALISA DAN DESAIN SISTEM

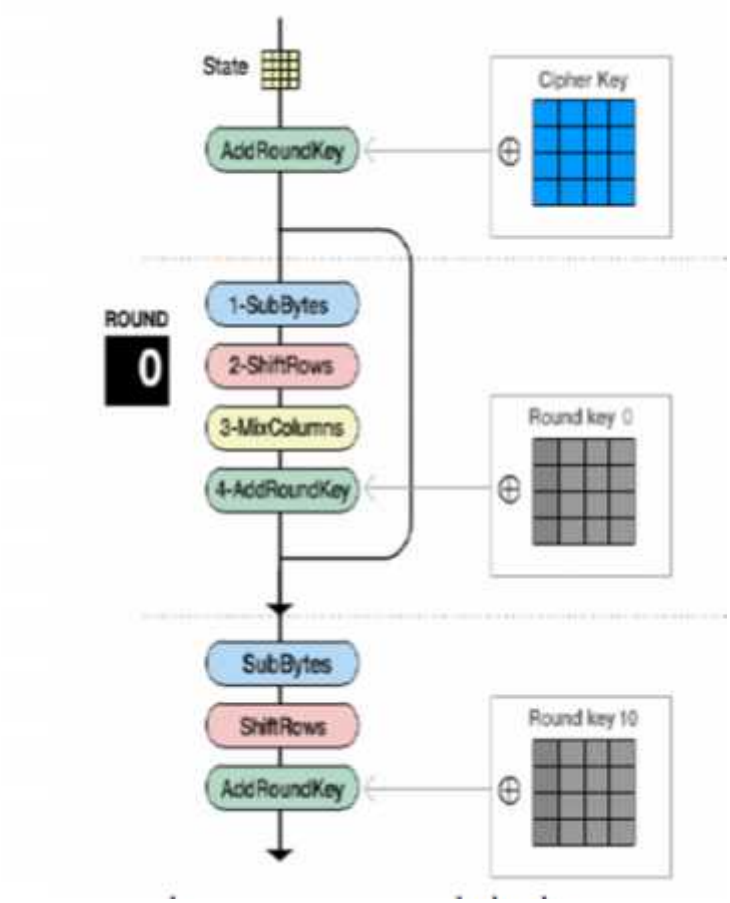
III.1. Analisa Masalah

Pada pembahasan bab ini, akan dilakukan penganalisaan mengenai analisa dan perancangan pembuatan kriptografi" **Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image***". *Image* yang disimpan dalam komputer perlu dilindungi dari akses yang tidak diizinkan, kerusakan/perubahan yang merugikan. Bentuk-bentuk akses yang secara sengaja dapat merusak citra ataupun merugikan pemilik *image* dapat berupa pengeditan citra (merubah bentuk asli), penghapusan dan penyebaran kepada publik sebagai bentuk kejahatan. Pengamanan *image* merupakan aspek dalam jaringan yang mengacu upaya-upaya pengamanan dari akses yang merugikan tersebut. Dalam mengevaluasi suatu proses diperlukan tahap analisis untuk menguji tingkat kelayakan terhadap pembuatan sistem keamanan dengan visual basic 2010. Proses pembuatan aplikasi ini akan dilakukan dan masih dalam tahap perencanaan.

III.2. Penerapan Metode

Pembuatan aplikasi kriptografi ini membutuhkan serangkaian perangkat yang dapat mendukung kelancaran proses pembuatan dan pengujian aplikasi. Berikut ini aspek – aspek yang dibutuhkan dalam pembuatan aplikasi Sistem enkripsi dan dekripsi *file image*.

III.2.1. Algoritma AES



Gambar III.1. Urutan Enkripsi

1. AddRoundKey

Add Round Key pada dasarnya adalah mengkombinasikan chiper teks yang sudah ada dengan chiper key yang chiper key dengan hubungan XOR.

2. Subbytes

Proses SubBytes () memetakan setiap byte dari array State dengan menggunakan tabel substitusi S-Box. Tidak seperti Des S-box berbeda pada setiap putaran, AES hanya mempunyai satu buah S-Box.

3. SiftRows

Proses ShiftRows() ini adalah proses yang sangat sederhana. Pada ShiftRows() melakukan pergeseran wrapping (sikklik) pada 3 baris terakhir dari array state. Jumlah pergeseran bergantung nilai baris (r). Baris r = 1 digeser sejauh 1 byte, baris r = 2 digeser 2 byte, dan baris r = 3 digeser sejauh 3 byte. Baris r = 0 tidak digeser.

4. MixColums

Transformasi menggunakan MixColumns() adalah proses ketiga dalam satu Ronde enkripsi AES

Tabel III.1. Bilangan Polynominal

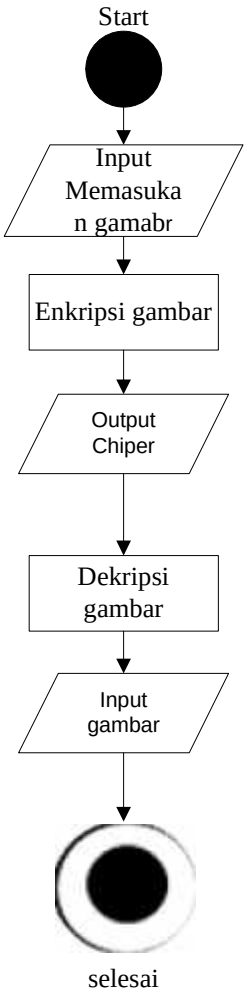
02	**01**	**01**	**03**
03	**02**	**01**	**01**
01	**03**	**02**	**01**

01	**01**	**02**	**03**

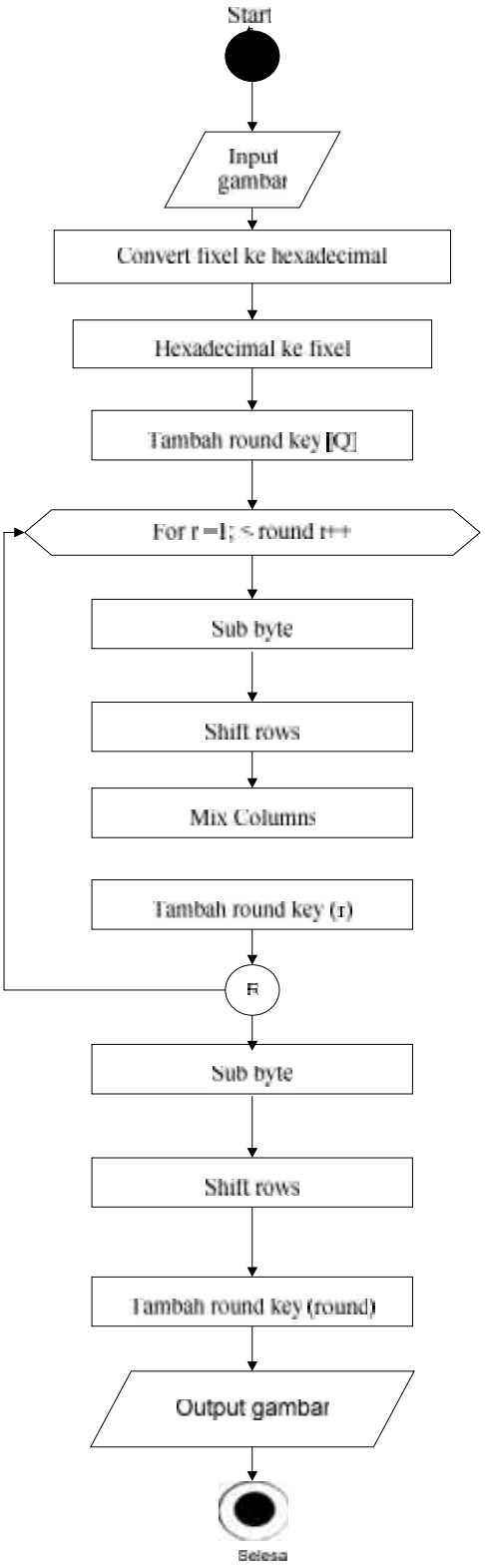
MixColums Transformasi menggunakan MixColumns() adalah proses ketiga dalam satu Ronde enkripsi AES.

III.2.2. Sistem Flowchat

Sistem ini dibangun untuk menjaga kerahasiaan data dengan cara menyisipkan sebuah kunci dan dienkripsi dengan menggunakan metode AES. Pada penelitian, yakni enkripsi dan dekripsi. Berikut flowchart umum tentang Algoritma AES di tunjukan pada gambar di bawah:



Gambar III.2. flowchat sistem enkripsi dan dekripsi gambar



Gambar III.3. flowchat enkripsi dan dekripsi gambar

proses enkripsi dan dekripsi gambar berdasarkan gambar flowchart enkripsi dekripsi gambar :

1. Diambil *file* gambar .
2. *File* gambar dikonvert fixel ke bentuk *hexadecimal*
3. Dilakukan pembentukan dari *hexadecimal* ke fixel
   (bentuk matrik 4x4)
4. Dilakukan proses penambahan *round key* menggunakan *chiper key*.
5. Dilakukan 9 kali perulangan untuk proses *sub bytes, shift rows, mix columns,* dan penambahan *round key*. Pada proses penambahan *round key* menggunakan *chiper key* baru yang sudah dibangkitkan dari proses *key schedule*.
6. Pada iterasi ke-10 dilakukan proses *sub bytes, shift rows*, dan penambahan *round key* ke-10.
7. Dihasilkan gambar hasil enkripsi.

II.2.1 Perangkat Keras (*Hardware)*

Hardware merupakan komponen yang terlihat secara fisik, yang saling bekerjasama dalam pengolahan data. Perangkat keras (*hardware)* yang digunakan meliputi :

a. Notebook
b. Processor AMD Dual-Core C60
c. Harddisk 320 GB
d. Memory 2 GB DDR3
e. Battery 6-cell Li-ion

III.2.2. Perangkat Lunak (*Software)*

Software adalah intruksi atau program komputer yang dapat digunakan oleh komputer dengan memberikan fungsi serta penampilan yang diinginkan. Dalam hal ini, perangkat lunak yang digunakan penulis untuk aplikasi enkripsi dan dekripsi *file image*:

a. Sistem Operasi Windows 7
b. Visual Basic 2010

III.2.3. Unsur Manusia (*Brainware)*

Brainware merupakan factor manusia yang menangani fasilitas komputer yang ada. Faktor manusia yang dimaksud adalah orang – orang yang memiliki bagian untuk menangani sistem dan merupakan unsur manusia yang meliputi :

a. Analisa Sistem, yaitu orang membentuk dan membangun fasilitas rancangan system.
b. *Programmer,* yaitu orang yang mengerti bahasa pemrograman yang digunakan dalam membuat dan membangun suatu program.
c. *Operator* (Administrator), yaitu orang yang mengoperasikan system seperti memasukan data untuk dioperasikan oleh computer dalam menghasilkan informasi dan lain sebagainya.

d. *Public* (Pengguna), yaitu orang yang memakai system yang telah dirancang untuk mendapatkan informasi yang dibutuhkan.

III.3. Analisis Perancangan

Dalam suatu pembangunan aplikasi, analisis perlu dilakukan sebelum tahap perancangan dilakukan. Perancangan aplikasi harus menganalisis kebutuhan apa saja yang diperlukan untuk membangun suatu perangkat lunak.

Bagian desain proyek berarti pengetahuan dan keterampilan mengenai komputer, keahlian dalam perancangan program yang logis melalui informasi, semuanya difokuskan untuk membuat Sesuatu yang nyata. Mendesain berarti berfikir, memilih, membuat, dan mengerjakan.

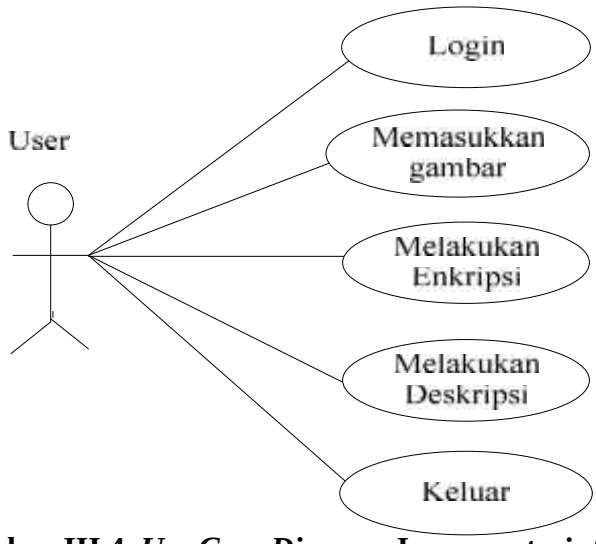
Kebutuhan utama dalam perancangan Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image* perangkat lunak yang digunakan untuk membangun aplikasi yaitu : Visual Basic 2010, Semua kebutuhan itu harus dapat dituangkan ke dalam perancangan agar hasil aplikasi dapat sesuai dengan konsep pembangunan.

III.3.1. Desain Sistem Secara Global

Adapun perancangan dari sistem yang diusulkan atau yang akan dirancang, dalam tahap ini menggunakan *Unified Modeling Language* berupa use case diagram dan class diagram

III.3.1.1 *Use Case Diagram*

Rancangan Aplikasi ini akan dibentuk menggunakan *Use Case Diagram*. Dibawah ini merupakan *use case diagram* Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image.*



Gambar III.4. *Use Case Diagram* Impementasi AES (*Advanced Encyrption Standart*) Untuk Enkripsi Dan Dekripsi *File Image*

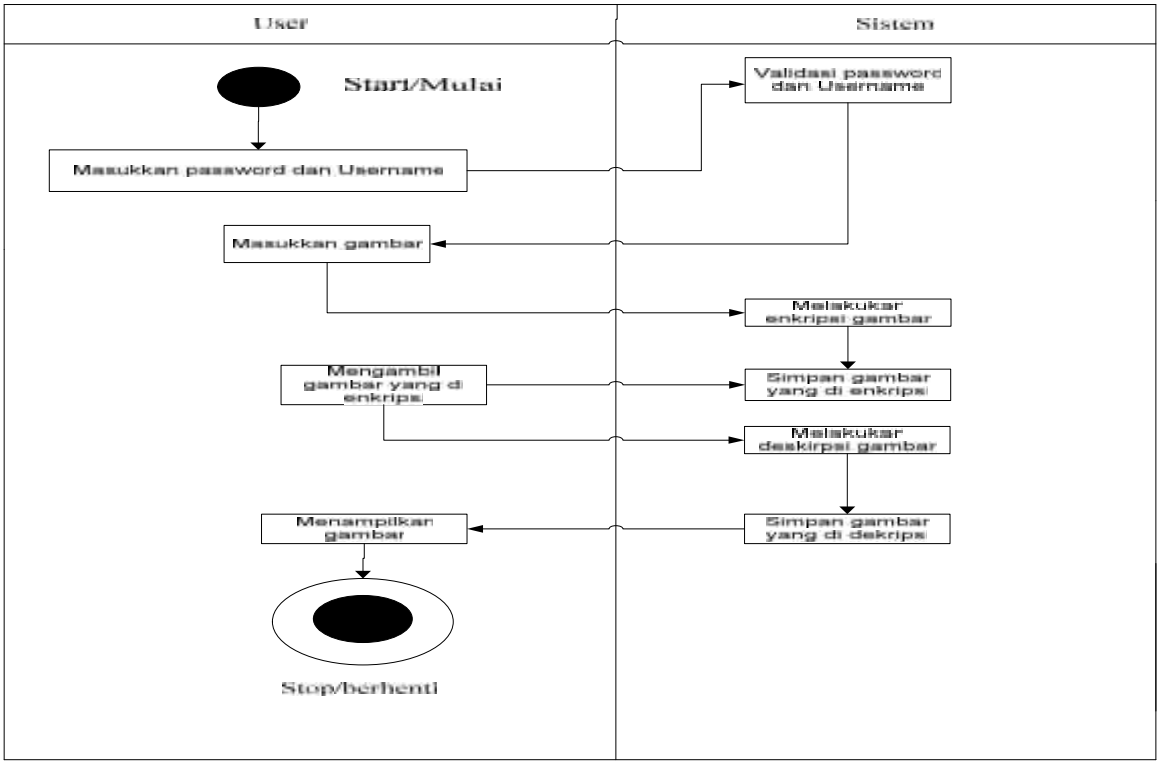
Pada Gambar III.2, merupakan *usecase* diagram dari aplikasi keamanan data pada *image*. *User* yang didefenisikan pada aplikasi ini adalah orang yang menjalankan aplikasi. Ketika aplikasi dijalankan, aplikasi akan menampilkan aplikasi enkripsi dan dekripsi *image*. Setelah tampil, *user* dapat melakukan penginputan data pada kolom yang sudah tersedia dan mengeksekusi perintah.

III.3.1.2 *Activity Diagram*

Activity Diagram menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis

III.3.1.3 *Activity Diagram* Enkripsi dan Deskripsi

Tabel III.2. *Activity* Diagram Enkripsi dan Deskripsi



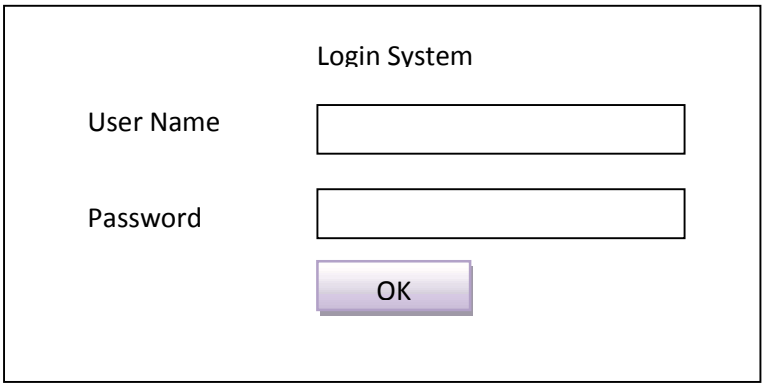
Pada gambar *activity* diagram enkripsi, menunjukkan bahwa hal pertama yang harus dilakukan adalah pengambilan gambar. Setelah tampil, maka lakukan pengenkripsian terhadap gambar yang diinput. Dalam hal ini pengenkripsian dilakukan dengan menggunakan AES. Kemudian data yang sudah dienkripsi dapat disimpan. Pada saat melakukan proses penyimpanan, data tersebut sudah dienkripsi dengan menggunakan AES.

III.3.2. Perancangan Aplikasi

Perancangan tampilan *form* utama dalam program ini sangat diperlukan dalam programan visual karena *form* utama ini merupakan bentuk tampilan saat program dijalankan. Pada Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image* ini terdapat beberapa *form* yang dirancang yaitu :

1. Tampilan *login* Aplikasi Program

Pada tampilan *login* Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image* ini berfungsi sebagai tampilan pertama untuk masuk ke tampilan menu. *login* aplikasi program ini dapat dilihat pada gambar III.5.

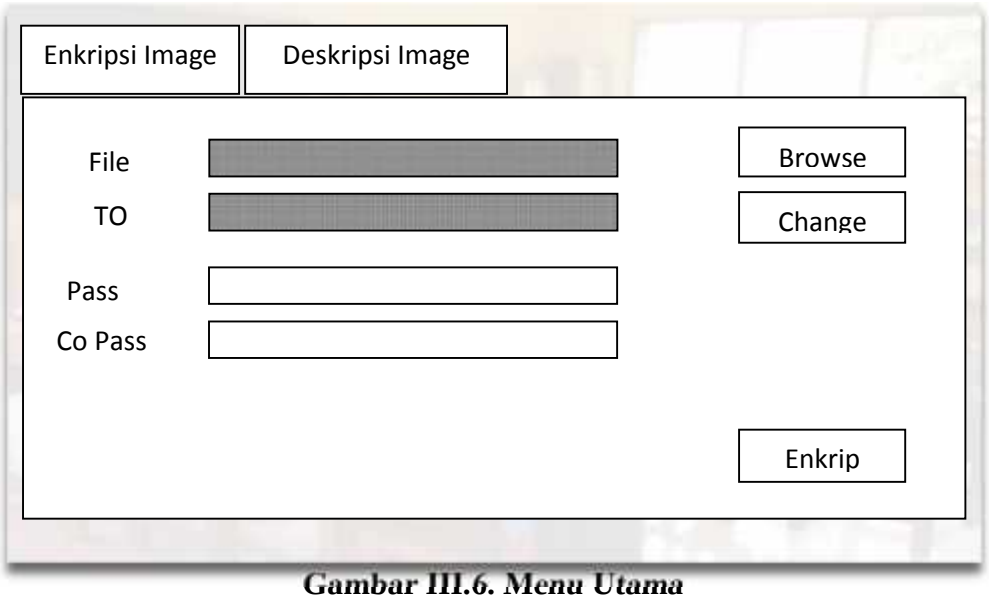


Gambar III.5. Tampilan *Login* Aplikasi Program

Pada gambar III.5. adalah tampilan *login* aplikasi program yang akan pertama kali muncul saat program dijalankan. Fungsi *login* ini untuk masuk ke formUtama

2. Tampilan Form Utama

Pada tampilan from Utama program aplikasi ini berisikan tentang button untuk ke sub – sub menu aplikasi program ini dapat dilihat pada gambar III.6.



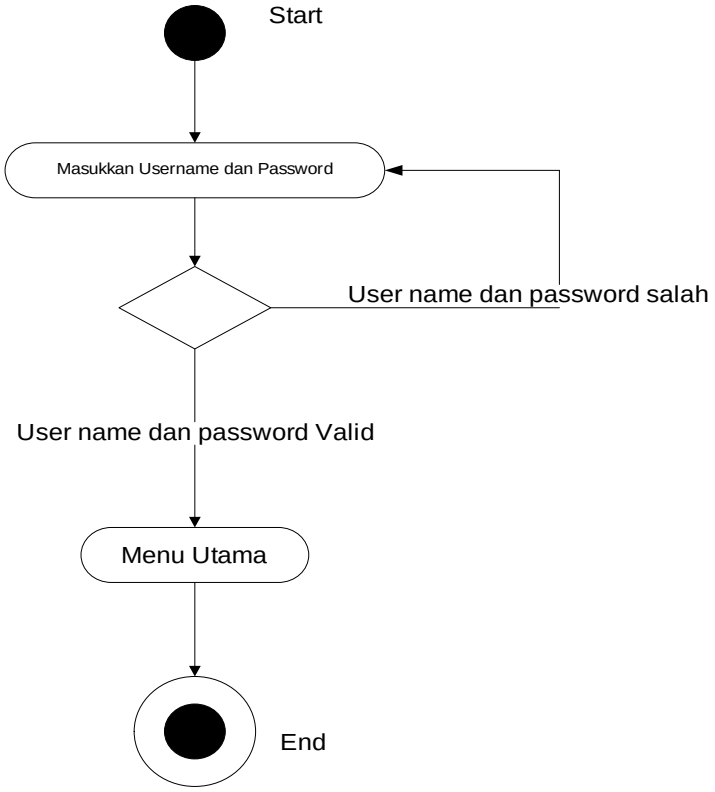
Gambar III.6. Mena Utama

III.3.4 Logika Program

III.3.4.1 *Activity Diagram*

1. *Activity Diagram* Untuk *Login*

Gambar III.7. dibawah ini menggambarkan *diagram activity* untuk *login* ke Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image*.



Gambar III.7. *Diagram Activity Login*

2. *Diagram Activity Input* Data

Berikut ini gambar III.8. merupakan *diagram activity* untuk input data.

Gambar III.8. *Diagram Activity Input* Data

3. *Diagram Activity Edit* Data

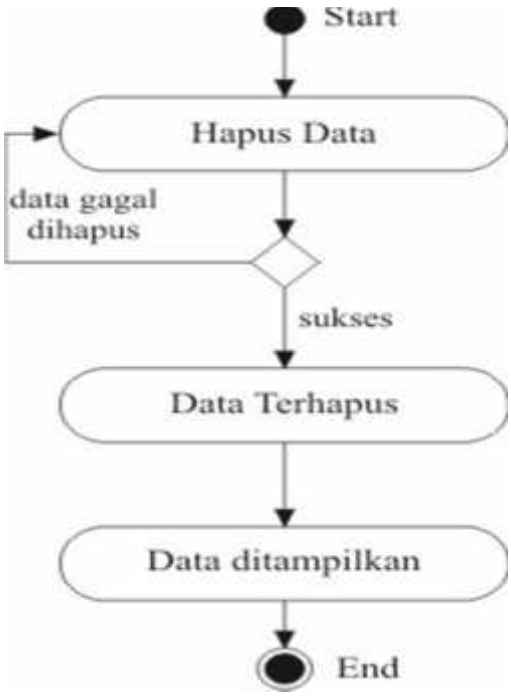
Berikut ini diagram *activity* untuk edit data pada Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image*.

Gambar III.9. *Diagram Activity Edit* Data

Pada gambar III.6. adalah gambar activity edit data yang akan meneruskan kesimpan data jika edit benar, jika salah data nya tidak akan tersimpan dan kembali lagi ke edit data seperti semula.

4. *Diagram Activity* Hapus Data

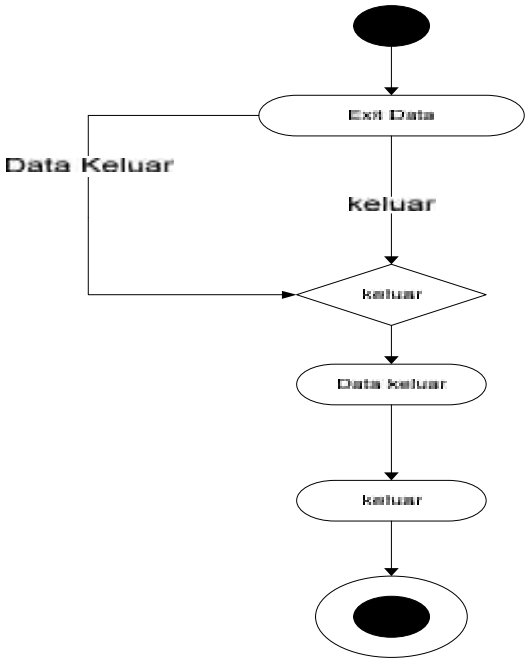
Berikut ini diagram *activity* untuk hapus data pada Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image*.



Gambar III.10. *Diagram Activity* Hapus Data

Pada gambar III.10. adalah gambar activity hapus data yang akan meneruskan ketampilan data jika hapus data benar, jika salah data nya tidak akan terhapus dan kembali lagi ke menu hapus data seperti semula

5. *Diagram Activity* Exit Data



Gambar III.11. *Diagram Activity* Exit Data

Pada gambar III.11. adalah gambar activity exit data yang akan meneruskan ke data keluar jika exit data benar, jika salah tidak bisa keluar dari exit data.