

BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisis Permasalahan

File program acara TV bisa dengan mudah disalah gunakan oleh pihak-pihak yang tidak bertanggung jawab yang seharusnya menjadi program legal dari perusahaan. Pada Kantor TVRI Sumatera Utara terdapat suatu permasalahan dimana sering terjadinya kehilangan suatu data program acara TV yang disebabkan oleh pegawai dalam kelalaiannya menjaga file program acara TV sehingga dapat merugikan dan memperlambat kinerja pada Kantor TVRI Sumatera Utara. Sehingga untuk menjaga keamanan suatu data dari ancaman yang dijelaskan diatas, maka solusi nya diperlukan suatu aplikasi pengamanan data agar terhindar dari gangguan pelaku yang tidak bertanggung jawab. Dimana pelaku yang tidak bertanggung jawab tidak dapat mengetahui isi dari data program acara TV tersebut. Dalam penelitian ini sistem yang akan dibangun adalah mengubah data program acara TV yang terdapat di dalam sebuah file dokumen kedalam bentuk yang tidak dapat dikenali agar kerahasiaannya dapat terjaga

III.2. Strategi Pemecahan Permasalahan

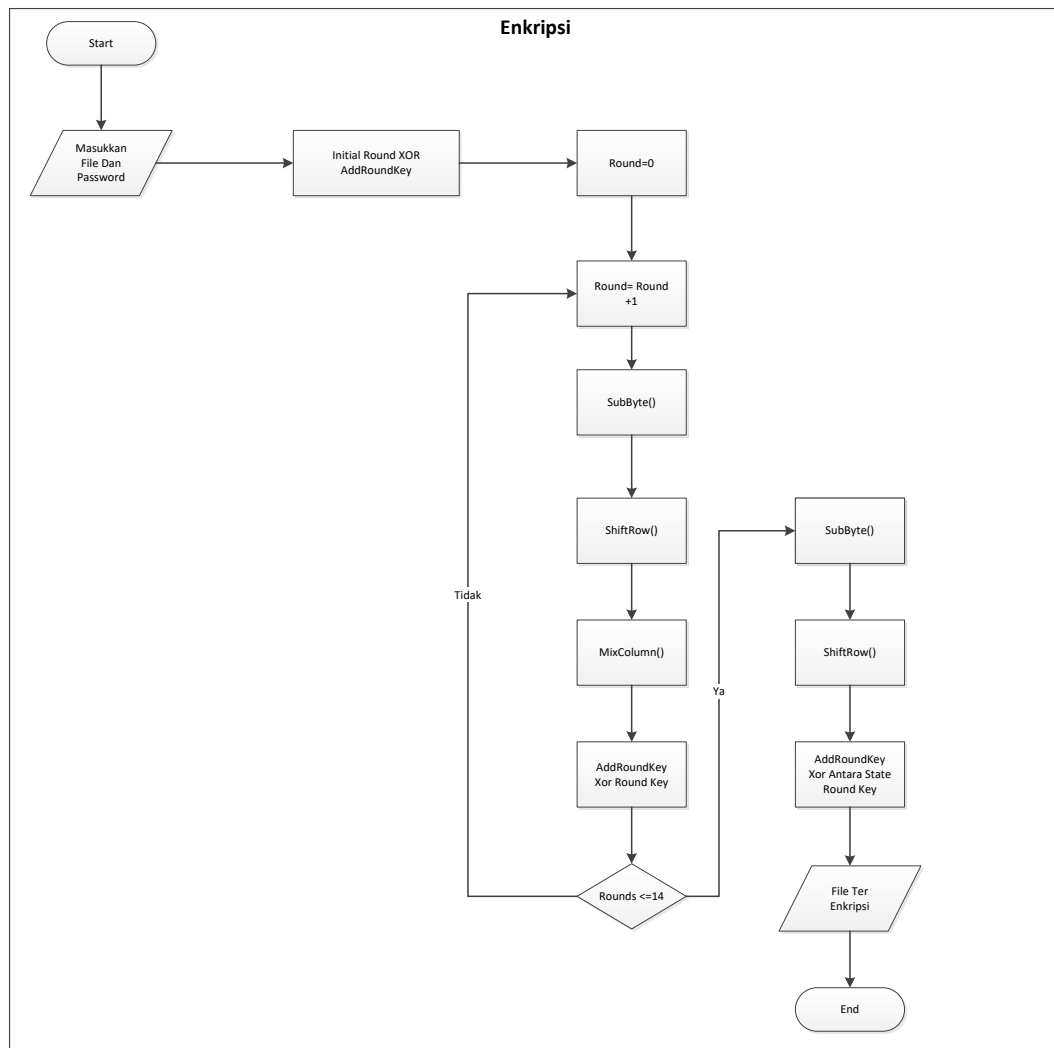
Sebelum melakukan perancangan terhadap sistem, penulis terlebih dahulu melakukan analisa tentang sistem yang akan dirancang. Dalam analisa ini, penulis melakukan analisa mengenai fasilitas apa yang disediakan dalam sistem yang akan dirancang:

Adapun strategi pemecahan masalah dari sistem enkripsi data yang dirancang adalah sebagai berikut :

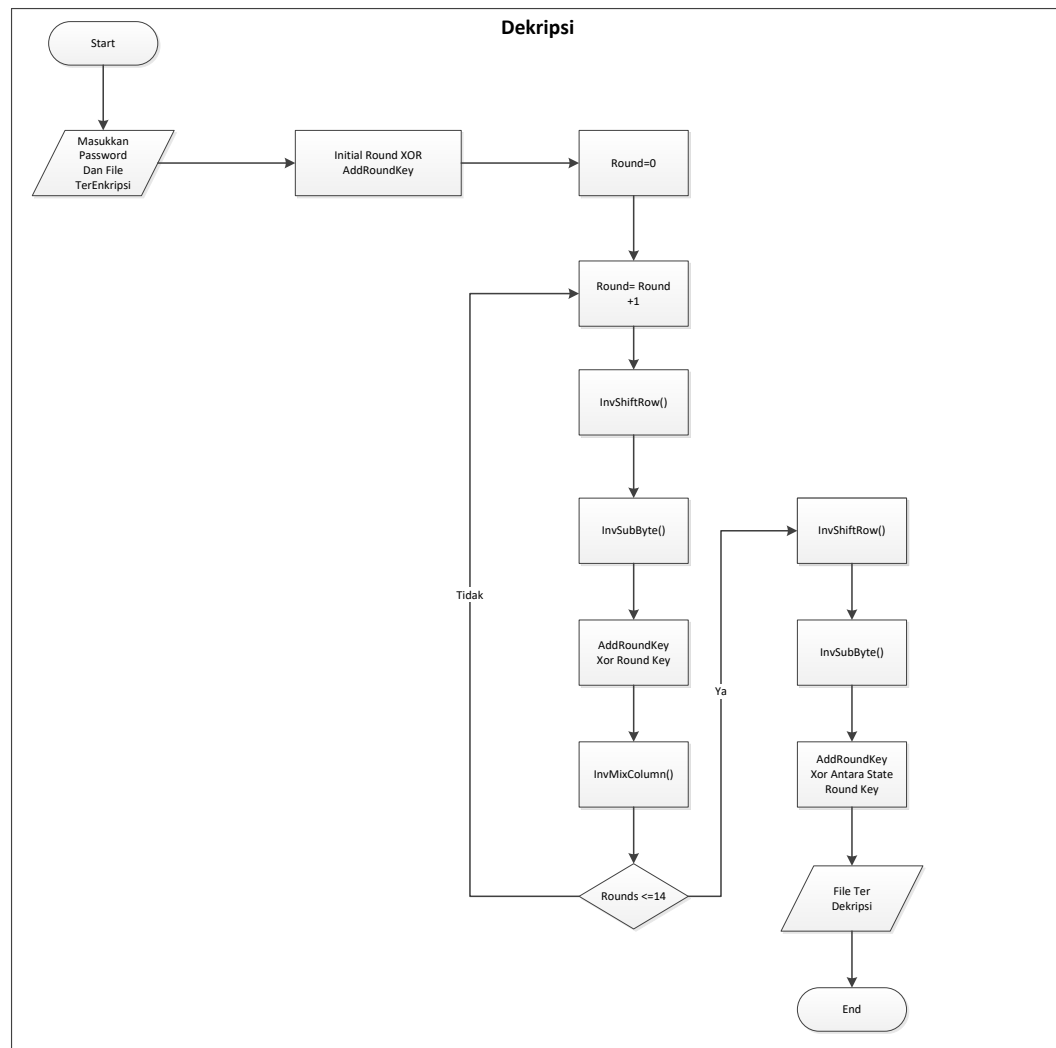
1. Untuk menghindari data dirusak atau dicuri orang lain perlu dibuat sebuah aplikasi yang mengamankan data dalam satu folder, lalu folder tersebut dilakukan enkripsi tetapi bukan folder-nya yang terenkripsi melainkan semua file terenkripsi didalam sebuah folder.
2. Menghasilkan suatu aplikasi yang dapat mengamankan data file dan folder dengan menerapkan Metode AES.
3. Agar data tersebut aman dari kerusakan perangkat keras maka data tersebut harus dipindahkan ke lokasi yang lebih aman misalnya di flashdisk, aplikasi enkripsi data ini sudah dirancang tempat pemindahan file tersebut didalam sebuah folder yang terenkripsi.

III.3. Flowchart Sistem Proses Enkripsi

Pada tahap ini proses dalam aplikasi dibuat sesuai dengan fungsi dari algoritma enkripsi dan dekripsi yang digunakan. Jika langkah-langkah dalam proses enkrip dan dekrip berlawanan dengan fungsi algoritma yang digunakan, maka proses yang di inginkan tidak akan berjalan. Langkah yang harus dilakukan dalam proses enkripsi dan dekripsi digambarkan dalam flowchart berikut :



Gambar III.1. Flowchart Enkripsi AES



Gambar III.2. Flowchart Dekripsi AES

III.3.1 Contoh Kasus Algoritma AES

Berikut ini adalah contoh kasus penggunaan Algoritma AES, untuk lebih jelasnya dapat dilihat sebagai berikut :

Misal, sebuah CipherText sebagai berikut :

CipherText : TwoOneNineTwo

Key : ThatsMyKungFu

Langkah selanjutnya adalah mengubah nama file dan juga kunci kedalam bentuk hexadecimal.

File :

T	w	O	O	n	E	N	I	N	e	T	w	O
54	77	6F	4F	6E	65	4E	69	6E	65	54	77	6F

Key :

T	h	A	T	s	M	Y	K	U	n	g	F	U
54	68	61	74	73	4D	79	4B	75	6E	67	46	75

Langkah selanjutnya yang dilakukan adalah mencari nilai Roundkey pertama, untuk mencari Roundkey pertama dapat dilakukan sebagai berikut :

$$w[0] = (54, 68, 61, 74)$$

$$w[1] = (73, 20, 6D, 79)$$

$$w[2] = (20, 4B, 75, 6E)$$

$$w[3] = (67, 20, 46, 75)$$

$g(w[3])$:

- byte kiri bergeser dari $w[3]$: (20, 46, 75, 67)
- Substitusi Byte (S-Box): (B7, 5A, 9D, 85)
- Menambahkan putaran konstan (01, 00, 00, 00)
- Memberi : $g(w[3]) = (B6, 5A, 9D, 85)$

$$w[4] = w[0] \oplus g(w[3]) = (E2, 32, FC, F1) :$$

0101 0100 1011 0110	0110 1000 0101 1010	0110 0001 1001 1101	0111 0100 1000 0101
1110 0010 E2	0011 0010 32	1111 1100 FC	1111 0001 F1

$$w[5] = w[4] \oplus w[1] = (91, 12, 91, 88)$$

$$w[6] = w[5] \oplus w[2] = (B1, 59, E4, E6)$$

$w[7] = w[6] \quad w[3] = (D6, 79, A2, 93)$

Roundkey pertama : E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

Round0 : 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

Round1 : E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79

Round2 : 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA

Round3 : D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03

Round4 : A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B

Round5 : B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69

Round6 : BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E

Round7 : CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A

Round8 : 8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C

Round9 : BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8

Round10 : 28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

Pertama dilakukan proses inisialisasi dengan operasi XOR antara State dan Key.

State Matrix dan Round key No.0 Matrix :

$$\begin{pmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{pmatrix} \quad \begin{pmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{pmatrix}$$

XOR entri yang sesuai, misalnya, 69 XOR 4B = 22

0110 1001

0100 1011

0010 0010

State Matrix baru adalah :

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

Gantikan setiap entri (byte) dari matriks keadaan saat ini dengan entri yang sesuai di AES S-Box. Misalnya : byte 6E diganti dengan masuknya S-Box di baris 6 dan kolom E, yaitu, oleh 9F. Ini mengarah ke Matriks Status baru :

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

Lapisan non-linear ini untuk ketahanan terhadap serangan kriptanalisis yang berbeda dan linier. empat baris digeser secara siklis ke kiri dengan offset 0,1, 2, dan 3. State Matrix baru adalah :

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

Langkah pencampuran linier ini menyebabkan difusi bit pada beberapa putaran.

Campur Kolom mengalikan matriks tetap terhadap Matriks Status saat ini :

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

Entri BA adalah hasil dari (02x63) XOR (03x2F) XOR (01xAF) XOR (01xA2) :

$$02 \times 63 = 00000010 \times 01100011 = 11000110$$

$$03 \times 2F = (02 \times 2F) \text{ XOR } 2F = (00000010 \times 00101111) \text{ XOR } 00101111 = 01110001$$

$$01 \times AF = AF = 10101111 \text{ dan } 01 \times A2 = A2 = 10100010$$

Dikarenakan :

$$11000110$$

$$01110001$$

$$10101111$$

$$10100010$$

$$10111010$$

State Matrix dan Round key No.1 Matrix:

$$\begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix} \quad \begin{pmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{pmatrix}$$

XOR menghasilkan Matriks Status baru:

$$\begin{pmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{pmatrix}$$

Output AES setelah Putaran 1: 58 47 08 8B 15 B6 1C BA 59 D4 E2 E8 CD 39 DF

CE

Putaran 2 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 6A & 59 & CB & BD \\ A0 & 4E & 48 & 12 \\ 30 & 9C & 98 & 9E \\ 3D & F4 & 9B & 8B \end{pmatrix}$$

$$\begin{pmatrix} 6A & 59 & CB & BD \\ 4E & 48 & 12 & A0 \\ 98 & 9E & 30 & 9B \\ 8B & 3D & F4 & 9B \end{pmatrix}$$

Putaran 2 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 15 & C9 & 7F & 9D \\ CE & 4D & 4B & C2 \\ 89 & 71 & BE & 88 \\ 65 & 47 & 97 & CD \end{pmatrix}$$

$$\begin{pmatrix} 43 & 0E & 09 & 3D \\ C6 & 57 & 08 & F8 \\ A9 & C0 & EB & 7F \\ 62 & C8 & FE & 37 \end{pmatrix}$$

Putaran 3 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 1A & AB & 01 & 27 \\ B4 & 5B & 30 & 41 \\ D3 & BA & E9 & D2 \\ AA & E8 & BB & 9A \end{pmatrix}$$

$$\begin{pmatrix} 1A & AB & 01 & 27 \\ 5B & 30 & 41 & B4 \\ E9 & D2 & D3 & BA \\ A9 & AA & E8 & BB \end{pmatrix}$$

Putaran 3 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} AA & 65 & FA & 88 \\ 16 & 0C & 05 & 3A \\ 3D & C1 & DE & 2A \\ B3 & 4B & 5A & 0A \end{pmatrix}$$

$$\begin{pmatrix} 78 & 70 & 99 & 4B \\ 76 & 76 & 3C & 39 \\ 30 & 7D & 37 & 34 \\ 54 & 23 & 5B & F1 \end{pmatrix}$$

Putaran 4 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} BC & 51 & EE & B3 \\ 38 & 38 & EB & 12 \\ 04 & FF & 9A & 18 \\ 20 & 26 & 39 & A1 \end{pmatrix}$$

$$\begin{pmatrix} BC & 51 & EE & B3 \\ 38 & EB & 12 & 38 \\ 9A & 18 & 04 & FF \\ A1 & 20 & 26 & 39 \end{pmatrix}$$

Putaran 4 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 10 & BC & D3 & F3 \\ D8 & 94 & E0 & E0 \\ 53 & EA & 9E & 25 \\ 24 & 40 & 73 & 7B \end{pmatrix}$$

$$\begin{pmatrix} B1 & 08 & 04 & E7 \\ CA & FC & B1 & B2 \\ 51 & 54 & C9 & 6C \\ ED & E1 & D3 & 20 \end{pmatrix}$$

Putaran 5 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} C8 & 30 & F2 & 94 \\ 74 & B0 & C8 & 37 \\ D1 & 20 & DD & 50 \\ 55 & F8 & 66 & B7 \end{pmatrix}$$

$$\begin{pmatrix} C8 & 30 & F2 & 94 \\ B0 & C8 & 37 & 74 \\ DD & 50 & D1 & 20 \\ B7 & 55 & F8 & 66 \end{pmatrix}$$

Putaran 5 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 2A & 26 & 8F & E9 \\ 78 & 1E & 0C & 7A \\ 1B & A7 & 6F & 0A \\ 5B & 62 & 00 & 3F \end{pmatrix}$$

$$\begin{pmatrix} 9B & 23 & 5D & 2F \\ 51 & 5F & 1C & 38 \\ 20 & 22 & BD & 91 \\ 68 & F0 & 32 & 56 \end{pmatrix}$$

Putaran 6 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 14 & 26 & 4C & 15 \\ D1 & CF & 9C & 07 \\ B7 & 93 & 7A & 81 \\ 45 & 8C & 23 & B1 \end{pmatrix}$$

$$\begin{pmatrix} 14 & 26 & 4C & 15 \\ CF & 9C & 07 & D1 \\ 7A & 81 & B7 & 93 \\ B1 & 45 & 8C & 23 \end{pmatrix}$$

Putaran 6 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} A9 & 37 & AA & F2 \\ AE & D8 & 0C & 21 \\ E7 & 6C & B1 & 9C \\ F0 & FD & 67 & 3B \end{pmatrix} \qquad \begin{pmatrix} 14 & 8F & C0 & 5E \\ 93 & A4 & 60 & 0F \\ 25 & 2B & 24 & 92 \\ 77 & E8 & 40 & 75 \end{pmatrix}$$

Putaran 7 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} FA & 73 & BA & 58 \\ DC & 49 & D0 & 76 \\ 3F & F1 & 36 & 4F \\ F5 & 9B & 09 & 9D \end{pmatrix} \qquad \begin{pmatrix} FA & 73 & BA & 58 \\ 49 & D0 & 76 & DC \\ 36 & 4F & 3F & F1 \\ 9D & F5 & 9B & 09 \end{pmatrix}$$

Putaran 7 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} 9F & 37 & 51 & 37 \\ AF & EC & 8C & FA \\ 63 & 39 & 04 & 66 \\ 4B & FB & B1 & D7 \end{pmatrix} \qquad \begin{pmatrix} 53 & 43 & 4F & 85 \\ 39 & 06 & 0A & 52 \\ 8E & 93 & 3B & 57 \\ 5D & F8 & 95 & BD \end{pmatrix}$$

Putaran 8 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} ED & 1A & 84 & 97 \\ 12 & 6F & 67 & 00 \\ 19 & DC & E2 & 5B \\ 4C & 41 & 2A & 7A \end{pmatrix} \qquad \begin{pmatrix} ED & 1A & 84 & 97 \\ 6F & 67 & 00 & 12 \\ E2 & 5B & 19 & DC \\ 7A & 4C & 41 & 2A \end{pmatrix}$$

Putaran 8 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} E8 & 8A & 4B & F5 \\ 74 & 75 & EE & E6 \\ D3 & 1F & 75 & 58 \\ 55 & 8A & 0C & 38 \end{pmatrix}$$

$$\begin{pmatrix} 66 & 70 & AF & A3 \\ 25 & CE & D3 & 73 \\ 3C & 5A & 0F & 13 \\ 74 & A8 & 0A & 54 \end{pmatrix}$$

Putaran 9 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 33 & 51 & 79 & 0A \\ 3F & 8B & 66 & 8F \\ EB & BE & 76 & 7D \\ 92 & C2 & 67 & 20 \end{pmatrix}$$

$$\begin{pmatrix} 33 & 51 & 79 & 0A \\ 8B & 66 & 8F & 3F \\ 76 & 7D & EB & BE \\ 20 & 92 & C2 & 67 \end{pmatrix}$$

Putaran 9 setelah kolom Mix dan setelah Roundkey:

$$\begin{pmatrix} B6 & E7 & 51 & 8C \\ 84 & 88 & 98 & CA \\ 34 & 60 & 66 & FB \\ E8 & D7 & 70 & 51 \end{pmatrix}$$

$$\begin{pmatrix} 09 & A2 & F0 & 7B \\ 66 & D1 & FC & 3B \\ 8B & 9A & E6 & BE \\ 78 & 65 & C4 & 89 \end{pmatrix}$$

Putaran 10 setelah Pengganti Byte dan setelah Shift Rows:

$$\begin{pmatrix} 01 & 3A & 8C & 21 \\ 33 & 3E & B0 & E2 \\ 3D & B8 & 8E & 04 \\ BC & 4D & 1C & A7 \end{pmatrix}$$

$$\begin{pmatrix} 01 & 3A & 8C & 21 \\ E3 & B0 & E2 & 33 \\ 8E & 04 & 3D & 8C \\ A7 & BC & 4D & 1C \end{pmatrix}$$

Putaran 10 setelah Roundkey (Perhatian: tidak ada kolom Mix di round terakhir):

$$\begin{pmatrix} 29 & 57 & 40 & 1A \\ C3 & 14 & 22 & 02 \\ 50 & 20 & 99 & D7 \\ 5F & F6 & B3 & 3A \end{pmatrix}$$

Cipher File yang dihasilkan adalah sebagai berikut :

29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

III.4. Perancangan

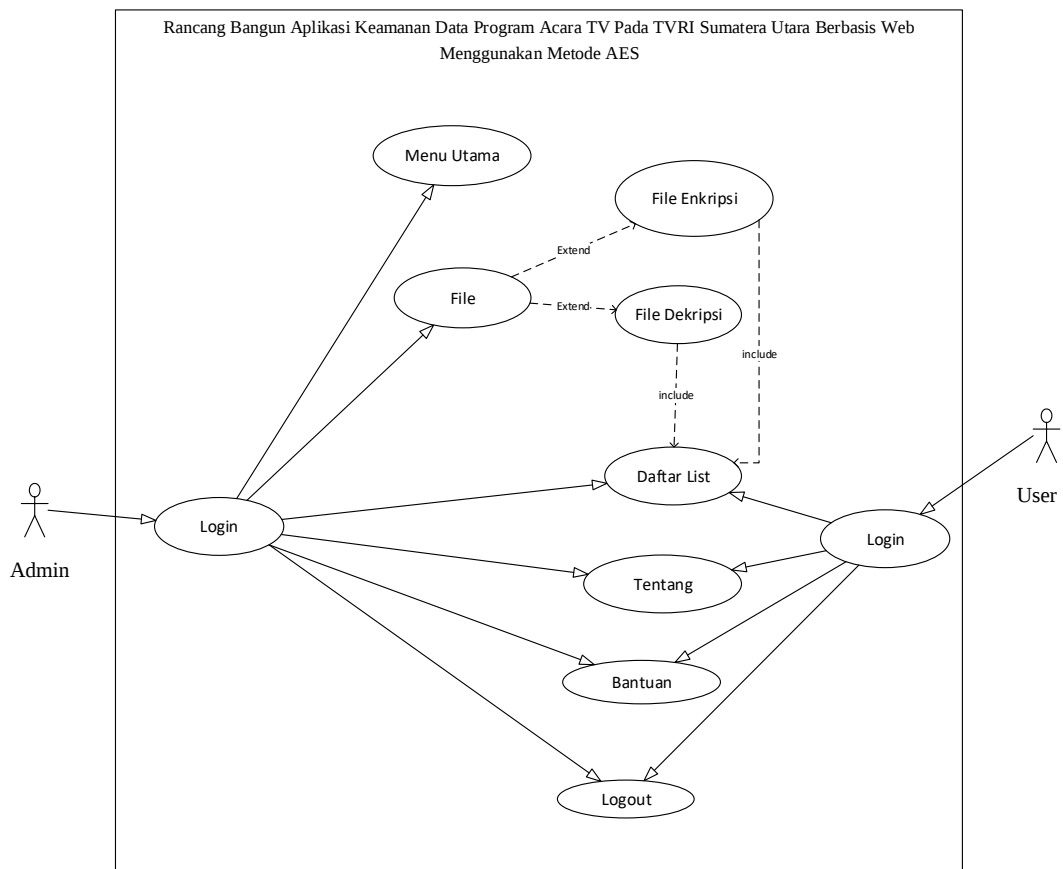
Perancangan aplikasi merupakan perancangan yang dilakukan untuk merancang sebuah aplikasi dengan menggunakan salah satu bahasa pemrograman *PHP*, dalam kasus ini penulis merancang sebuah aplikasi keamanan data *file* Dan *Folder* Dokumen dengan menggunakan *PHP*. Secara umum gambaran sistemnya adalah aplikasi keamanan ini dibuat untuk di implementasikan pada laptop dengan sistem operasi *windows 7*. Aplikasi ini bersifat *Kriptografi*, tugas utama aplikasi ini adalah enkripsi dan dekripsi Pengamanan Data File Dan Folder Dokumen.

III.5. Desain Sistem

Perancangan ini akan memberikan penjelasan mengenai rancangan aplikasi serta pembentukan dan pembangunan aplikasi kriptografi algoritma AES dalam mengamankan data *file* Rancang Bangun Aplikasi Keamanan Data Program Acara TV Pada TVRI Sumatera Utara Berbasis Web Menggunakan Metode AES.

III.5.1. Use Case Diagram

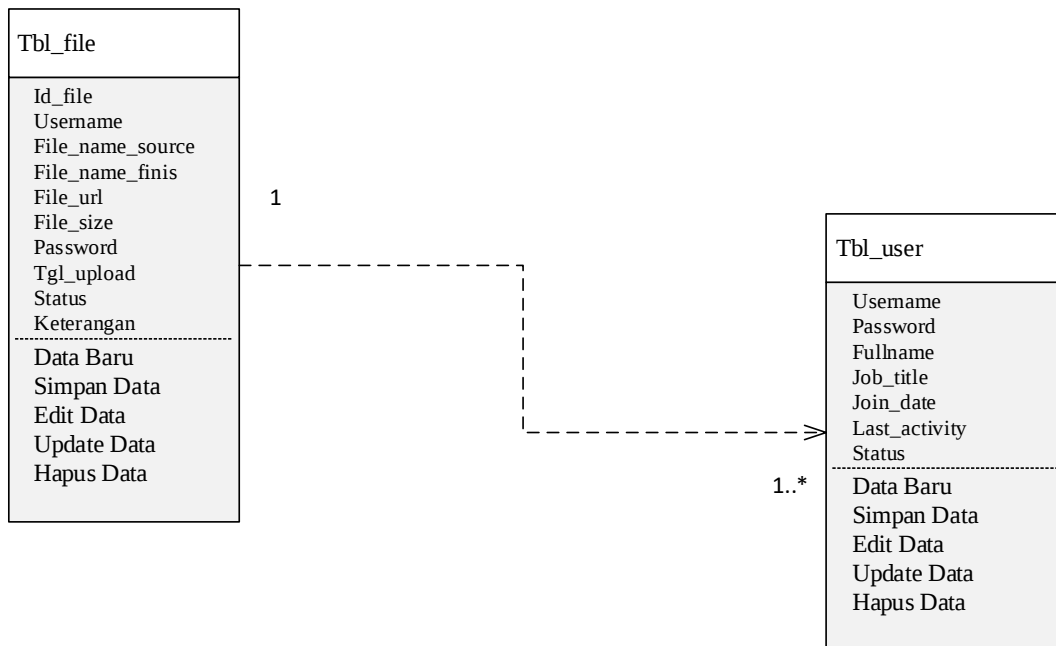
Perilaku beserta tugas-tugas dari tiap-tiap elemen maupun aktor yang terlibat dalam sistem yang akan dirancang, akan digambarkan dalam diagram *use case* yang bertujuan untuk memberikan gambaran secara umum tentang sistem yang akan dirancang gambar III.3 sebagai berikut:



Gambar III.3. Use Case Diagram

III.2.2.2. Class Diagram

Rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat pada gambar III.2 :



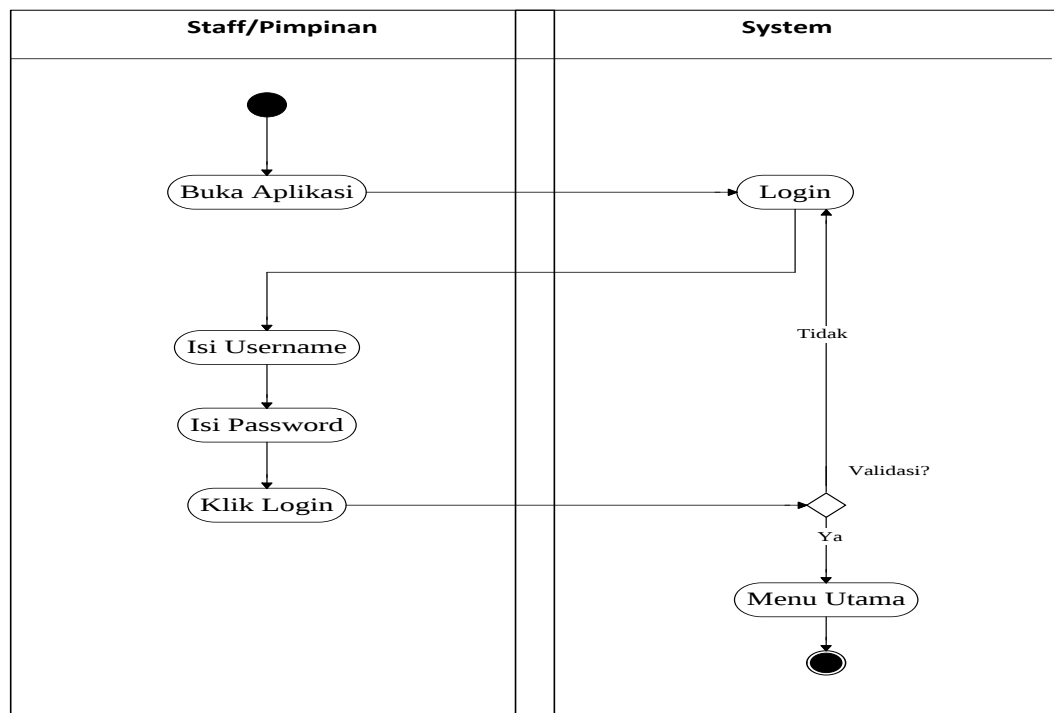
Gambar III.2. Class Diagram Rancang Bangun Aplikasi Keamanan Data Program Acara TV Pada TVRI Sumatera Utara Berbasis Web Menggunakan Metode AES

III.5.2. Activity Diagram

Activity Diagram menggambarkan berbagai alir aktivitas, bagaimana masing-masing alir berawal, *decision* (keputusan) yang mungkin terjadi, dan bagaimana sebuah sistem berakhir.

1. Activity Diagram Login

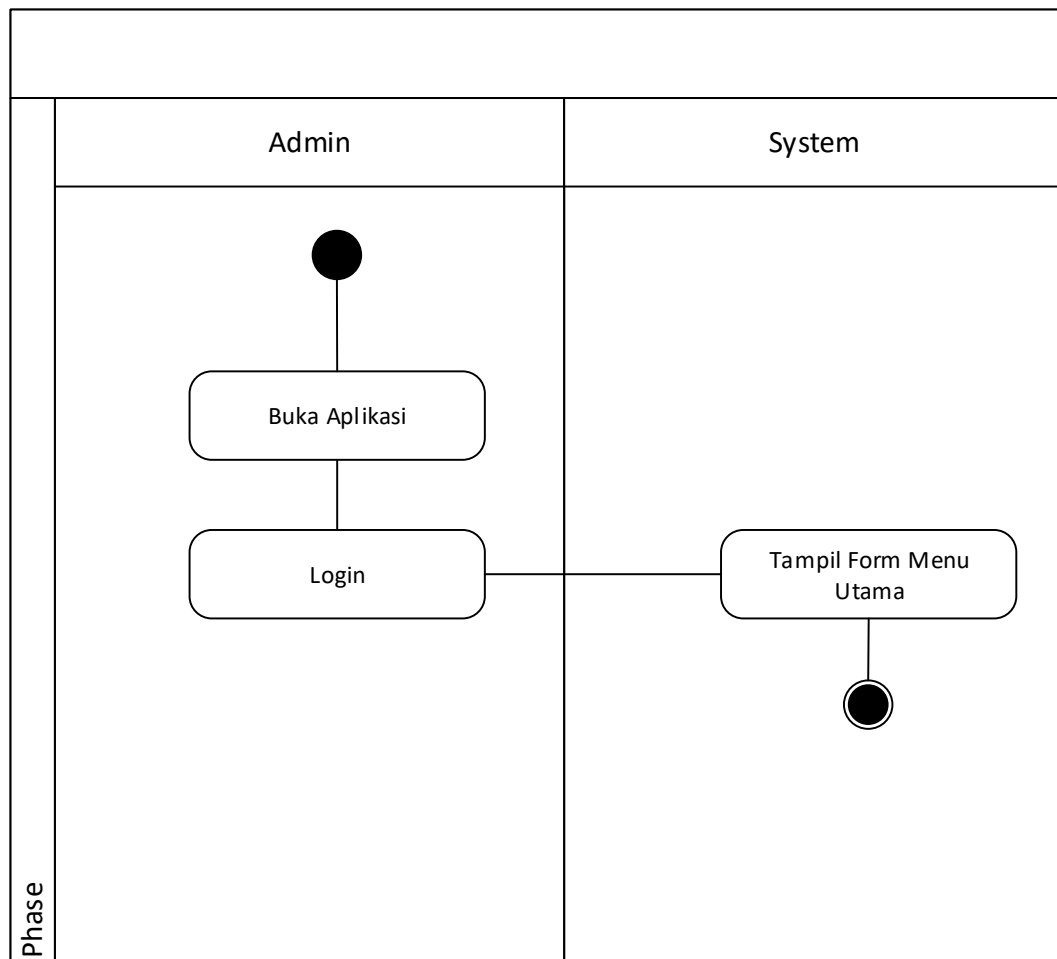
Serangkaian aktivitas login yang dapat dikelola admin agar masuk kedalam sebuah sistem yang sedang berjalan, dapat dilihat seperti pada gambar III.4 berikut :



Gambar III.4. Activity Diagram Login

2. Activity Diagram Menu Utama

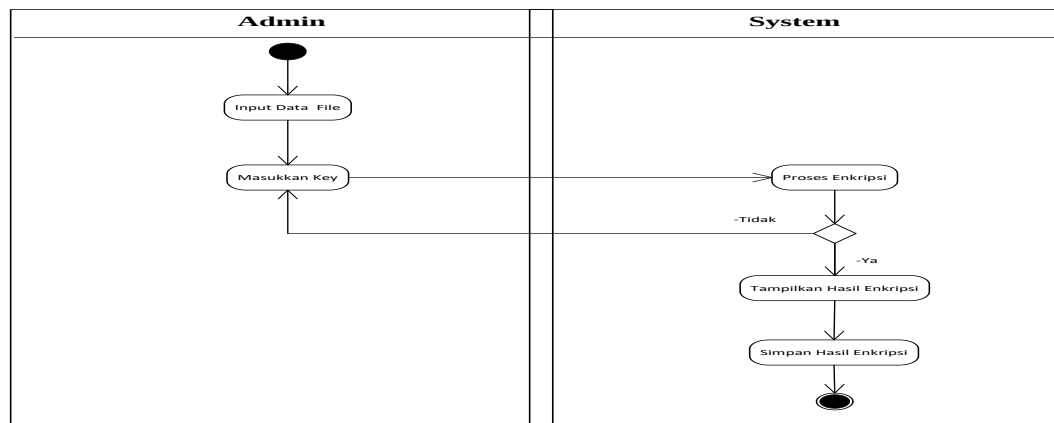
Serangkaian aktivitas menu utama yang dapat dilakukan admin dalam mengelola seluruh data yang terpusat dalam suatu program, dapat dilihat seperti pada gambar III.5. berikut :



Gambar III.5. Activity Diagram Menu Utama

3. Activity Diagram File Enkripsi

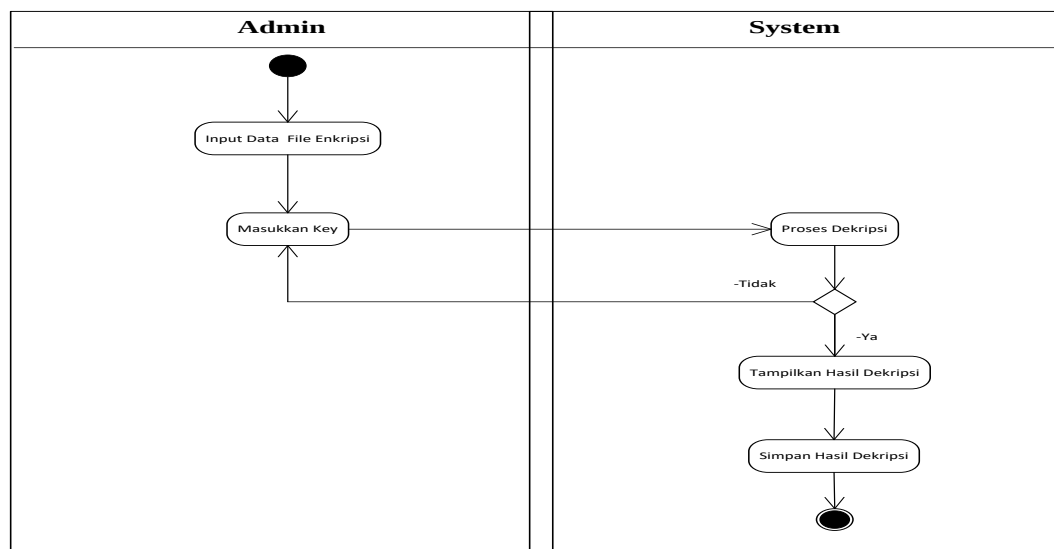
Serangkaian aktivitas file enkripsi yang dapat dilakukan admin dalam mengelola data, dapat dilihat seperti pada gambar III.6 berikut :



Gambar III.6. Activity Diagram Enkripsi

4. Activity Diagram Dekripsi

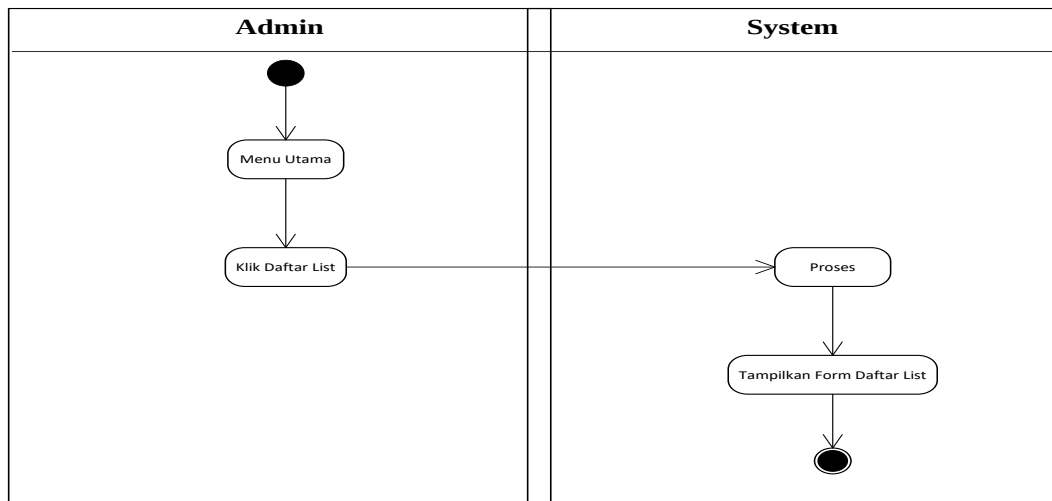
Serangkaian aktivitas file dekripsi yang dapat dilakukan admin dalam mengelola data, dapat dilihat seperti pada gambar III.7 berikut :



Gambar III.7. Activity Diagram Dekripsi

5. Activity Diagram Daftar List

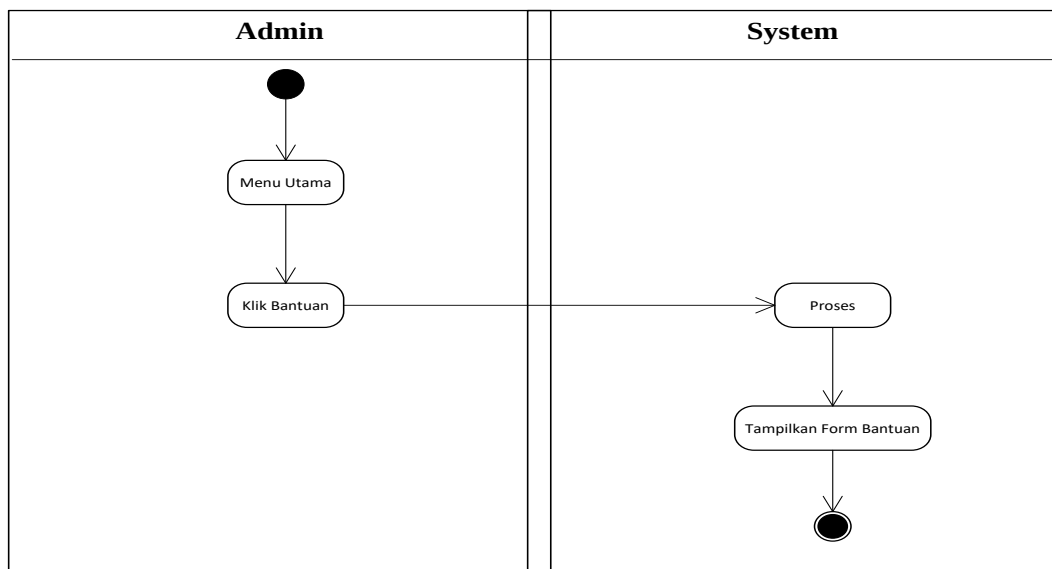
Serangkaian aktivitas Daftar List yang dapat dilakukan admin dalam mengelola data file yang sudah dienkripsi dan dekripsi, dapat dilihat seperti pada gambar III.8 berikut :



Gambar III.8. Activity Diagram Daftar List

6. Activity Diagram Bantuan

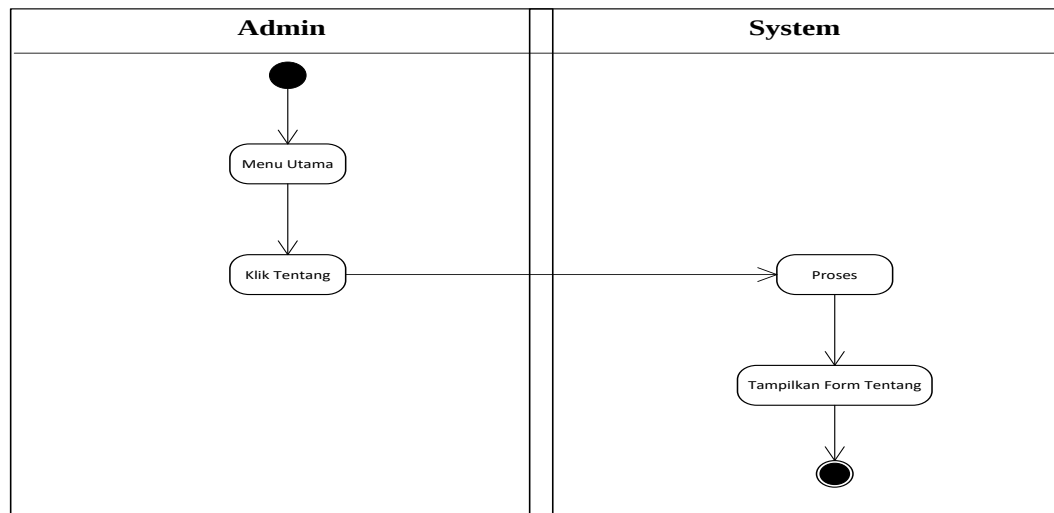
Serangkaian aktivitas bantuan yang dapat dilakukan admin dalam mengetahui tentang aplikasi, dapat dilihat seperti pada gambar III.9 berikut :



Gambar III.9. Activity Diagram Bantuan

7. Activity Diagram Tentang

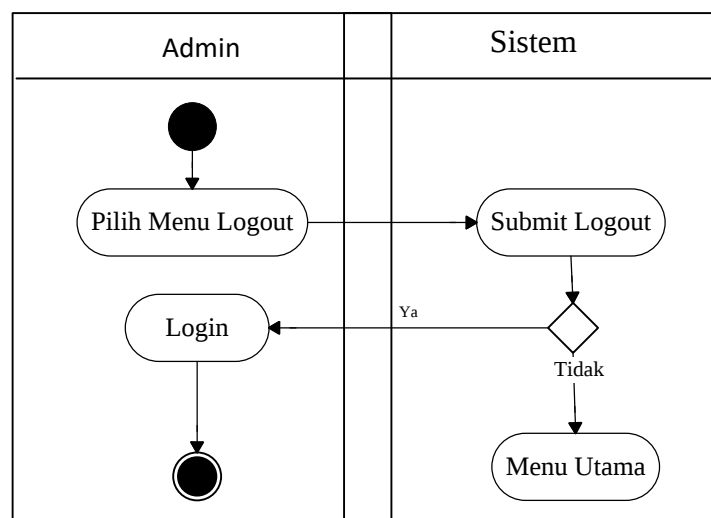
Serangkaian aktivitas tentang yang dapat dilakukan admin dalam mengetahui tentang aplikasi, dapat dilihat seperti pada gambar III.9 berikut :



Gambar III.9. Activity Diagram Tentang

8. Activity Diagram Log Out

Serangkaian aktivitas *logout* yang dapat dilakukan adalah admin akan keluar dari sebuah sistem yang sedang berjalan, dapat dilihat seperti pada gambar III.10 berikut :



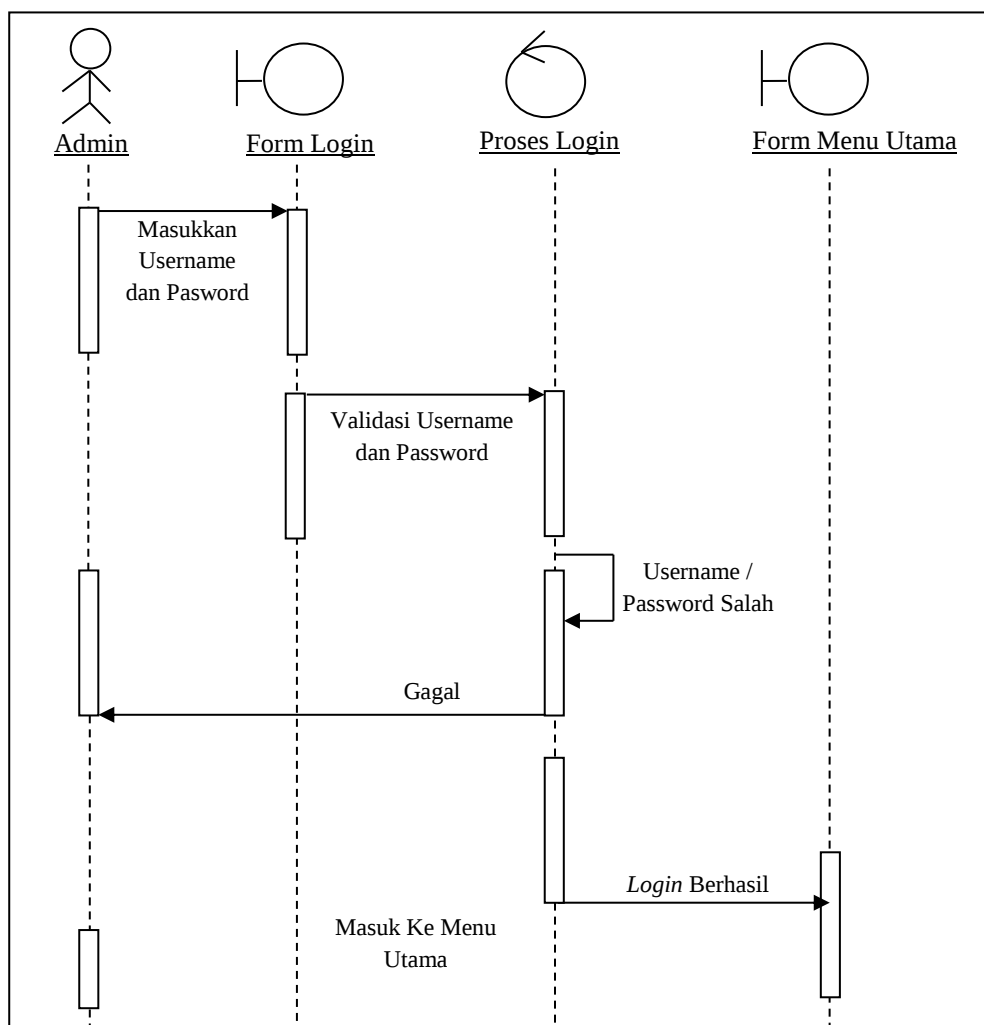
Gambar III.10. Activity Diagram Log Out

III.6.3. Sequence Diagram

Sequence Diagram adalah suatu diagram yang memperlihatkan atau menampilkan interaksi-interaksi antar objek di dalam sistem yang disusun pada sebuah urutan atau rangkaian waktu. Interaksi antar objek tersebut termasuk pengguna, *display*, dan sebagainya berupa pesan/*message*.

1. Sequence Diagram Login

Serangkaian kerja melakukan *login* dapat dilihat pada Gambar III.11 dibawah ini .

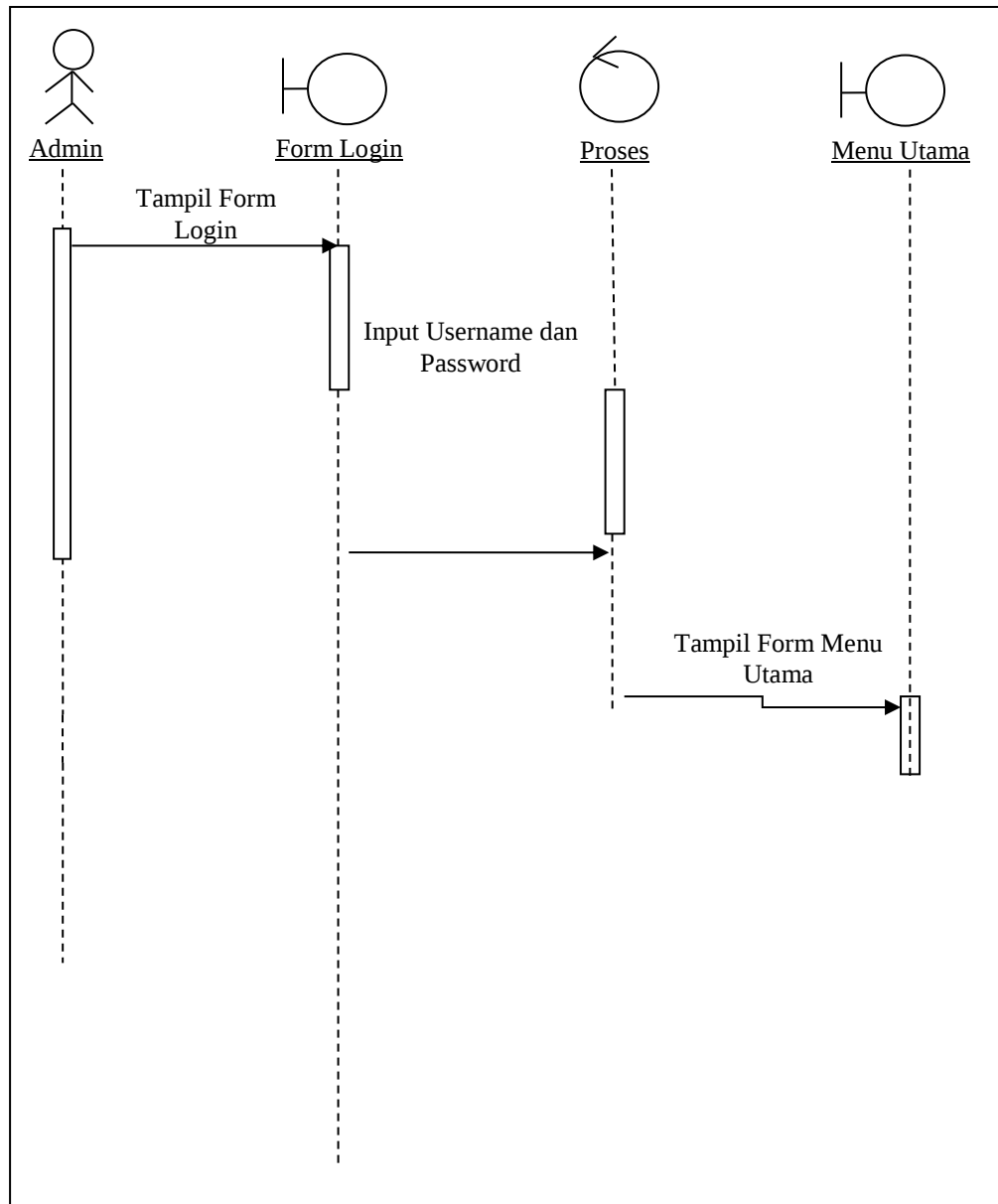




Gambar III.11. Sequence Diagram Login

2. Sequence Diagram Menu Utama

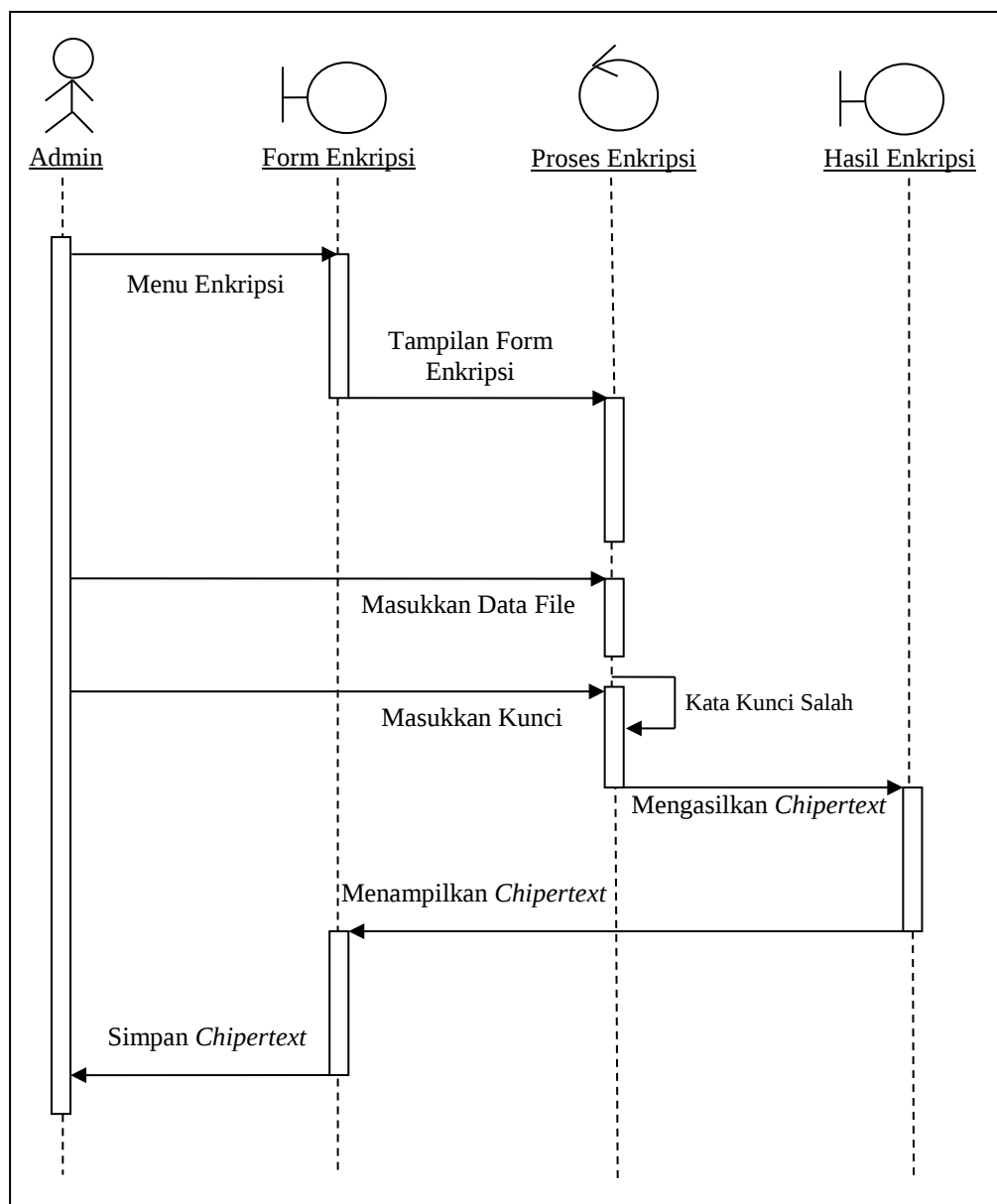
Serangkaian kerja untuk mengolah data yang terpusat pada sebuah sistem dapat dilihat pada Gambar III.12. dibawah ini.



Gambar III.12. Sequence Diagram Menu Utama

3. Sequence Diagram Enkripsi

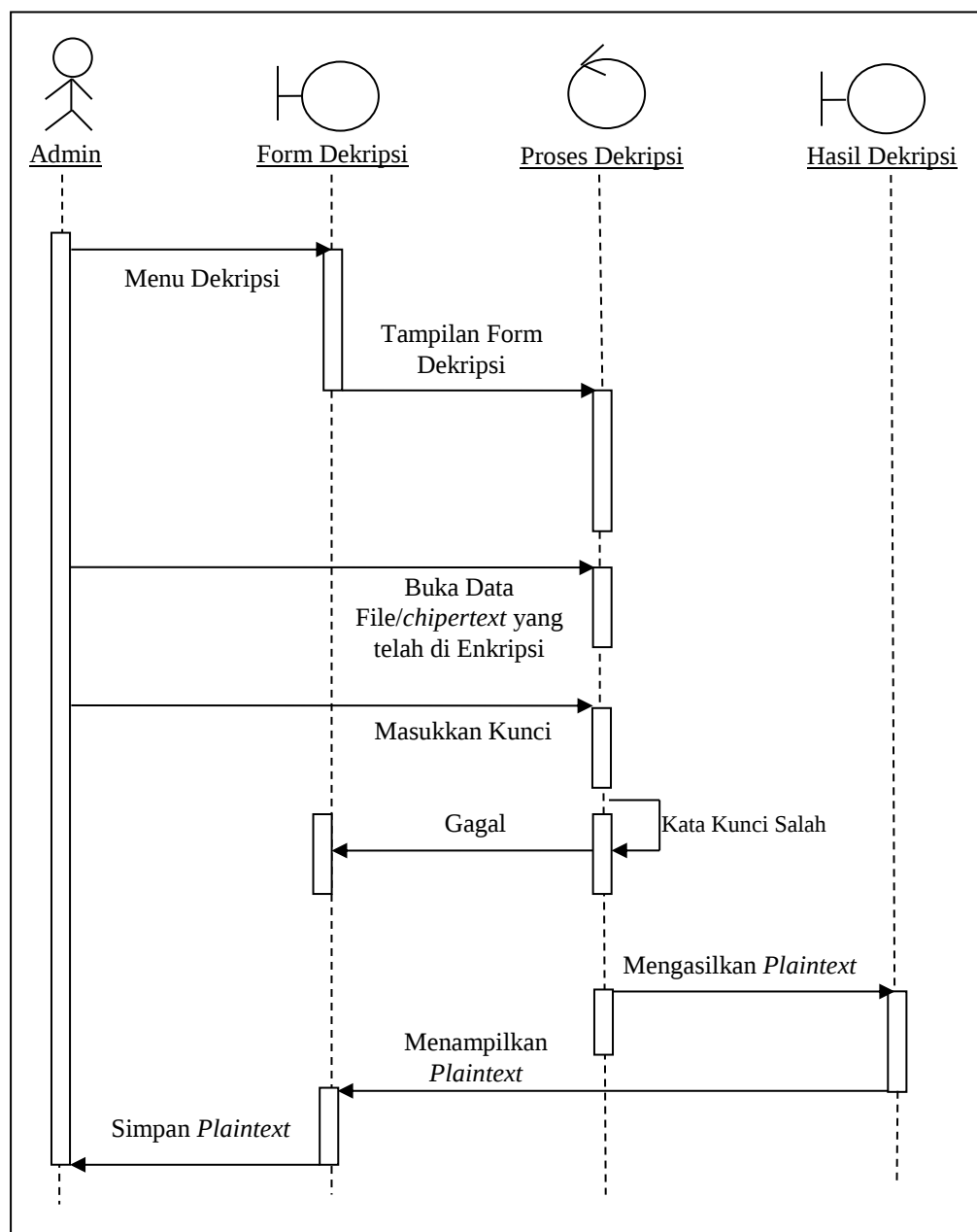
Serangkaian kerja melakukan enkripsi dapat dilihat pada Gambar III.13. dibawah ini.



Gambar III.13. Sequence Diagram Enkripsi

4. Sequence Diagram Dekripsi

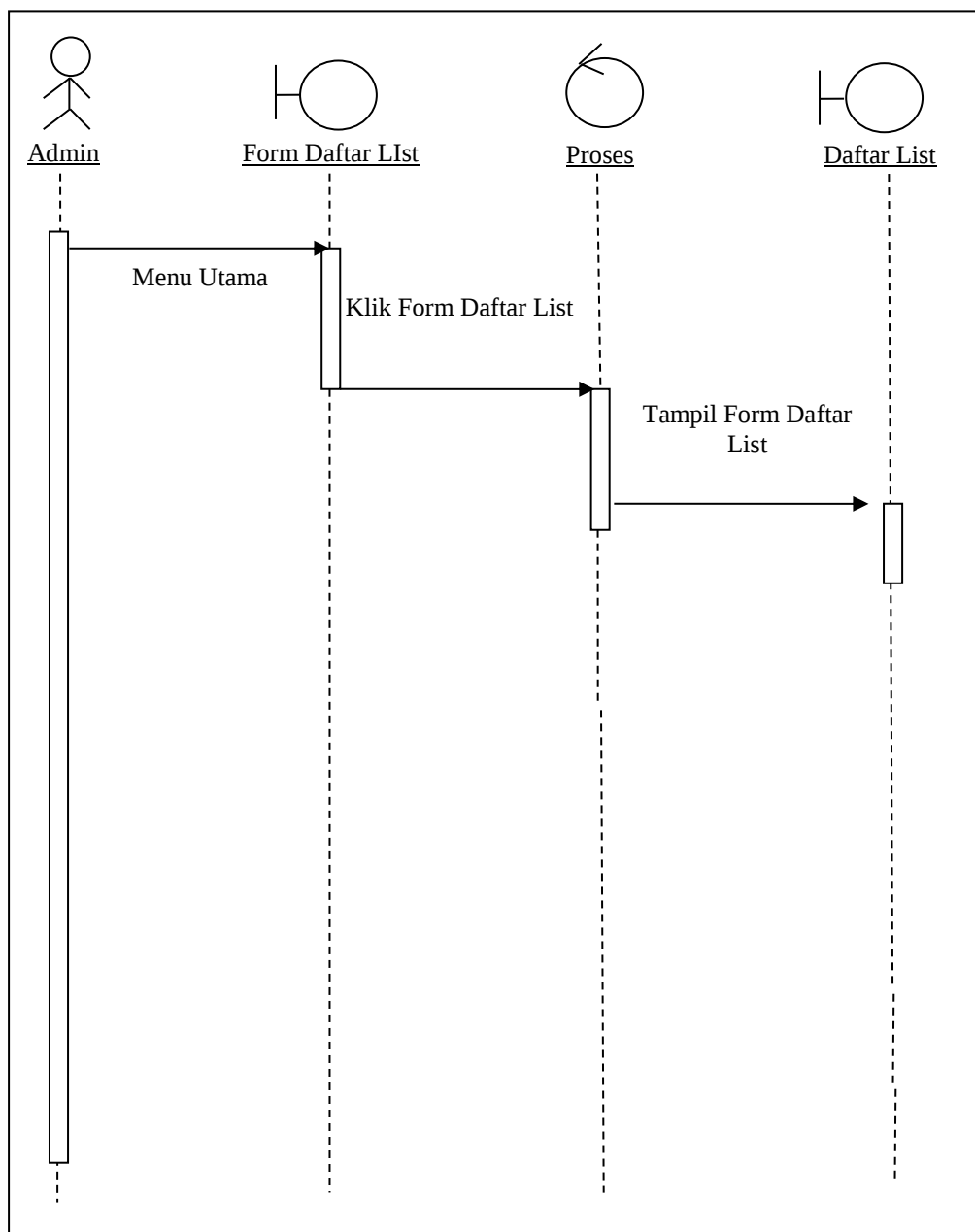
Serangkaian kerja melakukan dekripsi dapat dilihat pada Gambar III.14. dibawah ini.



Gambar III.14. Sequence Diagram Dekripsi

5. Sequence Diagram Daftar List

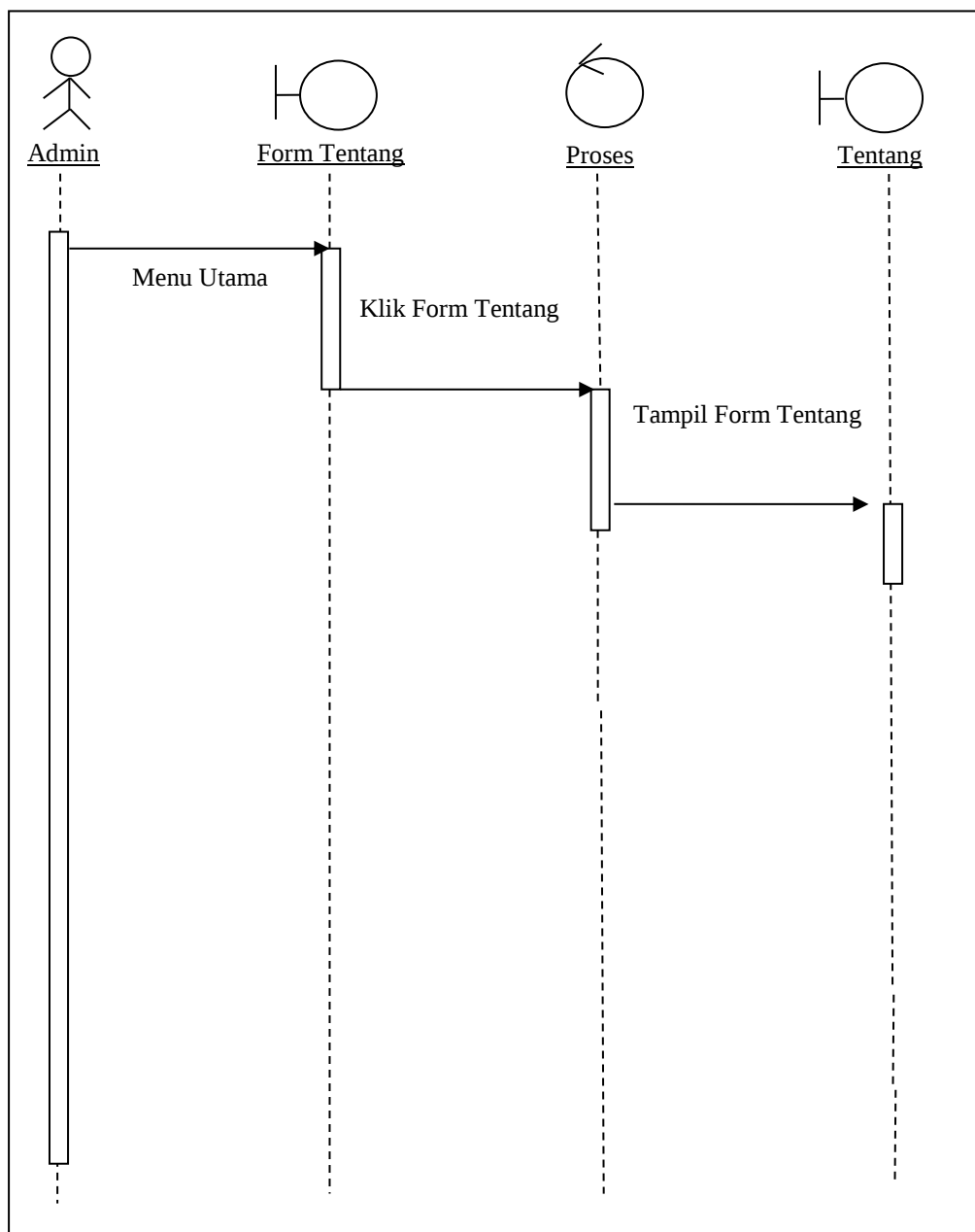
Serangkaian kerja melakukan daftar list dapat dilihat pada Gambar III.15 dibawah ini.



Gambar III.15. Sequence Diagram Daftar List

6. Sequence Diagram Tentang

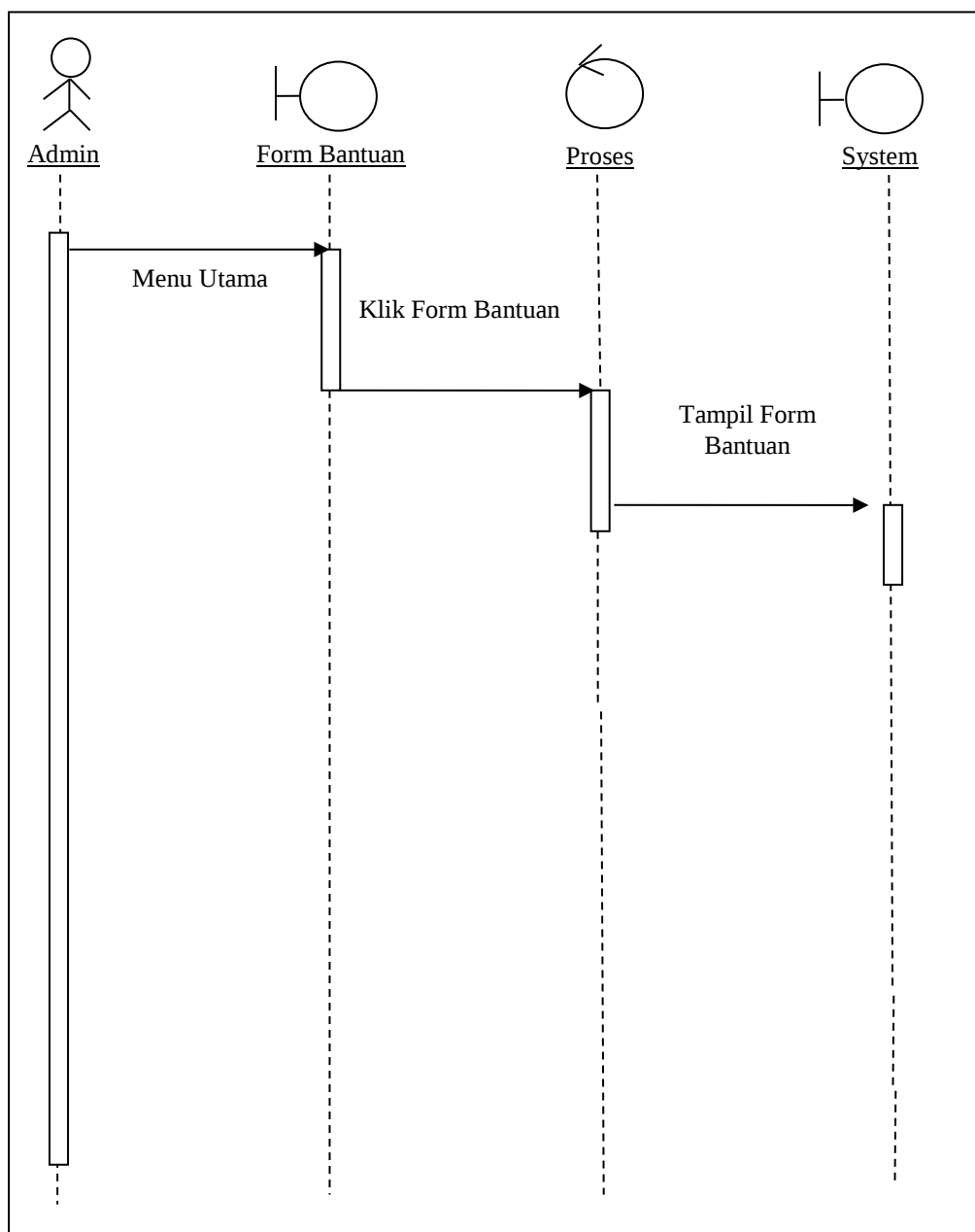
Serangkaian kerja melakukan tentang dapat dilihat pada Gambar III.16 dibawah ini.



Gambar III.14. Sequence Diagram Tentang

7. Sequence Diagram Bantuan

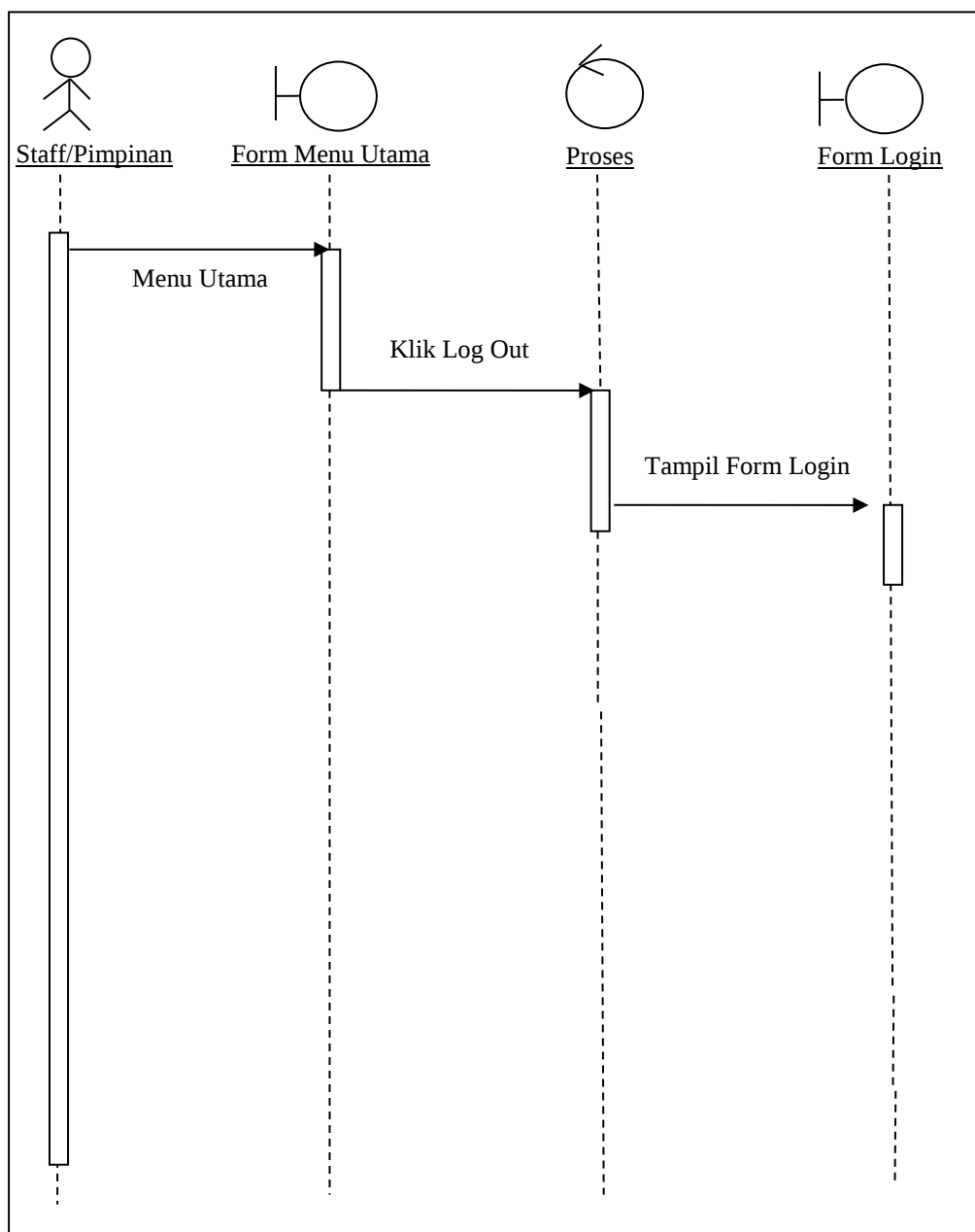
Serangkaian kerja melakukan bantuan dapat dilihat pada Gambar III.16 dibawah ini.



Gambar III.14. Sequence Diagram Bantuan

8. Sequence Diagram Log Out

Serangkaian kerja melakukan log out dapat dilihat pada Gambar III.15 dibawah ini.



Gambar III.15. Sequence Diagram Log Out

III.3.1. Desain Tabel

Tahap selanjutnya yang dikerjakan yaitu merancang struktur tabel pada basis data sistem yang akan dibuat, berikut ini merupakan rancangan struktur tabel tersebut :

1. Struktur Tabel File

Tabel file digunakan untuk menyimpan data, selengkapnya mengenai struktur tabel ini dapat dilihat pada tabel III.1 di bawah ini:

Tabel III.1 Rancangan Tabel File

Nama Database		Kkp		
Nama Tabel		File		
No	Nama Field	Tipe Data	Boleh Kosong	Kunci
1.	Id_file	Int	Tidak	Primary Key
2.	Username	Varchar	Tidak	-
3.	File_name_source	Varchar	Tidak	-
4.	File_name_finis	Varchar	Tidak	-
5.	File_url	Varchar	Tidak	
6.	File_size	Float	Tidak	
7.	Password	Varchar	Tidak	
8.	Tgl_upload	Timestamp	Tidak	
9.	Status	Enum	Tidak	
10.	Keterangan	Varchar	Tidak	

2. *Struktur Tabel users*

Tabel users digunakan untuk menyimpan data, selengkapnya mengenai struktur tabel ini dapat dilihat pada tabel III.2 di bawah ini:

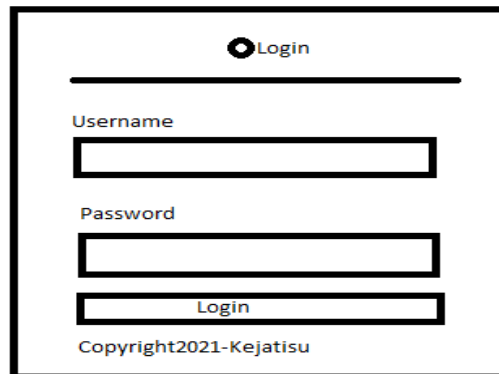
Tabel III.2 Rancangan Tabel Users

Nama <i>Database</i>		Kkp		
Nama Tabel		Users		
No	Nama Field	Tipe Data	Boleh Kosong	Kunci
1.	Username	Varchar	Tidak	<i>Primary Key</i>
2.	Password	Varchar	Tidak	-
3.	Fullname	Varchar	Tidak	-
4.	Job_title	Varchar	Tidak	
5.	Join_date	Timestamp	Tidak	
6.	Last_activity	Timestamp	Tidak	
7.	Status	Enum	Tidak	

III.7. *Desain Interface*

III.7.1. *Perancangan Form Login*

Perancangan *form login* ini terdiri dari satu buah gambar, satu buah *checkbox*, empat buah *label*, dua buah *button* dan dua buah *textfield*. Untuk lebih jelasnya, perancangan *form login* dapat dilihat pada Gambar III.16 sebagai berikut:.

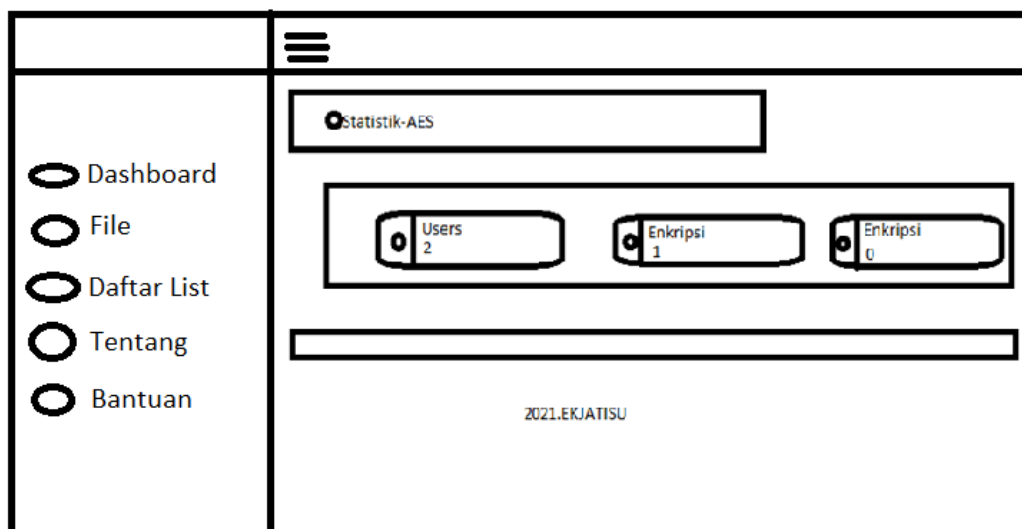


A login form design within a rectangular border. At the top center is a circular icon with a dot inside, followed by the text "Login". Below this is a horizontal line. Under the line are two input fields: the first is labeled "Username" and the second is labeled "Password". Below the password field is a "Login" button. At the bottom of the form is the text "Copyright2021-Kejatisu".

Gambar III.16. Perancangan *Form Login*

III.7.2. Perancangan *Form Utama*

Perancangan *form* Utama ini terdiri dari empat buah *menu bar*. Untuk lebih jelasnya, perancangan *form* Utama dapat dilihat pada Gambar III.17 sebagai berikut:



A main form design with a sidebar on the left and a main content area on the right. The sidebar contains five menu items, each with a circular icon: "Dashboard", "File", "Daftar List", "Tentang", and "Bantuan". The main content area has a header bar with a hamburger menu icon on the left and a "Statistik-AES" button on the right. Below the header bar is a row of three cards: "Users" with a value of 2, "Enkripsi" with a value of 1, and "Enkripsi" with a value of 0. Below the cards is a long horizontal bar. At the bottom center of the main content area is the text "2021.EKJATISU".

Gambar III.17. Perancangan *Form Utama*

III.7.3. Perancangan *Form Enkripsi*

Perancangan *form* Enkripsi, untuk lebih jelasnya, perancangan *form* Enkripsi dapat dilihat pada Gambar III.18 sebagai berikut:

Gambar III.18. Perancangan *Form* Enkripsi

III.7.4. Perancangan *Form* Dekripsi

Perancangan *form* Dekripsi, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar III.19 sebagai berikut:

Gambar III.19. Perancangan *Form* Dekripsi

III.7.5. Perancangan *Form* Daftar List

Perancangan *form* Daftar List, untuk lebih jelasnya, perancangan *form* Daftar List dapat dilihat pada Gambar III.20. sebagai berikut:

Administrator Project Manager	History Aplikasi Enkripsi dan Dekripsi-ACS							
Dashboard File Daftar List Tentang Bantuan	Search							
	Id File Username Nama File Nm.File Enkripsi Uk.File Tanggal Status							
	62	sidang	xxx.com	xxx.rda	38 Kb	2021-10	Terenkripsi	
	63	admin	xxx.kejati	xxx.kejati.rda	1284.4 Kb	10-2021	Terenkripsi	
	64	admin	xxx.sumut	xxx.rda	12 Kb	2021-10	Sudah Dideskripsi	
	Id File Username Nm.File smbr Nm.File Enkripsi Uk.File Tanggal Status							
Showing 1 to 3 of 3 entries								
					Previous	1	Next	

Gambar III.20. Perancangan *Form* Daftar List