BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisis Permasalahan

Perkembangan sistem keamanan sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Teknologi juga memberikan kemudahan untuk bertukar informasi sehingga keamanan data tidak dapat lepas dari berbagai aspek kegiatan manusia yang memungkinkan dapat menjaga kerahasiaan informasi tersebut, namun dalam implementasinya masih terdapat kecurangan dan ancaman terhadap data khususnya pada data ekspor kayu.

Terdapat banyak metode pengamanan data yang bisa dimanfaatkan untuk mencegah adanya kecurangan ataupun manipulasi data salah satunya menggunakan kriptografi atau teknik penyamaran lainnya. Kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi. Kecurangan terhadap data absensi karyawan tersebut dapat diatasi dengan memanfaatkan metode *RSA dan Afiine Chiper* secara *enkrip dan deskrip*.

Oleh karena itu dibutuhkan suatu sistem keamanan yang mampu menjaga kerahasiaan data dari ancaman lain yang dilakukan oleh pihak yang tidak bertanggung

jawab. Dengan memanfaatkan algoritma RSA dan *Affine chiper* ini *system* akan mengenkripsi data asli yang diinputkan pengguna menjadi *chiperteks* dengan menggunakan *key*. Sehingga data absensi yang dilakukan oleh karyawan bisa diamankan melalui keamanan algoritma RSA dan *Affine chiper* menjadi lebih muda dipahami oleh pengguna tersebut.

III.2. Strategi Pemecahan Masalah

Beberapa strategi pemecahan masalah dalam perancangan keamanan data keamanan absensi karyawan dengan menggunakan algoritma RSA dan algoritma *affine chiper* ini adalah sebagai berikut:

1. Sistem pengamanan data ekspor kayu ini dapat digunakan pada semua perangkat yang telah *support* menggunakan *Web browser*.
2. Sistem yang dibangun ini digunakan untuk mengamankan data ekspor kayu dengan menggunakan RSA yang telah disandikan isinya dan menggunakan algoritma *affine cipher*.
3. Sistem yang dibangun nantinya akan memiliki sebuah aplikasi khusus untuk mengamankan data ekspor kayu.

III.3. Algoritma RSA

RSA merupakan salah satu dari *Public Key Cryptosystem* yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data digital. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk

memfaktorkan modulus yang sangat besar Sistem yang dibangun nantinya akan memiliki sebuah aplikasi khusus untuk mendeskripsikan data ekspor kayu.

Dalam *kriptografi*, RSA adalah algoritma untuk enkripsi kunci publik. Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi dan salah satu penemuan besar pertama dalam *kriptografi* kunci publik. RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapan-penerapannya yang sangat mutakhir.

Algoritma pembentukan kunci :

- Tentukan p dan q bernilai dua bilangan prima besar, acak dan dirahasiakan, $p \neq q$, p dan q memiliki ukuran yang sama. - Hitung $n = p \times q$, dan hitung $\phi(n) = (p - 1) \times (q - 1)$, bilangan integer n disebut (RSA) modulus. -Tentukan e bilangan prima acak yang memiliki syarat : $1 < e < 1(n)$, GCD(e, i(n)) = 1, disebut e relatif prima terhadap i(n), bilangan integer n disebut (RSA) enciphering component, sehingga menghasilkan Dd (Ee(m)) = Ee(Dd(c)) ≡ md mod n.

III.4. Algoritma *Affine Cipher*

Metode *Affine Cipher* adalah perluasan dari metode Caesar Cipher, keunggulan metode ini terletak pada kuncinya, yaitu nilai integer yang menunjukkan pergeseran karakter-karakter, kekuatan kedua terletak pada barisan bilangan-bilangan yang berfungsi sebagai pengali dengan kunci. Barisan tersebut dapat berbentuk barisan bilangan ganjil, barisan fibonaci, barisan bilangan prima, serta deret yang dapat kita modifikasi sendiri.

Pada dasarnya *Affine Cipher* merupakan hasil pengembangan Caesar Cipher yang mengalikan *plaintext* dengan sebuah nilai P dan menambahkannya dengan sebuah pergeseran b menghasilkan *Ciphertext* C dinyatakan dengan fungsi kongruen :

$$C \equiv m\,P + b \pmod{n}$$

Yang mana n adalah ukuran alphabet, m adalah bilangan bulat yang harus relatif prima dengan n (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan) dan b adalah jumlah pergeseran (Caesar Cipher adalah bentuk khusus dari *Affine Cipher* dengan m=1). Untuk melakukan deskripsi, harus dipecahkan untuk memperoleh P. Solusi kekongruenan tersebut hanya ada jika inver m (mod n), dinyatakan dengan m -1. Jika m -1 ada maka dekripsi dilakukan dengan persamaan sebagai berikut:

$$P \equiv m\text{-}1(C - b\,) \pmod{n}$$

III.4.1. Enkripsi

1. ***Affine Cipher***

Berikut adalah contoh enkripsi menggunakan metode *Affine Cipher* :

Misalkan *plaintext*:

eben

Yang ekuivalen dengan:

4 1 4 13 (dengan memisalkan ‘A’ = 0, ‘B’ = 1 dst)

Dienkripsi dengan *Affine Cipher* dengan mengambil m = 7 (karena 7 relatif prima dengan 26) dan b = 10. Karena alphabet yang digunakan 26 huruf, maka n = 26.

Enkripsi *plaintext* dihitung dengan kekongruenan:

$C \equiv 7P + 10 \pmod{26}$

Perhitungannya adalah sebagai berikut:

P1 = 4 ⟶ $C_1 \equiv 7 * 4 + 10 \equiv 38 \pmod{26} \equiv 12$ (huruf ‘m’)

P2 = 1 ⟶ $C_2 \equiv 7 * 1 + 10 \equiv 17 \pmod{26} \equiv 17$ (huruf ‘r’)

P3 = 4 ⟶ $C_3 \equiv 7 * 4 + 10 \equiv 38 \pmod{26} \equiv 12$ (huruf ‘m’)

P4 = 13 ⟶ $C_4 \equiv 7 * 13 + 10 \equiv 101 \pmod{26} \equiv 4$ (huruf ‘x’)

Ciphertext yang dihasilkan adalah:

mrmx

2. RSA

Penerapan algoritma Algoritma *RSA*. Pada sistem ini akan mengenkripsi data file berekstensi dokumen *word* disimpan ke dalam sistem dengan menerapkan algoritma *RSA*.

Contoh Proses Enkrip :

Plaintext : mrmx

Enkrip Pertama :

m = 109

$C_i = P_i^e \bmod n$

$= 109^7 \bmod 143$

$= 182.803.912.081.669 \bmod 143$

= 21

Enkrip Kedua :M4

r = 114

$C_i = P_i^e \bmod n$

$= 114^7 \bmod 143$

$= 250,226,879,128,704 \bmod 143$

$=49$

Enkrip Ketiga :

m = 109

$C_i = P_i^e \bmod n$

$= 109^7 \bmod 143$

$= 182.803.912.081.669 \bmod 143$

$= 21$

Enkrip Keempat :

x = 120

$C_i = P_i^e \bmod n$

$= 120^7 \bmod 143$

$= 358,318,080,000,000 \bmod 143$

$=120$

Chipertext = (1.077, 917, 1.077, 20)

III.4.2. Dekripsi

1. **RSA**

Berikut ini adalah dekrip dari metode RSA, dekrip metode RSA merupakan fungsi eksponensial dalam modular n dengan menggunakan kunci *private* sebagai berikut :

$P_i = C_i^d \bmod n$

1. Terima kunci

d = 103

n = 143

Plainteks = (21, 49, 21, 120)

2. Dekrip *Ciphertext*

Contoh Proses Dekrip :

Dekrip Pertama :

C = 21

$P_i = C_i^d \bmod n$

$= 21^{103} \bmod 143$

= 109 = m

Dekrip Kedua :

C = 49

$P_i = C_i^d \bmod n$

$= 49^{103} \bmod 143$

= 114 = r

Dekrip Ketiga :

C = 21

$P_i = C_i^d \bmod n$

$= 21^{103} \bmod 143$

= 109 = m

Dekrip Keempat :

C = 120

$P_i = C_i^d \bmod n$

$= 120^{103} \bmod 143$

= 120 = x

Plaintext : mrmx

2. *Affine Cipher*

Untuk melakukan dekripsi, pertama-tama dihitung $7^{-1} \pmod{26}$, yang dapat dihitung dengan memecahkan kekongruenan lanjar:

$7x \equiv 1 \pmod{26}$.

Solusinya adalah $x \equiv 15 \pmod{26}$ sebab $7.15 = 105 \equiv 1 \pmod{26}$. Jadi, untuk dekripsi digunakan kekongruenan:

$P \equiv 15(C - 10) \pmod{26}$

Perhitungannya adalah sebagai berikut:

$C_1 = 12 \longrightarrow P_1 \equiv 15 * (12 - 10) \equiv 30 \pmod{26} \equiv 4$ (huruf 'e')

$C_2 = 17 \longrightarrow P_2 \equiv 15 * (17 - 10) \equiv 105 \pmod{26} \equiv 1$ (huruf 'b')

$C_3 = 12 \longrightarrow P_3 \equiv 15 * (12 - 10) \equiv 30 \pmod{26} \equiv 4$ (huruf 'e')

$C_4 = 4 \longrightarrow P_4 \equiv 15 * (4 - 10) \equiv -90 \pmod{26} \equiv 13$ (huruf 'n')

Plaintext yang dihasilkan adalah:

Eben

III.5. Perancangan

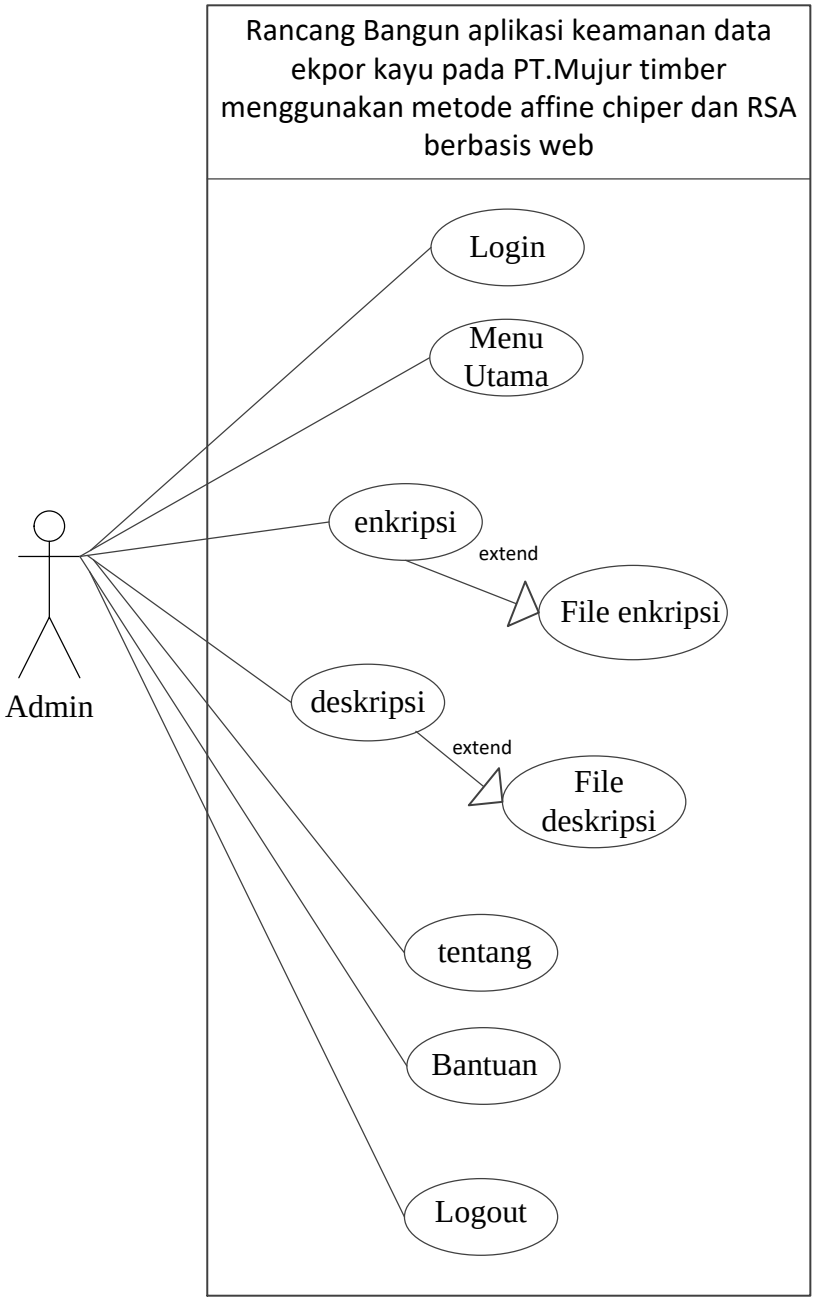
Perancangan aplikasi merupakan perancangan yang dilakukan untuk merancang sebuah aplikasi dengan menggunakan salah satu bahasa pemrograman PHP, dalam kasus ini penulis merancang sebuah aplikasi data ekspor kayu dengan menggunakan *PHP*.

III.6. Desain Sistem

Perancangan ini akan memberikan penjelasan mengenai rancangan aplikasi serta pembentukan dan pembangunan aplikasi *kriptografi* algoritma *RSA* dan *Affine Cipher* dalam mengamankan data ekspor kayu

III.6.1. *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.1 sebagai berikut:



Gambar III.2. ***Use Case Diagram***

Penjelasan **:**

1. Admin Bisa Melakukan Login, Kemudian Masuk Kedalam Menu Utama
2. Kemudian Admin Masuk Kedalam form Enkripsi dan Dekripsi selanjutnya Masuk Kedalam File Enkripsi Dan Deskripsi

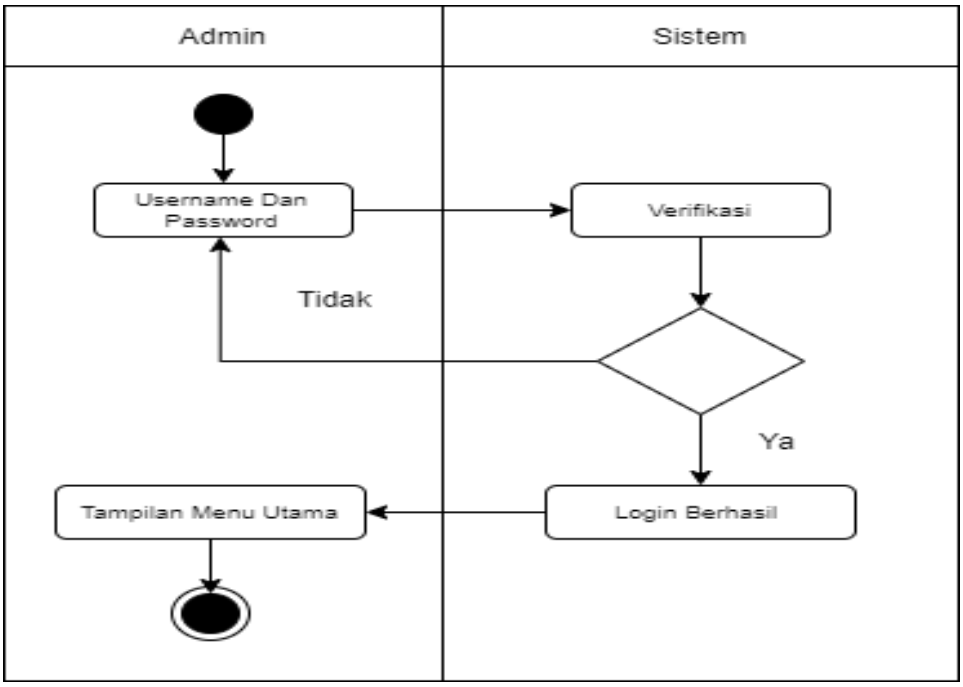
3. Kemudian Admin Masuk Ke dalam form tentang dan bantuan kemudian Logout.

III.6.2. *Activity Diagram*

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

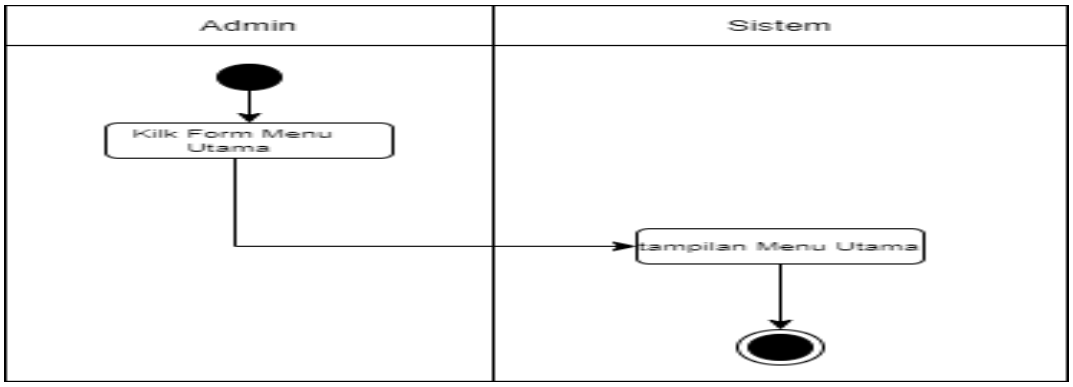
1. *Activity Diagram Login*

Activity Diagram Login berfungsi untuk



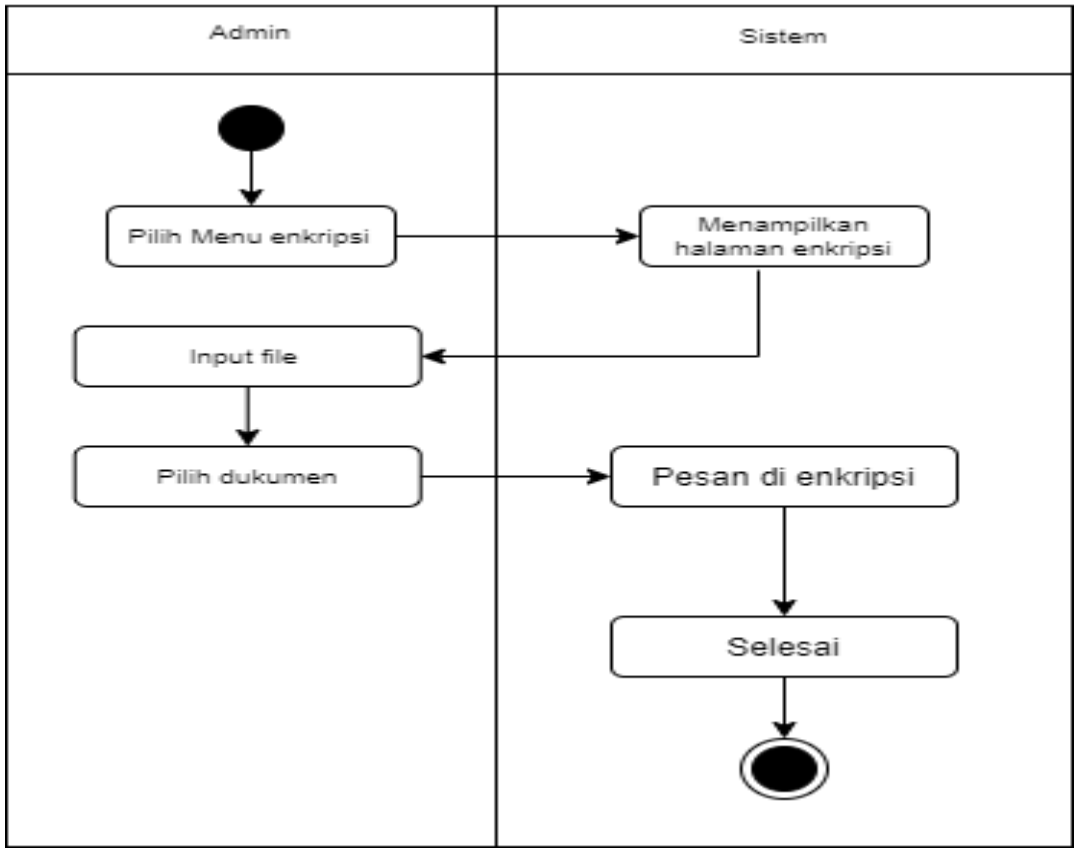
Gambar III.3. *Activity Login* Diagram *Affine Cipher dan RSA*

2. *Activity Diagram Menu Utama*



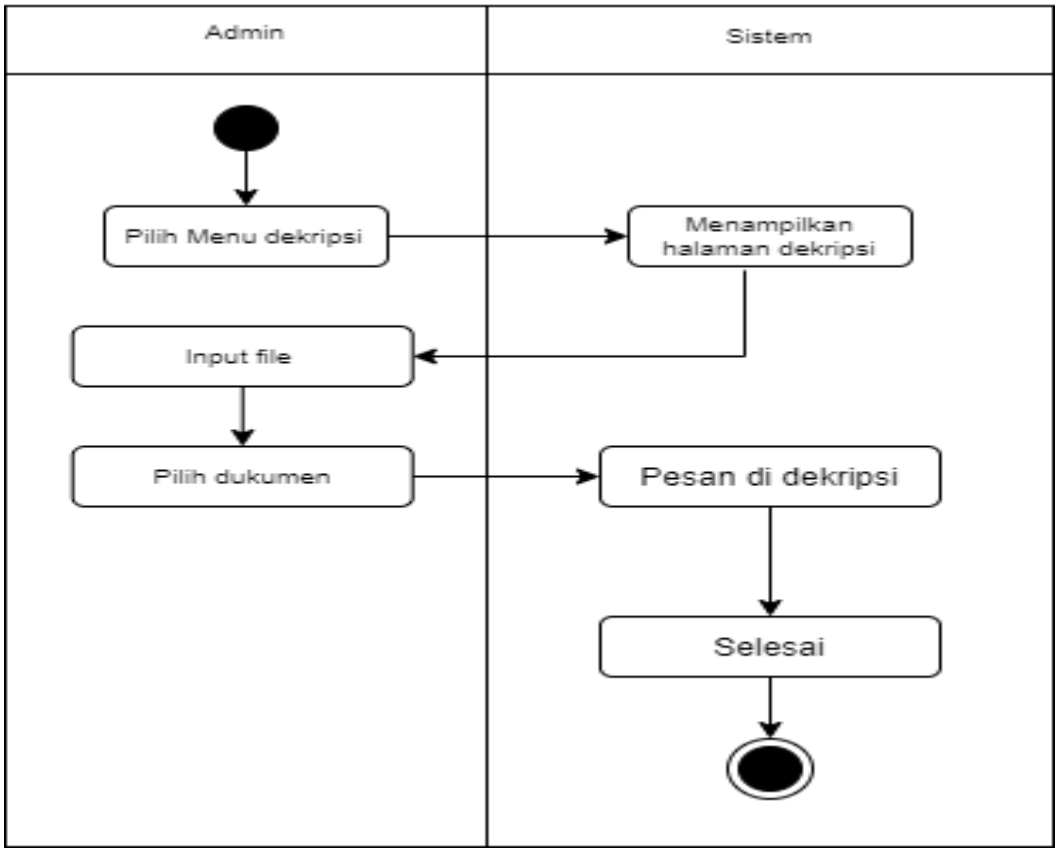
Gambar III.4. *Activity* Diagram *Menu Utama*

3. *Activity Diagram* Enkripsi *Affine Cipher* Dan RSA



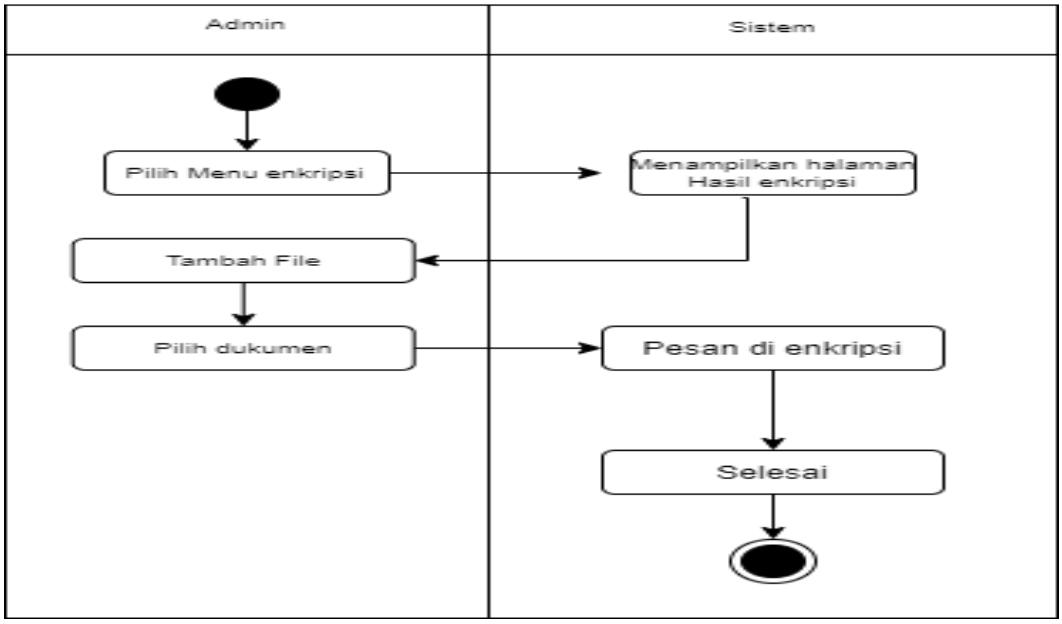
Gambar III.5. *Activity* Diagram Enkripsi *Affine Cipher dan RSA*

4. *Activity Diagram* dekripsi *Affine Cipher* Dan RSA



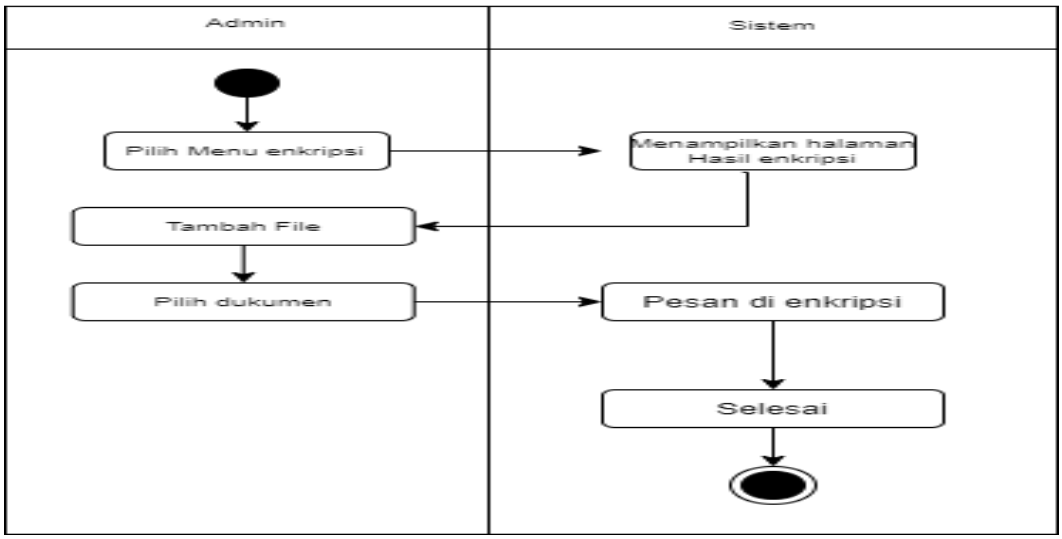
Gambar III.6. *Activity* Diagram Dekripsi *Affine Cipher* Dan *RSA*

5. *Activity Diagram* Hasil Enkripsi Affine Cipher Dan RSA



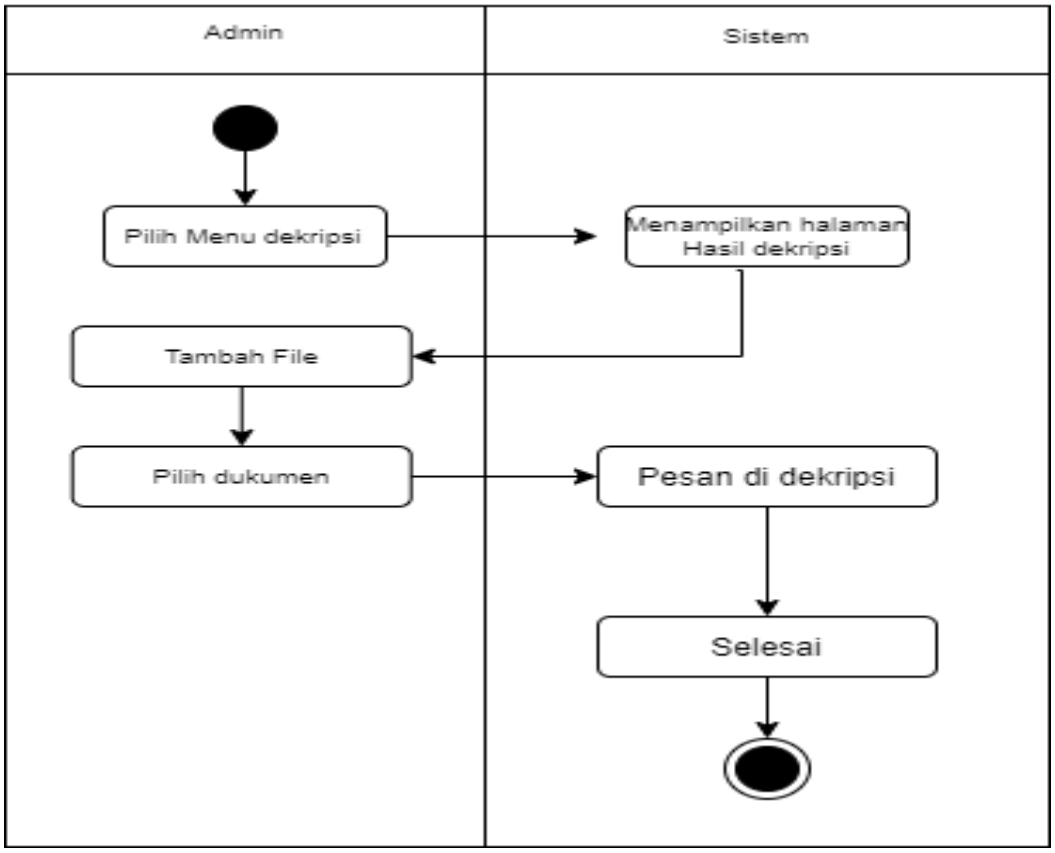
Gambar III.7. *Activity* Diagram Hasil Enkripsi *Affine Cipher* Dan *RSA*

6. *Activity Diagram* Hasil Enkripsi Affine Cipher Dan RSA



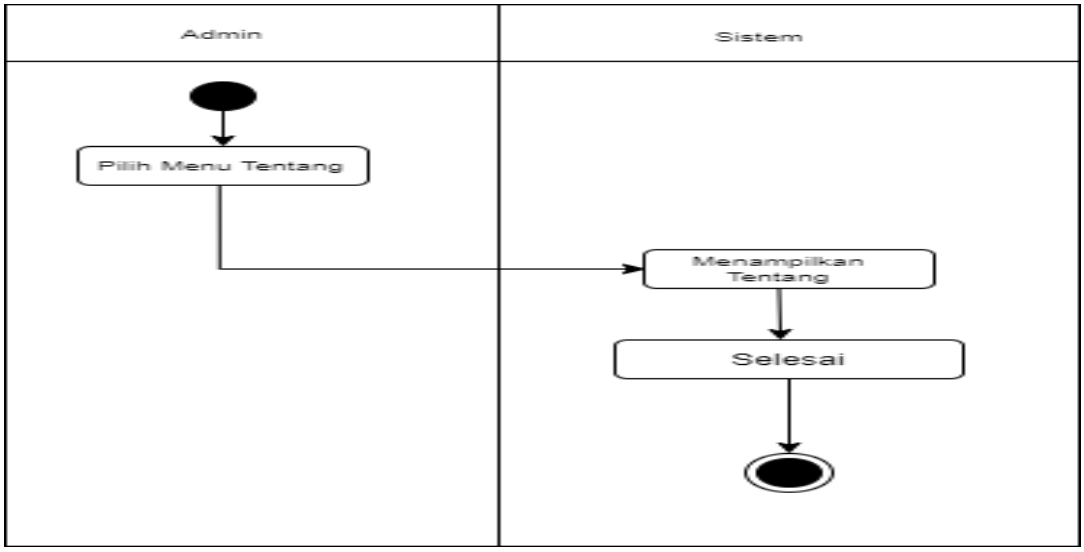
Gambar III.8. *Activity* Diagram Hasil Enkripsi *Affine Cipher* Dan *RSA*

7. *Activity Diagram* Hasil Dekripsi Affine Cipher Dan RSA



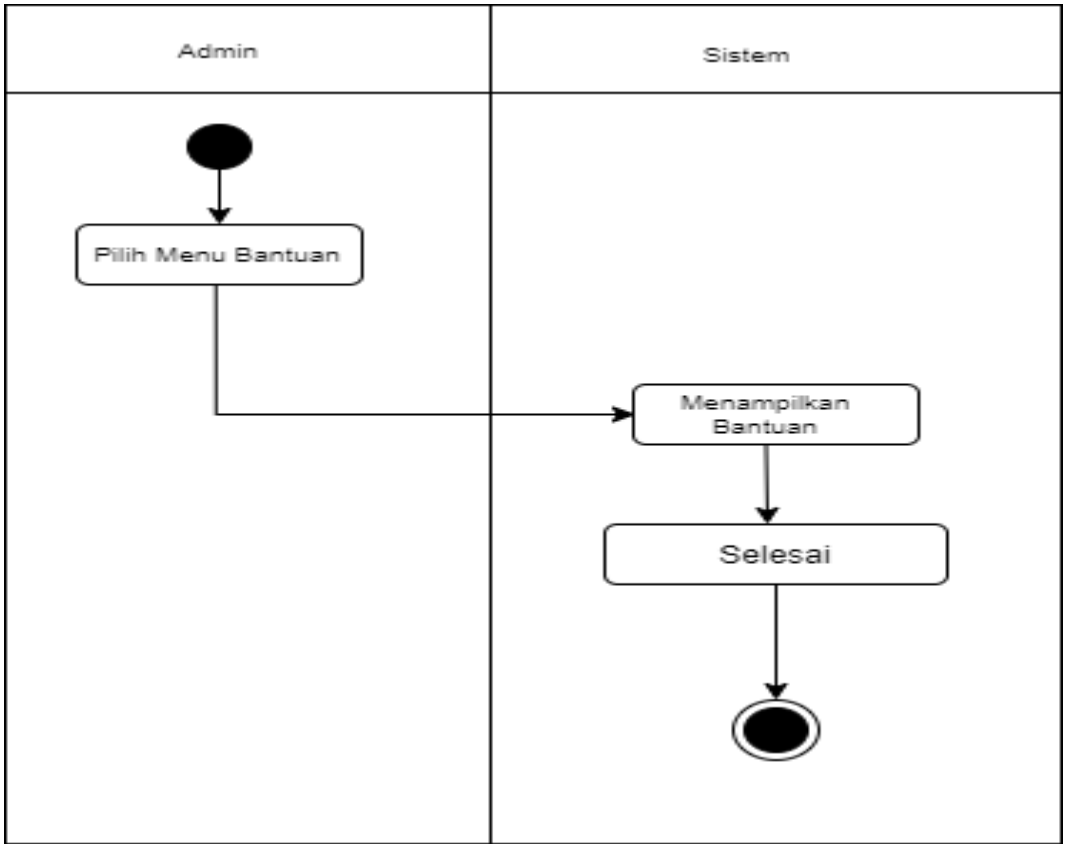
Gambar III.9. *Activity* Diagram Hasil Dekripsi *Affine Cipher* Dan *RSA*

8. *Activity Diagram* Tentang



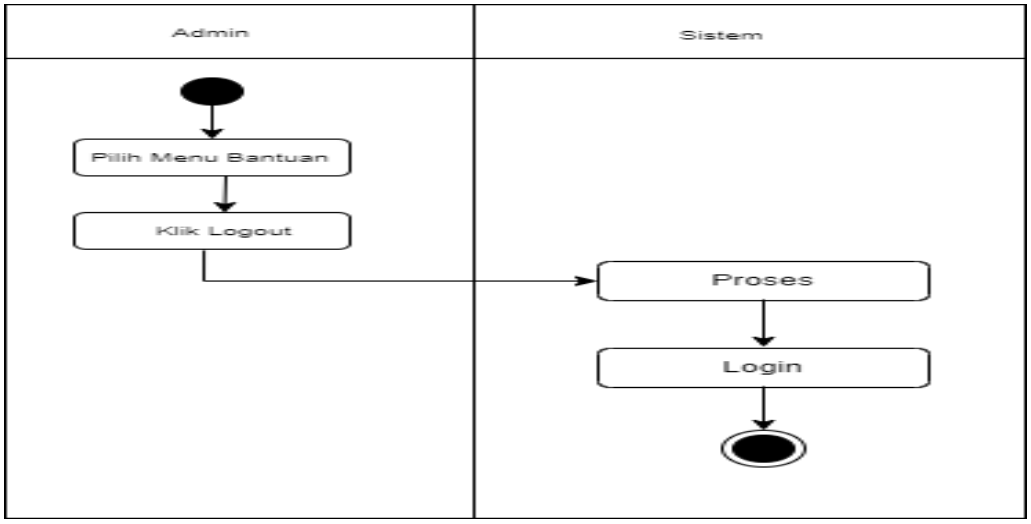
Gambar III.10. *Activity* Diagram Tentang

9. *Activity Diagram* Bantuan



Gambar III.11. *Activity* Diagram Bantuan

10. *Activity Diagram* Logout



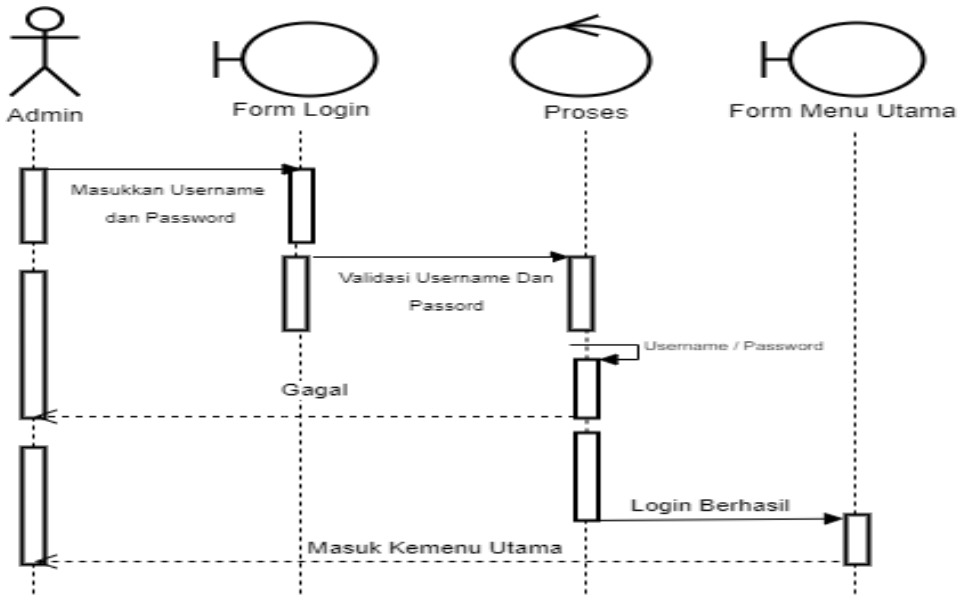
Gambar III.12. *Activity* Diagram Bantuan

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*

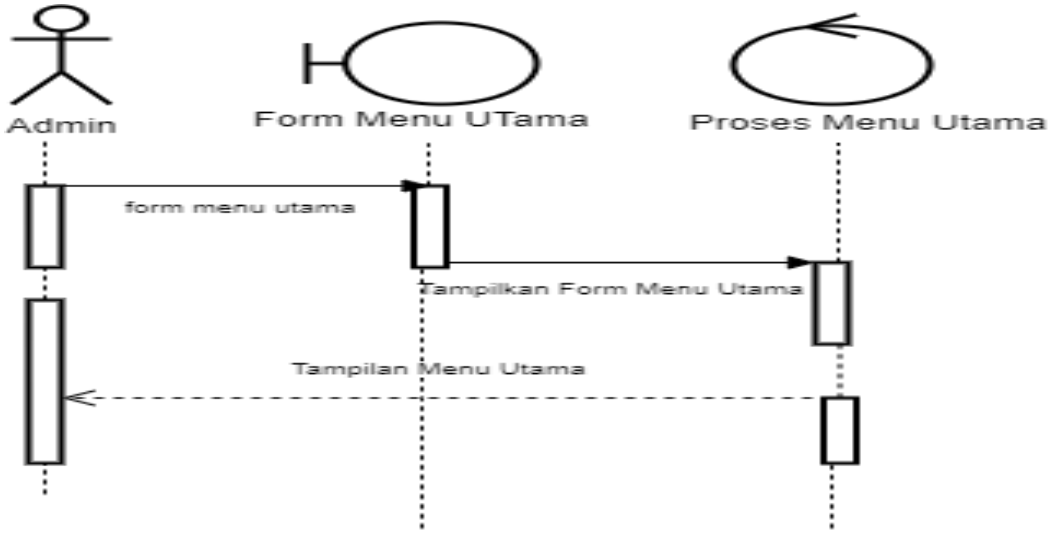
Serangkaian kerja melakukan *login* dapat dilihat pada Gambar III.13 Dibawah ini.



Gambar III.13. ***Sequence Diagram Login***

2. ***Sequence Diagram*** **Menu Utama** ***RSA*** **Dan** ***Affine Cipher***

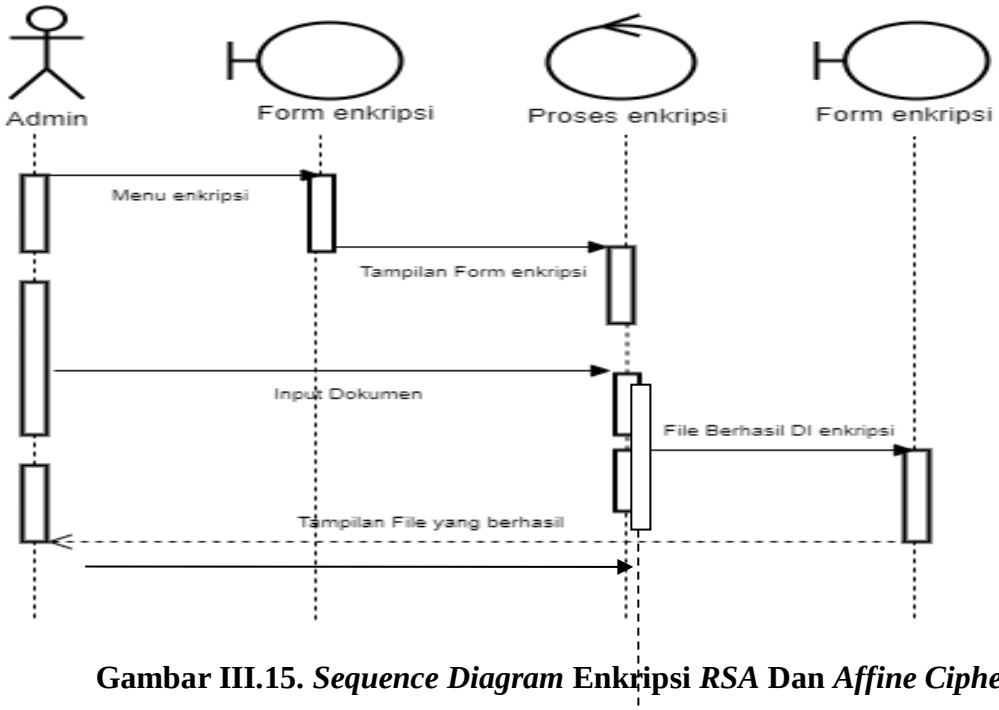
Serangkaian kerja melakukan Menu Utama *RSA* Dan *Affine Cipher* dapat dilihat pada Gambar III.14. dibawah ini.



Gambar III.14. ***Sequence Diagram*** **Enkripsi** ***RSA*** **Dan** ***Affine Cipher***

3. *Sequence Diagram* Enkripsi *RSA* Dan *Affine Cipher*

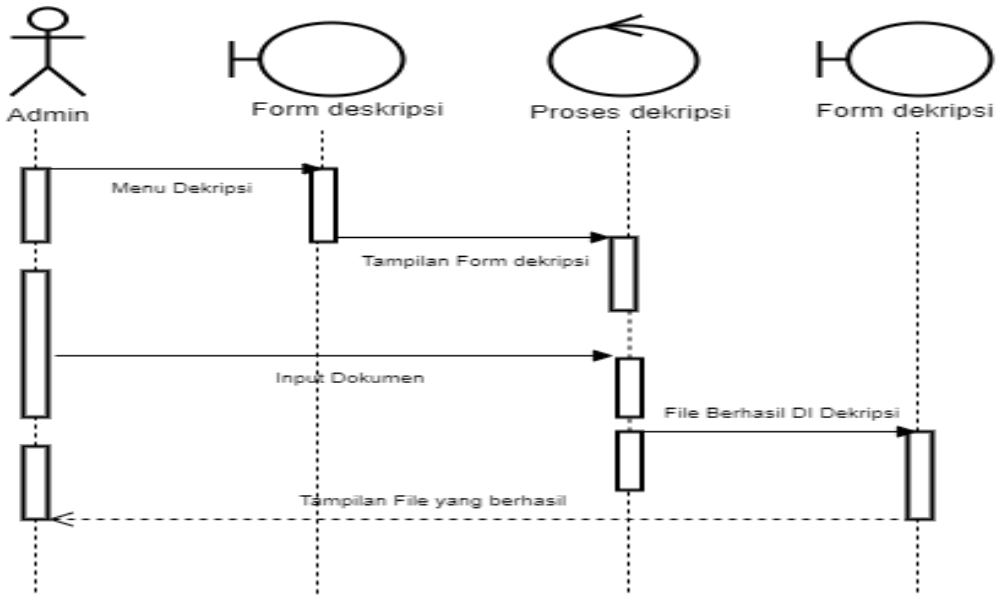
Serangkaian kerja melakukan enkripsi *RSA* Dan *Affine Cipher* dapat dilihat pada Gambar III.15. dibawah ini.



Gambar III.15. *Sequence Diagram* Enkripsi *RSA* Dan *Affine Cipher*

4. *Sequence Diagram* Dekripsi *Affine Cipher* Dan *RSA*

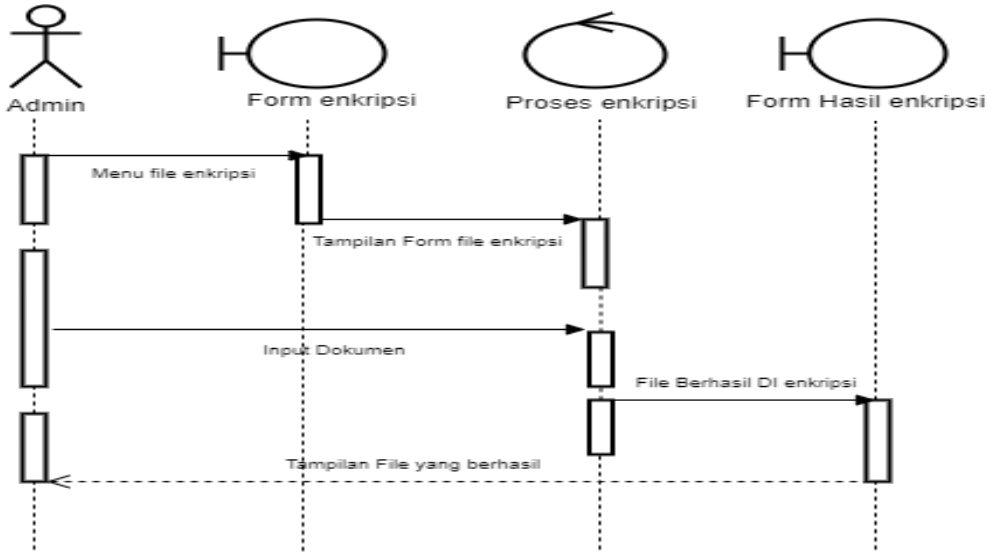
Serangkaian kerja melakukan dekripsi *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.16 dibawah ini.



Gambar III.16. *Sequence Diagram* Dekripsi *Affine Cipher* Dan *RSA*

5. *Sequence Diagram* Hasil Enkripsi *Affine Cipher* Dan *RSA*

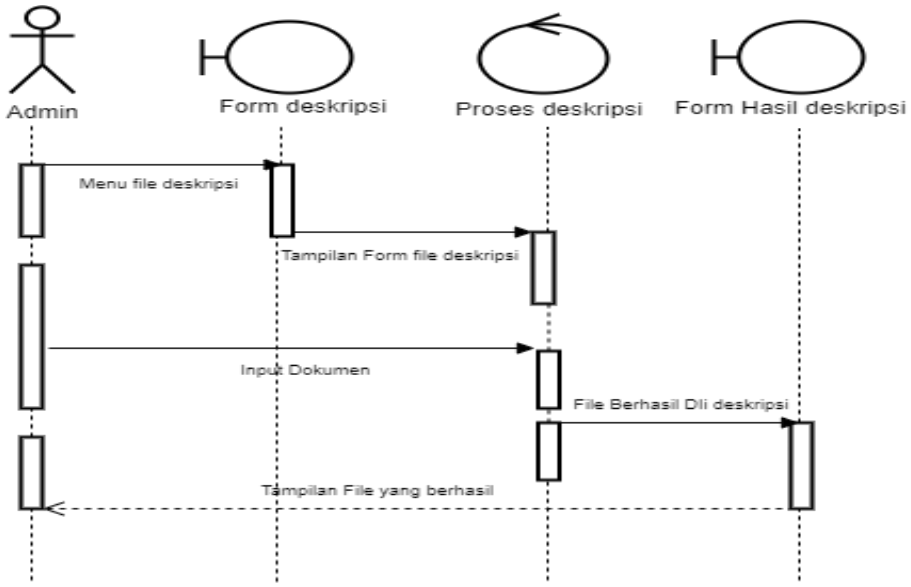
Serangkaian kerja melakukan Hasil Enkripsi *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.17 dibawah ini.



Gambar III.17. *Sequence Diagram* Hasil Enkripsi *Affine Cipher* Dan *RSA*

6. *Sequence Diagram* Hasil Deskripsi *Affine Cipher* Dan *RSA*

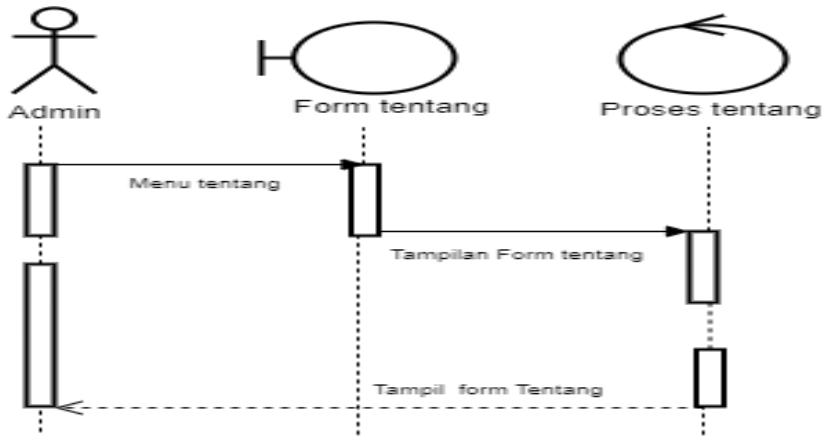
Serangkaian kerja melakukan Hasil Deskripsi *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.18 dibawah ini.



Gambar III.18. *Sequence Diagram* Hasil Deskripsi *Affine Cipher* Dan *RSA*

7. *Sequence Diagram* Tentang *Cipher* Dan *RSA*

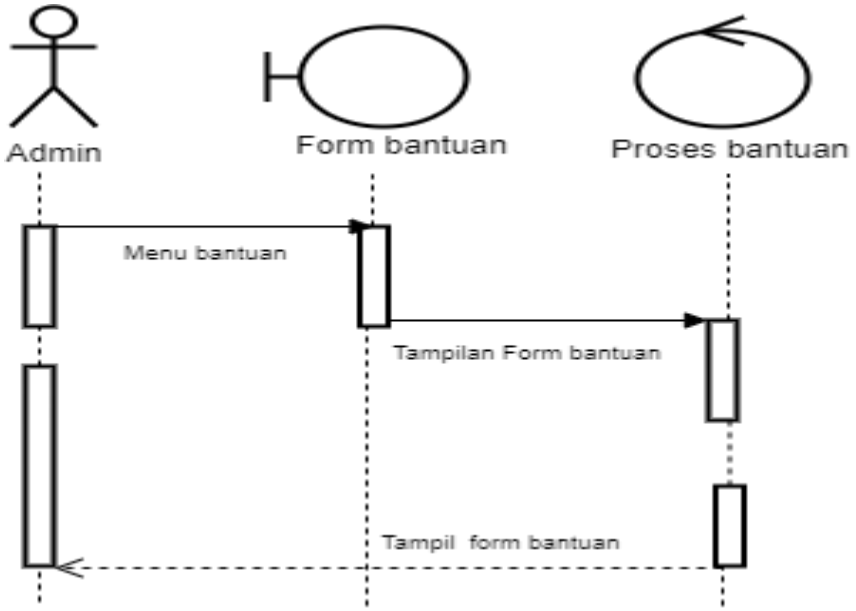
Serangkaian kerja melakukan Tentang *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.19 dibawah ini.



Gambar III.19. *Sequence Diagram* Tentang *Affine Cipher* Dan *RSA*

8. *Sequence Diagram* Bantuan *Cipher* Dan *RSA*

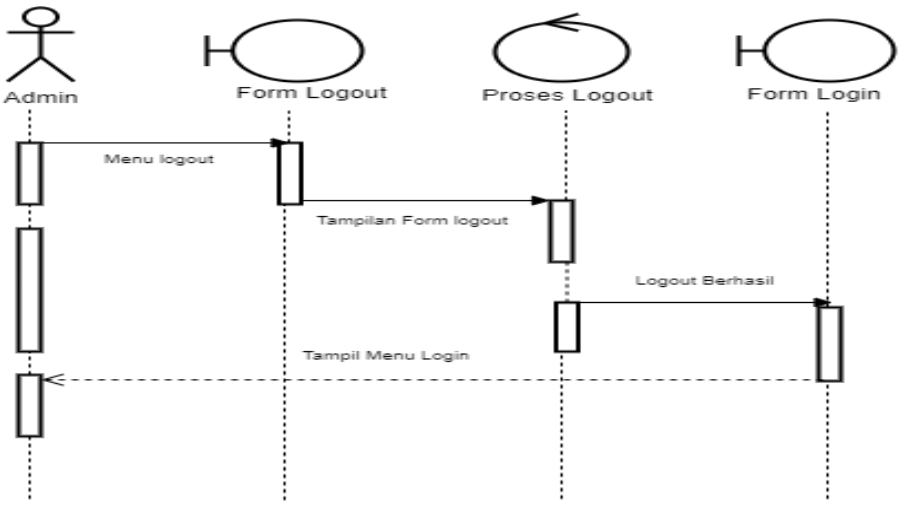
Serangkaian kerja melakukan Bantuan *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.20 dibawah ini.



Gambar III.20. *Sequence Diagram* Bantuan *Affine Cipher* Dan *RSA*

9. *Sequence Diagram* Log Out

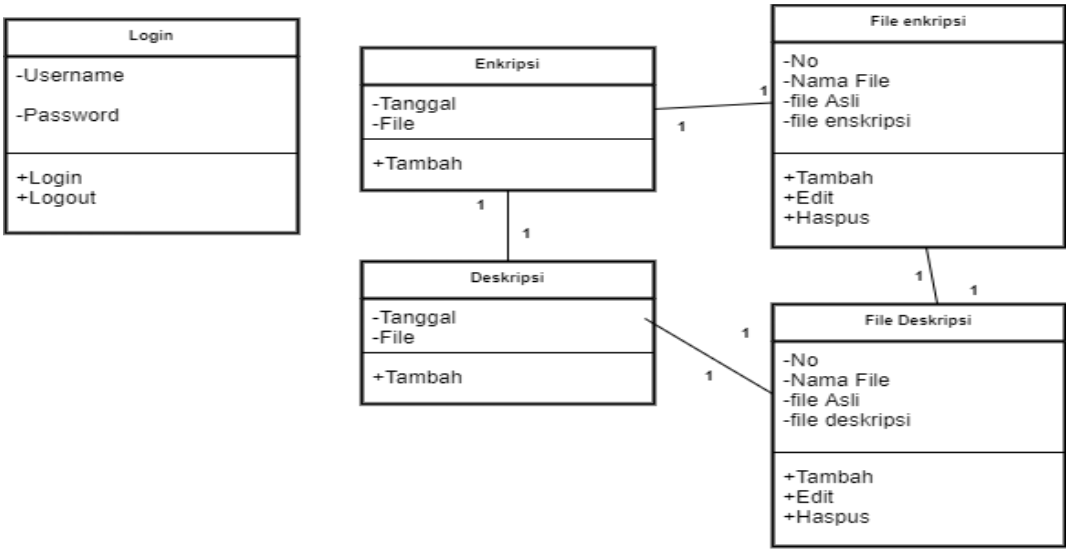
Serangkaian kerja melakukan log out dapat dilihat pada Gambar III.21 dibawah ini.



Gambar III.21. *Sequence Diagram* Log Out

III.6.4 *Class* Diagram

Class Diagram Keamanan Data File Ms. *Word* RSA dan *Affine Cipher* dapat dilihat pada Gambar III.10.



Gambar III.10. *Class Diagram* Keamanan Data File Ms. *Word Affine Cipher* dan RSA

III.7. Desain *Database*

III.7.1. Desain Tabel

Perancangan struktur database adalah untuk menentukan *file database* yang digunakan seperti *field*, tipe data, ukuran data. Sistem ini dirancang dengan menggunakan database *MySql.*

1. Tabel Admin

Tabel Admin berfungsi sebagai tabel untuk menampung data-data pengguna program yang akan menggunakan program.

Nama Database : dbadmin

Nama Tabel : tbl_admin

Primary Key : kd_admin

Foreign Key : -

Tabel III.1. Tabel Admin

No	Nama Field	Tipe Data	Ukuran	Kunci
1.	Kd_admin	Varchar	50	*Primary Key*
2.	nama_admin	Varchar	35	-
3.	username_admin	Varchar	30	-
4	password_admin	varchar	256	-

2. File_enkripsi

File enkripsi berfungsi sebagai tabel untuk menampung data-data pengguna program yang akan menggunakan program.

Nama Database : dbadmin

Nama Tabel : file_enkripsi

Primary Key : id

Foreign Key : -

Tabel III.2. Tabel Enkripsi

No	Nama Field	Tipe Data	Ukuran	Kunci
1.	id	Varchar	50	*Primary Key*
2.	Nama_file	Varchar	35	-
3.	tanggal	Varchar	30	-
4	lokasi_file_asli	varchar	255	-
5	lokasi_file_enkripsi	varchar	225	-
6	log_affine	longtext	-	-
7	log_rsa	longtext	-	-

1. File_deskripsi

File enkripsi berfungsi sebagai tabel untuk menampung data-data pengguna program yang akan menggunakan program.

Nama Database : dbadmin

Nama Tabel : file_deskripsi

Primary Key : id

Foreign Key : -

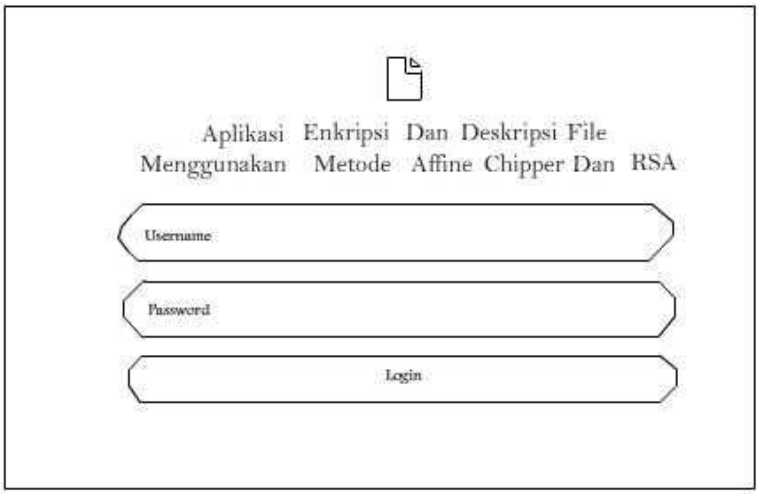
Tabel III.2. Tabel Deskripsi

No	Nama Field	Tipe Data	Ukuran	Kunci
1.	id	Varchar	50	*Primary Key*
2.	Nama_file	Varchar	35	-
3.	tanggal	Varchar	30	-
4	lokasi_file_asli	varchar	255	-
5	lokasi_file_enkripsi	varchar	225	-
6	log_affine	longtext	-	-
7	log_rsa	longtext	-	-

III.8. Desain *Interface*

III.8.1. Perancangan *Form Login*

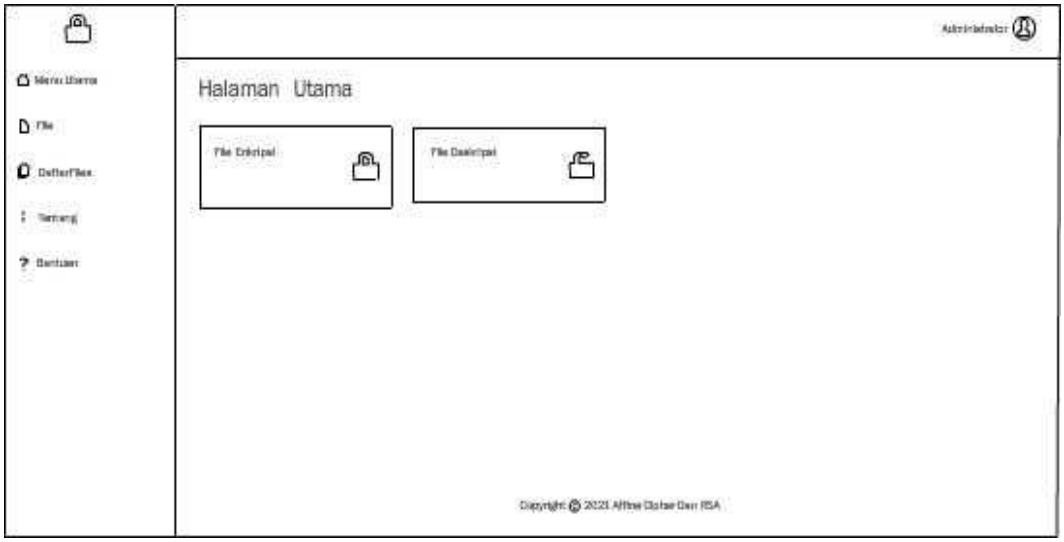
Perancangan *form login* ini terdiri dari satu buah gambar, satu buah *checkbox*, empat buah *label*, dua buah *button* dan dua buah *textfield*. Untuk lebih jelasnya, perancangan *form login* dapat dilihat pada Gambar III.11 sebagai berikut:.



Gambar III.11. Perancangan *Form Login*

III.8.2. Perancangan *Form* Utama

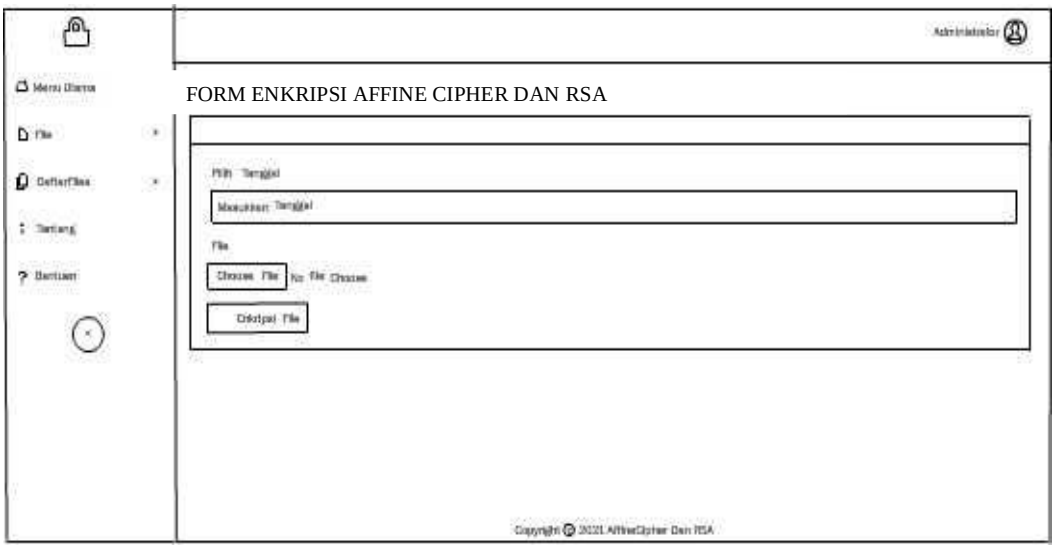
Perancangan *form* Utama ini terdiri dari empat buah *menu bar*. Untuk lebih jelasnya, perancangan *form* Utama dapat dilihat pada Gambar III.12 sebagai berikut:



Gambar III.12. Perancangan *Form* Utama

III.8.3. Perancangan *Form* Enkripsi *RSA* Dan *Affine Cipher*

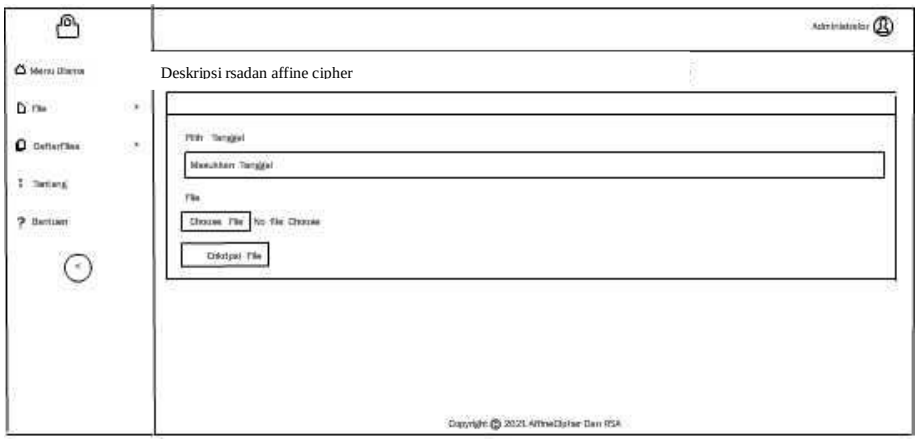
Perancangan *form* Enkripsi *RSA* Dan *Affine Cipher*, untuk lebih jelasnya, perancangan *form* Enkripsi dapat dilihat pada Gambar III.13 sebagai berikut:



Gambar III.13. Perancangan *Form* Enkripsi *Affine Cipher dan RSA*

III.8.4. Perancangan *Form* Dekripsi *RSA* Dan *Affine Cipher*

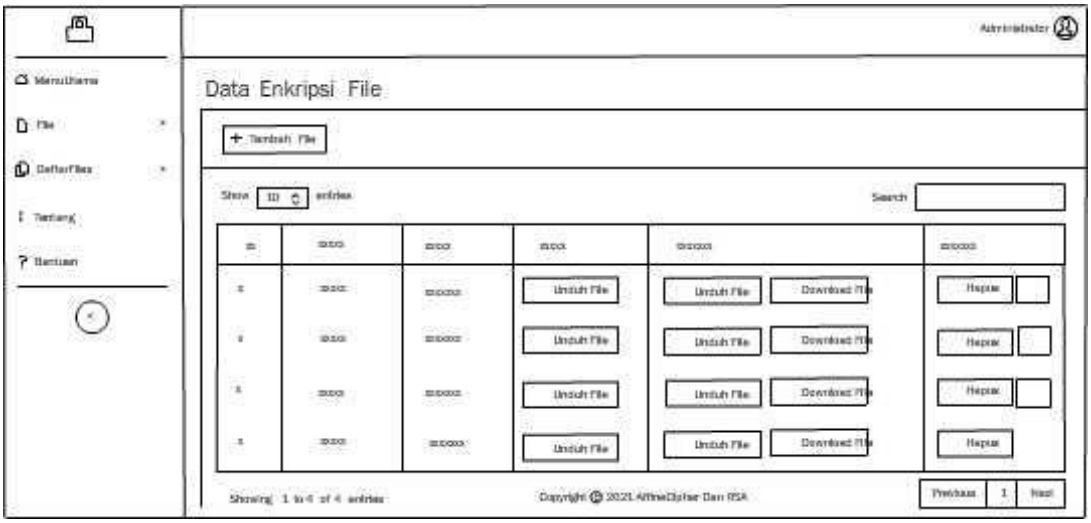
Perancangan *form* Dekripsi *RSA* Dan *Affine Cipher*, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar III.14 sebagai berikut:



Gambar III.14. Perancangan *Form* Dekripsi *RSA* Dan *Affine Cipher*

III.8.5. Perancangan *Form* Data Enkripsi *RSA* Dan *Affine Cipher*

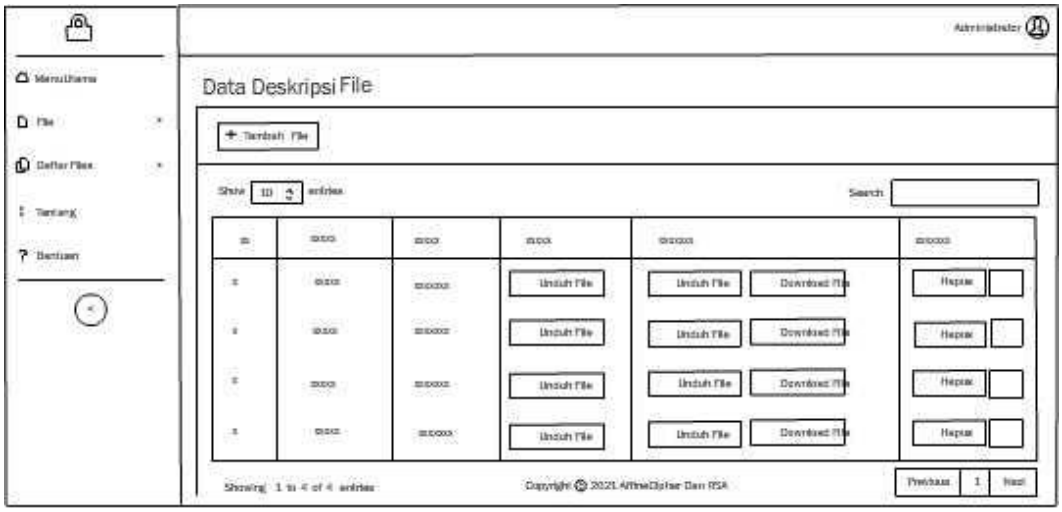
Perancangan *form* Enkripsi *RSA* Dan *Affine Cipher*, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar III.15 sebagai berikut:



Gambar III.15. Perancangan *Form* Data Enkripsi *RSA* Dan *Affine Cipher*

III.8.6. Perancangan *Form* Data Deskripsi *RSA* Dan *Affine Cipher*

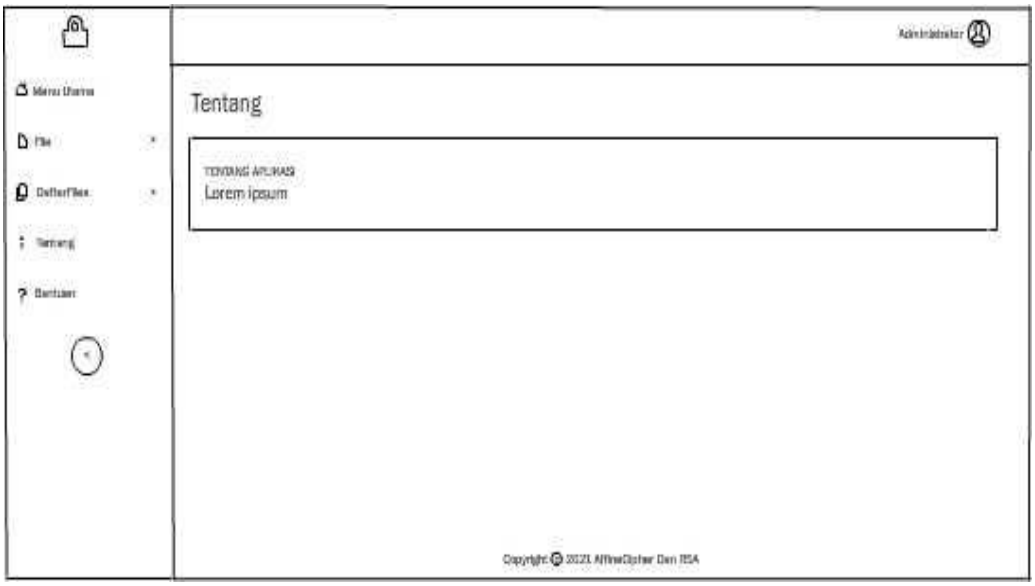
Perancangan *form* Dekripsi *RSA* Dan *Affine Cipher*, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar III.16 sebagai berikut:



Gambar III.16. Perancangan *Form* Data Deskripsi *RSA* Dan *Affine Cipher*

III.8.7. Perancangan *Form* Tentang

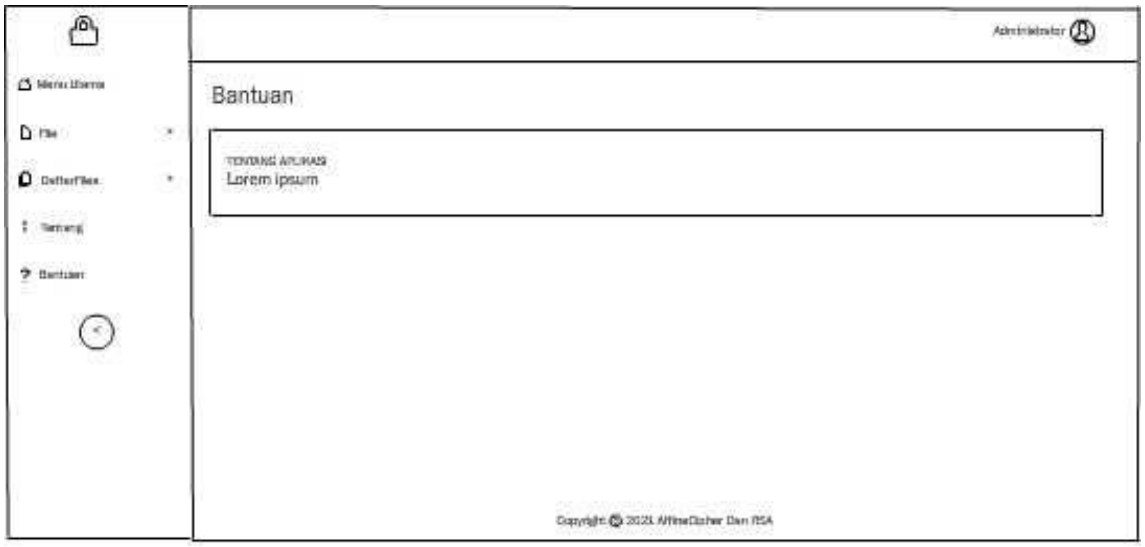
Perancangan *form* Tentang, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar III.17 sebagai berikut:



Gambar III.17. Perancangan *Form* Tentang

III.8.8. Perancangan *Form* Bantuan

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



Gambar III.18. Perancangan *Form* Bantuan