BAB III
ANALISIS DAN PERANCANGAN

III.1. Analisis Masalah

Analisis masalah adalah menyangkut upaya pemahaman dan pengkajian sesuatu yang harus diuraikan serta dipecahkan atau diselesaikan baik secara kualitatif maupun kuantitatif. Permasalahan yang ada pada penelitian ini adalah masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi, namun pada pengamanan *file Document* tingkat keamanan nya sangat rendah.

Strategi dalam melakukan pemecahan masalah yang sedang dianalisa oleh penulis mengenai perancangan Perancangan Aplikasi Pengamanan *File Document* Dengan Algoritma AES (*Advanced Encryption Standard*) adalah sebagai berikut:

1. Merancang sebuah aplikasi dengan memanfaatkan sistem keamanan data yang dapat menjaga kerahasiaan dan keamanan *file Document* pada aplikasi *Document*.
2. Merancang dan membangun sebuah aplikasi *Document* dengan menggunakan Algoritma AES (*Advanced Encryption Standard*).
3. Merancang sebuah aplikasi enkripsi untuk mengamankan *file document* berbasis web

III.2. Penerapan Algoritma AES

Algoritma kriptografi bernama Rijndael yang didesain oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES yang diadakan oleh NIST (*National Institutes of Standards and Technology*) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan *Advanced Encryption Standard* (AES). Setelah mengalami beberapa proses standardisasi oleh NIST, Rijndael kemudian diadopsi menjadi standard algoritma kriptografi secara resmi pada 22 Mei 2002. Pada 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik.

Pada algoritma AES, jumlah blok *input*, blok *output*, dan *state* adalah 128 bit. Dengan besar data 128 bit, berarti Nb = 4 yang menunjukkan panjang data 22 tiap baris adalah 4 byte. Dengan blok input atau blok data sebesar 128 bit, *key* yang digunakan pada algoritma AES tidak harus mempunyai besar yang sama dengan blok input. *Cipher key* pada algoritma AES bisa menggunakan kunci dengan panjang 128 bit, 192 bit atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan di implementasikan pada algoritma AES ini (Gilang Gumira ; 2016 : 280).

Misalkan seseorang akan mengamankan sebuah file plainteks yang berisi 128 bit atau 16 byte atau 16 karakter seperti berikut :

Plaintext : Potensi Utama

Kunci : Fauzan

Algoritma : AES 128 bit -> 16 byte

Maka plainteks ini dapat dibuat menjadi state berikut:

P	N	U	a	F	a	null	null
O	S	t	null	a	n	null	null
T	I	a	null	u	null	null	null
E	Space	m	null	z	null	null	null

Konversi Teks Ke Hexadecimal

50	6e	55	61	46	61	00	00
6f	73	74	61	61	6E	00	00
74	69	61	00	75	00	00	00
65	20	6d	00	7A	00	00	00

Konversi HExaDecimal ke Biner

01010000	01101110	01010101	01100001	01000110	01100001	00000000	00000000
01101111	01110011	01110100	01100001	01100001	01101110	00000000	00000000
01110100	01101001	01100001	00000000	01110101	00000000	00000000	00000000
01100101	00100000	01101101	00000000	01111010	00000000	00000000	00000000

Initial Round XoR

01010000	XoR	01000110	=	00010110	01101110	XoR	01100001	=	00001111
01101111	XoR	01100001	=	00001110	01110011	XoR	01101110	=	00000110
01110100	XoR	01110101	=	00000001	01101001	XoR	00000000	=	01101001
01100101	XoR	01111010	=	00011111	00100000	XoR	00000000	=	00100000

Hasil 00010110 00001111 01010101 01100001

Binary 00001110 00000110 01110100 01100001

00000001 01101001 01100001 00000000

00011111 00100000 01101101 00000000

01010101 XoR 00000000 = 01010101 01100001 XoR 00000000 = 01100001

01110100 XoR 00000000 = 01110100 01100001 XoR 00000000 = 01100001

01100001 XoR 00000000 = 01100001 00000000 XoR 00000000 = 00000000

01101101 XoR 00000000 = 01101101 00000000 XoR 00000000 = 00000000

Hasil Hexa	16	F	55	61
	E	6	74	61
	1	69	61	00
	1F	20	6D	00

Hasil XoR

16	F	55	61
E	6	74	61
1	69	61	00
1F	20	6D	00

Proses Sub-btes menggunakan tabel S-Box

Ff	fb	ed	d8
d7	a5	ca	d8
09	e4	d8	52
cb	54	b3	52

Proses Shift Rows

ff	fb	ed	d8	Baris 1 Tidak digeser
d7	a5	ca	d8	Geser 1

09	e4	d8	52	Geser 2
cb	54	b3	52	Geser 3

Hasil Shift Rows

ff	fb	ed	d8
ca	d8	d7	a5
d8	52	09	e4
52	cb	54	b3

Proses Mix Column

02	03	01	01		ff	fb	ed	d8	
01	02	03	01	*	ca	d8	d7	a5	=
01	01	02	03		d8	52	09	e4	
03	01	01	02		52	cb	54	b3	

11111101	11111000	11101100	011011001
11001011	11011010	11010100	11101000
11011001	01010011	00001011	10100100
01010001	11001010	01010101	10110001

Konversi Hexa

FD	F8	EC	D9
CB	DA	D4	E8
D9	53	0B	A4
51	CA	55	B1

Hasil putaran pertama adalah
FD CB D9 51 | F8 DA 53 CA | EC D4 0B 55 | D9 E8 A4 B1

Lanjut putaran selanjut nya sampe 10x putaran

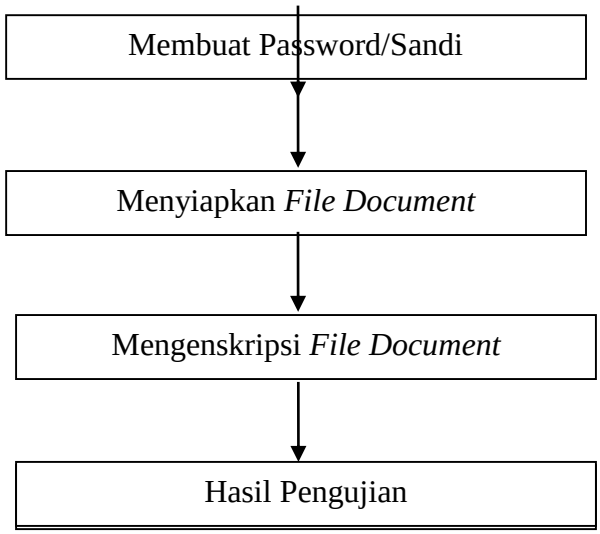
Putaran KE-SEPULUH (PUTARAN TERAKHIR)

FD	F8	EC	D9
DA	D4	E8	CB
0B	A4	D9	53
B1	51	CA	55

HASIL ENKRIPSI DALAM HEXA
FD DA 0B B1 | F8 D4 A4 51 | EC E8 D9 CA | D9 CB 53 55

III.3. Kerangka Kerja Aplikasi

Perancangan Kerangka Kerja Aplikasi Pengamanan *File Document* Dengan Algoritma AES (*Advanced Encryption Standard*) dengan perancangan sebagai berikut :



Gambar 3.1. Kerangka Kerja Aplikasi

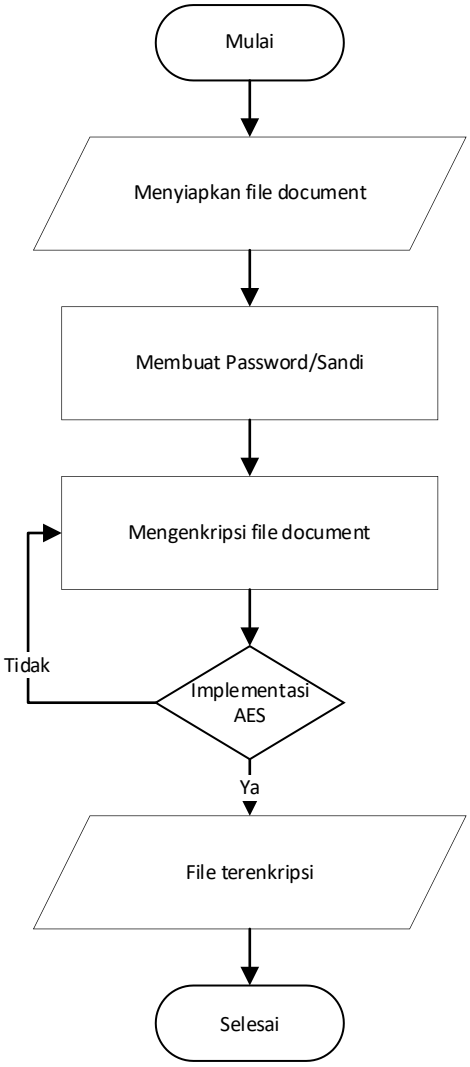
III.4. Desain Sistem

Desain sistem pada penelitian ini dibagi menjadi dua desain, yaitu desain sistem secara global untuk penggambaran model sistem secara garis besar dan desain sistem secara detail untuk membantu dalam pembuatan sistem. Perancangan Aplikasi Pengamanan *File Document* Dengan Algoritma AES (*Advanced Encryption Standard*) dengan perancangan sebagai berikut :

III.4.1. Desain Sistem Secara Global

III.4.1.1. *Flowchart* Enkripsi

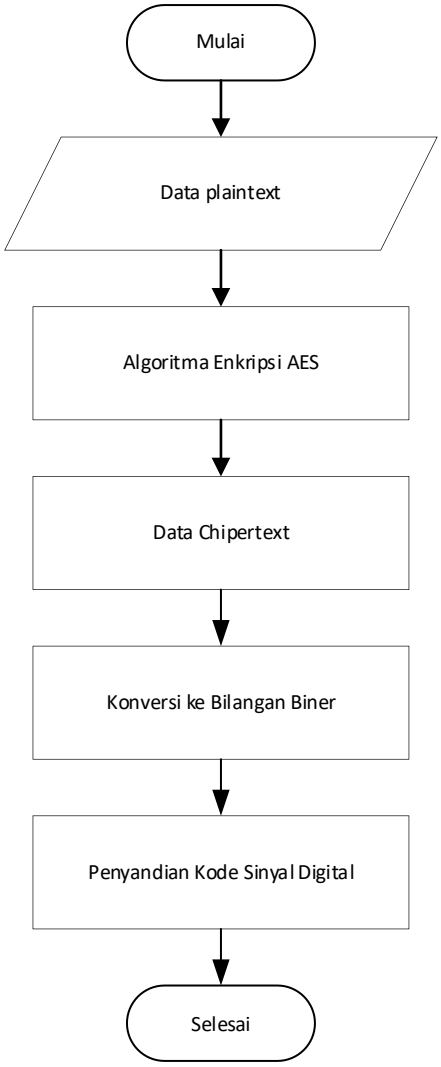
Flowchart merupakan penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program,. Biasanya mempengaruhi penyelesaian masalah yang khusunya perlu dipelajari dan dievaluasi lebih lanjut. Maka digambarlah suatu bentuk *flowchart* yang dapat dilihat pada gambar dibawah III.1. berikut :



Gambar III.1. *Flowchart* Enkripsi Perancangan Aplikasi Pengamanan *File Document* Dengan Algoritma AES (*Advanced Encryption Standard*)

III.4.1.2. *Flowchart* Implementasi AES

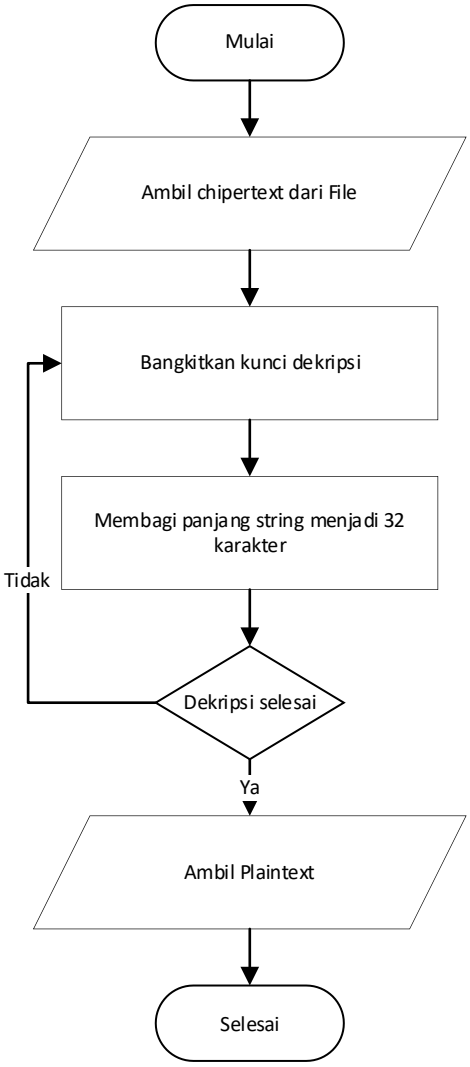
Flowchart merupakan penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program,. Biasanya mempengaruhi penyelesaian masalah yang khusunya perlu dipelajari dan dievaluasi lebih lanjut. Maka digambarlah suatu bentuk *flowchart* yang dapat dilihat pada gambar dibawah III.2. berikut :



Gambar III.2. *Flowchart* Algoritma AES (*Advanced Encryption Standard*)

III.4.1.3. *Flowchart* Dekripsi *File*

Flowchart merupakan penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program. Biasanya mempengaruhi penyelesaian masalah yang khusunya perlu dipelajari dan dievaluasi lebih lanjut. Maka digambarlah suatu bentuk *flowchart* yang dapat dilihat pada gambar dibawah III.3. berikut :

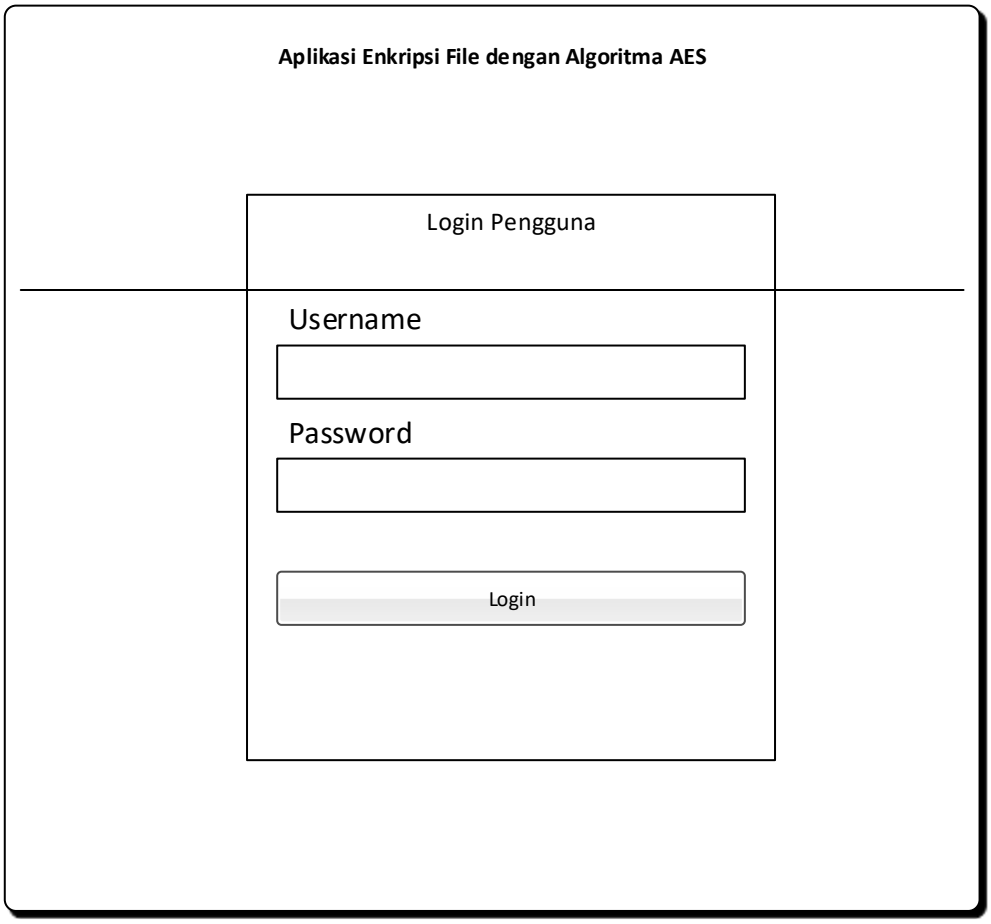


Gambar III.3. *Flowchart* Algoritma AES (*Advanced Encryption Standard*)

III.5. Desain Sistem Secara Detail

Tahap perancangan berikutnya yaitu desain sistem secara detail yang meliputi desain sistem.

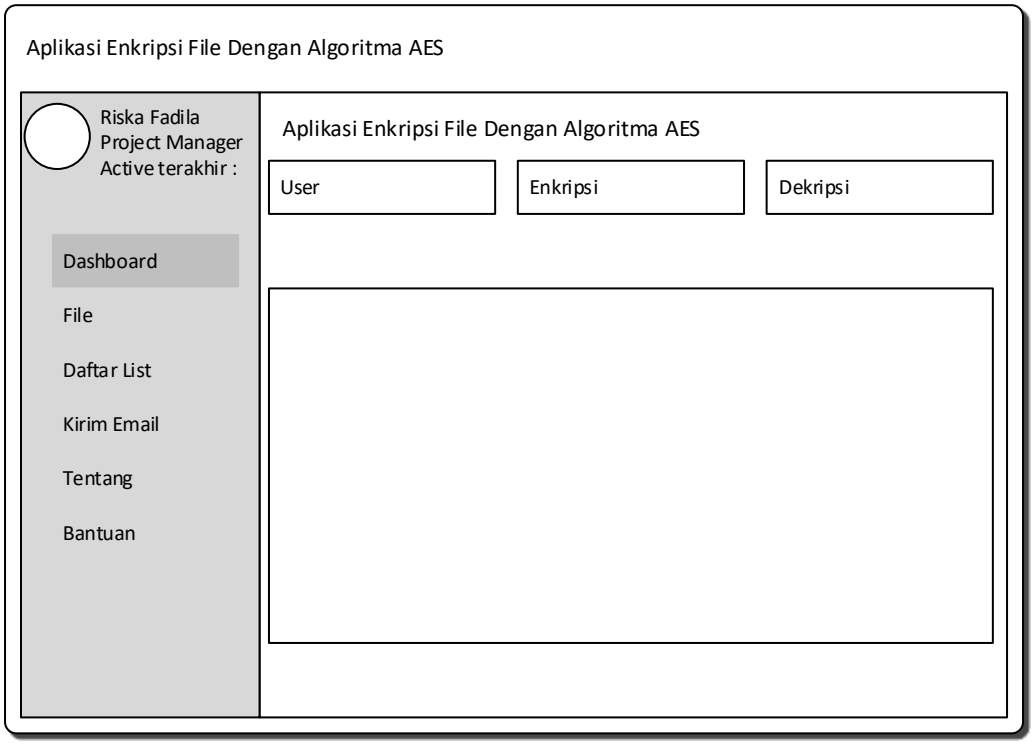
1. Tampilan Halaman Login



Gambar III.4. Tampilan Halaman Login

Gambar III.4 adalah merupakan tampilan yang akan tampil jika aplikasi dibuka, pada halaman ini pengguna wajib memasukan *username* dan *password* yang sesuai dengan data yang sudah tersimpan pada database, jika *username* dan *password* yang dimasukan sesuai.

2. Halaman *Dashboard* Pengguna

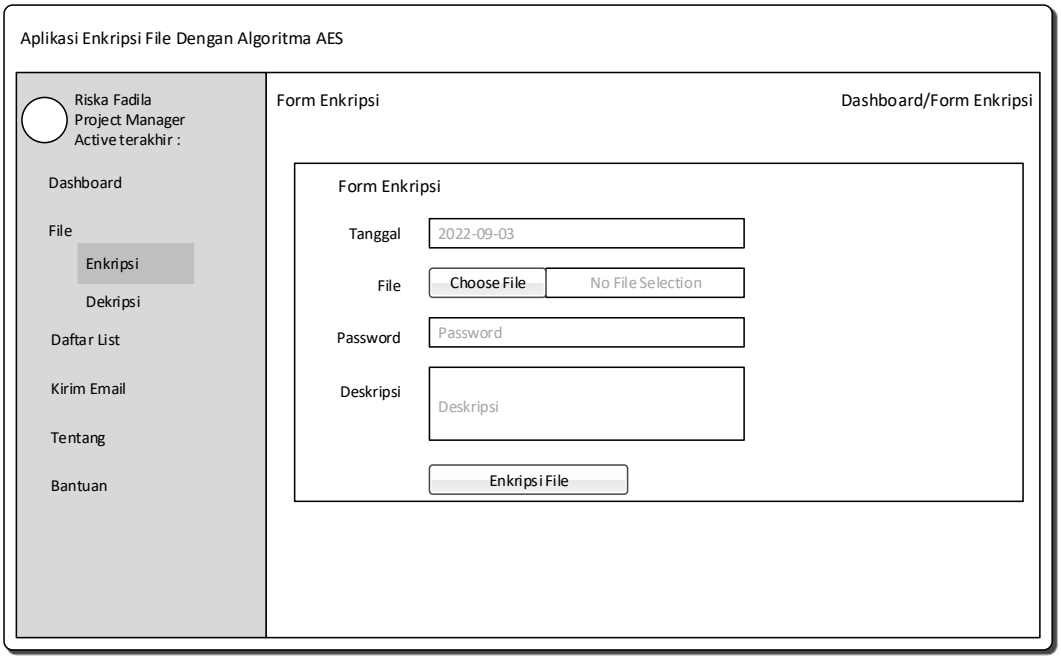


Gambar III.5. Tampilan Hasil Halaman *Dashboard* Pengguna

Halaman *Dashboard* adalah merupakan halaman utama dari aplikasi, pada halaman ini terdapat beberapa menu navigasi yang terletak pada bagian sebelah kiri halaman.

3. Halaman Sub Menu File Enkripsi

Halaman ini adalah merupakan sub menu dari menu file, halaman ini berisi form yang berfungsi untuk melakukan proses enkripsi, seperti yang terlihat pada gambar III.6.dibawah ini:

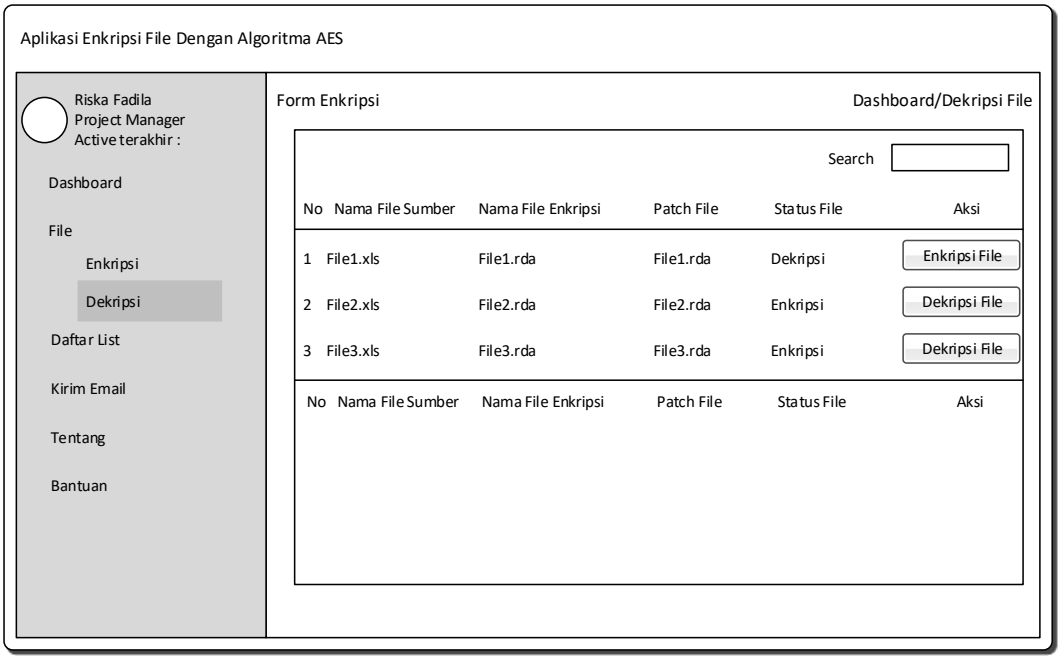


Gambar III.6. Tampilan Hasil Halaman Sub Menu Enkripsi

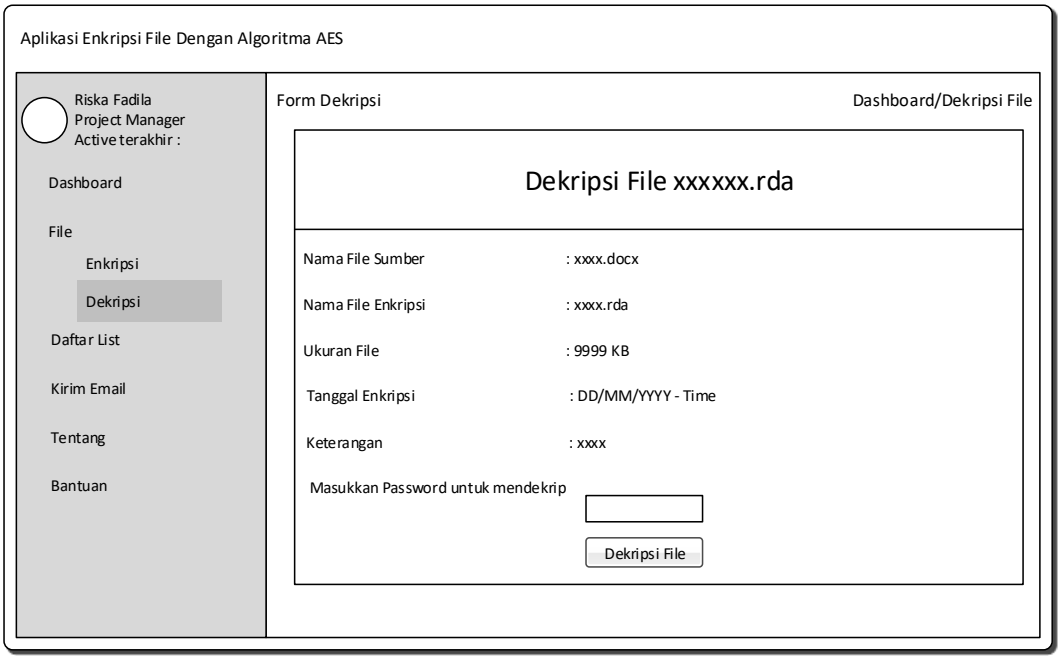
Untuk melakukan proses enkripsi pengguna harus mengisikan form yang sudah disediakan, file yang dapat dienkripsi adalah file-file yang berjenis teks seperti file Ms.Word, Ms.Excel,txt. Pada proses enkripsi hanya file yang memiliki ukuran maksimal 3Mb yang dapat diproses, file yang berhasil di enkripsi akan disimpan dalam sebuah folder tersendiri dan informasi mengenai proses yang telah berhasil dilakukan akan disimpan didalam databas.

4. Halaman Sub Menu File Dekripsi

Pada halaman ini akan menampilkan riwayat seluruh file yang sudah di enkripsi dan dekripsi dalam sebuah data tabel, untuk melakukan proses dekripsi pengguna dapat meng-klik pada tombol deskripsi yang berada pada masing-masing file.



Gambar III.7. Tampilan Hasil Halaman Sub Menu Dekripsi

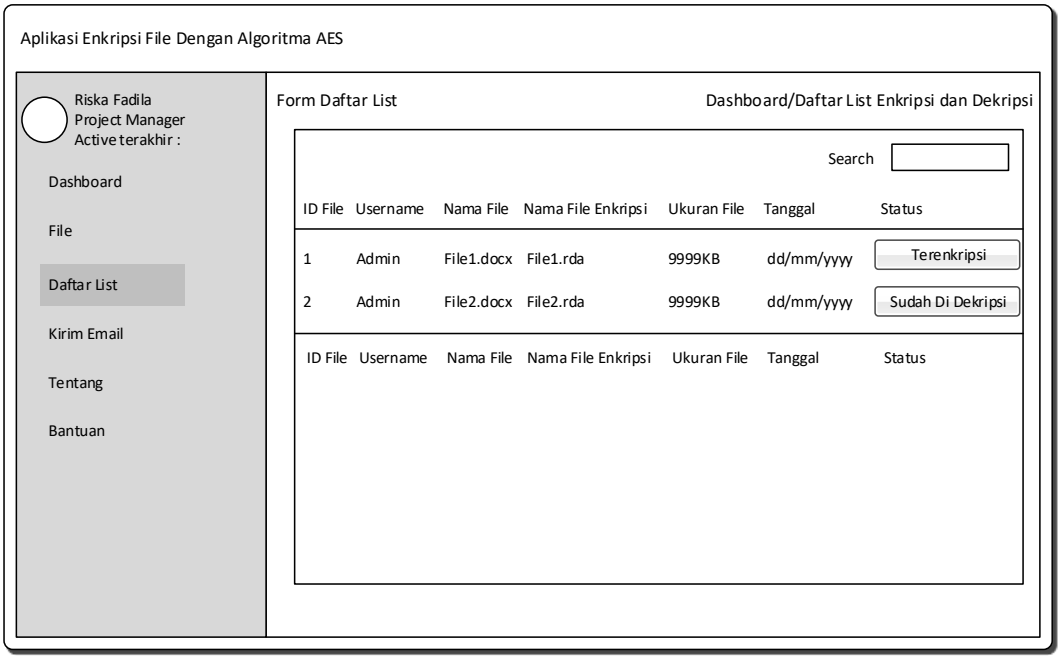


Gambar III.7. Tampilan Hasil Halaman Form Deskripsi

Pada saat melakukan proses dekripsi terhadap file, password atau kunci yang digunakan harus sama dengan kunci yang dipergunakan pada saat melakukan proses enkripsi.

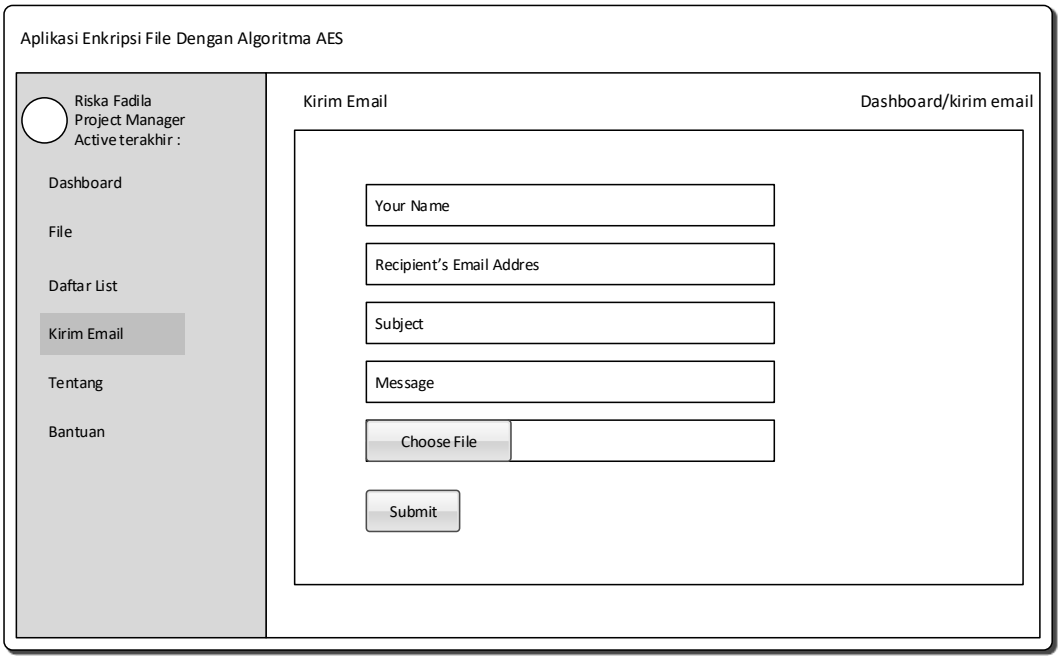
5. Halaman Sub Menu Daftar List

Pada halaman ini akan menampilkan riwayat seluruh file yang sudah di enkripsi dan dekripsi dalam sebuah data tabel.



Gambar III.8. Tampilan Hasil Halaman Daftar List

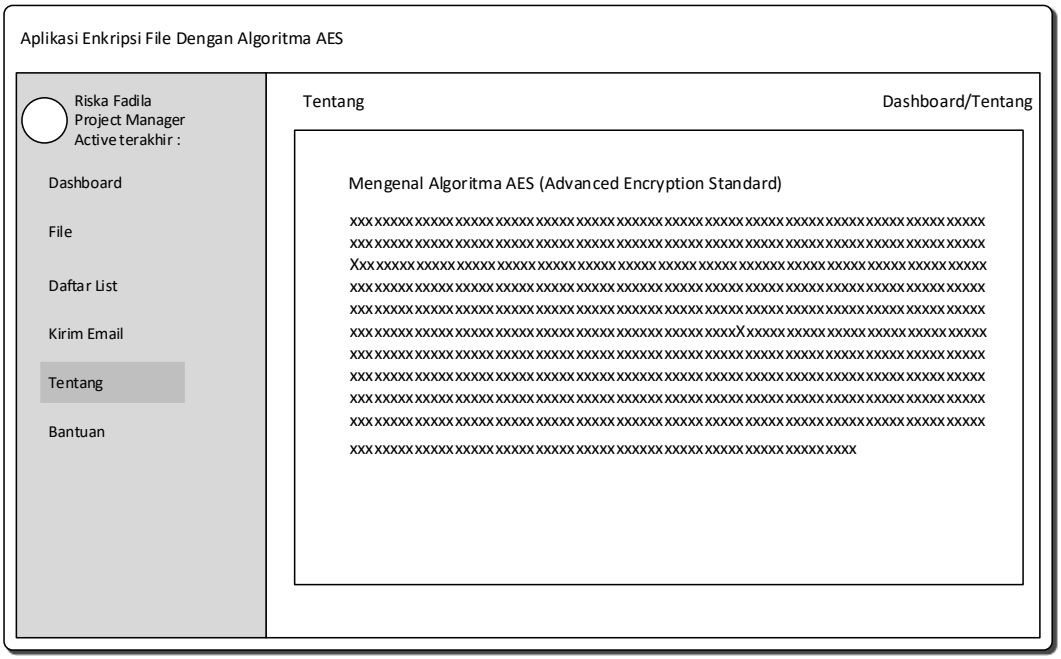
6. Halaman Menu Kirim Email



Gambar III.9. Tampilan Hasil Halaman Pengiriman email

File yang sudah dienkripsi dapat kirimkan dengan menggunakan form pengiriman email seperti yang terlihat pada gambar III.8 diatas.

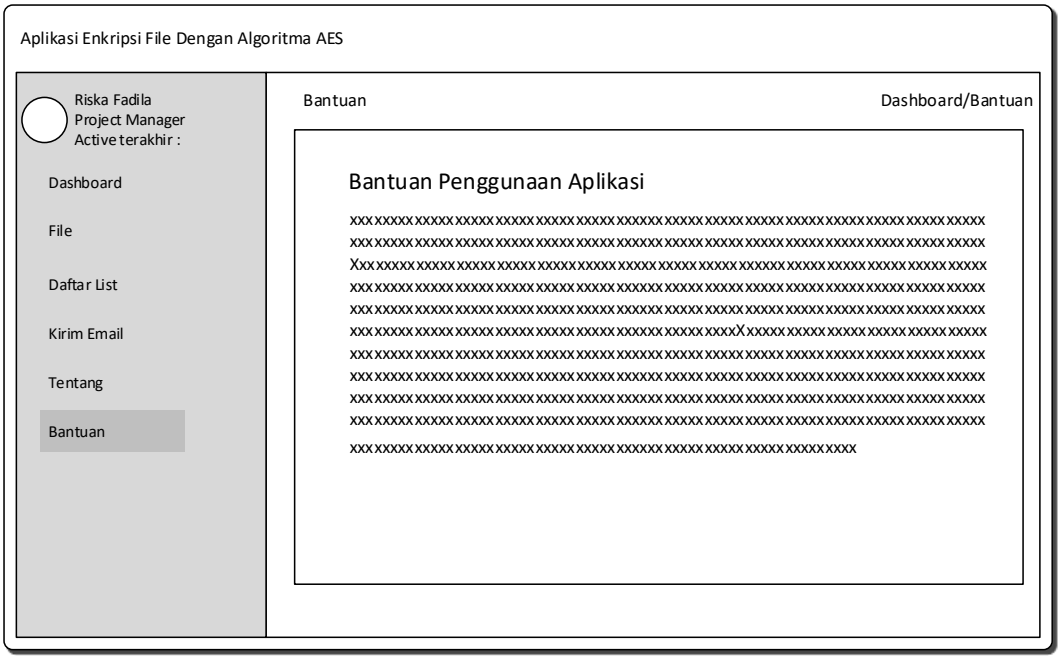
7. Halaman Menu Tentang



Gambar III.10. Tampilan Hasil Halaman Tentang aplikasi

Halaman tentang berfungsi untuk memberikan informasi singkat mengenai sejarah singkat mengenai algorit AES.

8. Halaman Menu Bantuan



Gambar III.11. Tampilan Halaman Bantuan

Halaman Bantuan berfungsi sebagai media penyampaian informasi mengenai tata cara penggunaan aplikasi, disini akan dijelaskan tahapan dan fungsi dari menu yang tersedia pada aplikasi.