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 keamanan absensi karyawan.

Pada saat ini perusahaan belum memiliki aplikasi yang melakukan pengamanan data yang berguna untuk mengamankan data absensi, sehingga kapan saja data absensi bisa mengalami kebocoran atau hilang data diakibatkan oleh orang-orang yang tidak bertanggung jawab.

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 *Affine Cipher* dan RSA ini system akan mengenkripsi data asli yang diinputkan pengguna menjadi *chipertext* dengan menggunakan *key*. Sehingga data absensi yang dilakukan oleh karyawan bisa diamankan melalui keamanan algoritma *Affine Cipher* dan RSA menjadi lebih mudah dipahami oleh pengguna tersebut.

III.2. Penerapan Algoritma

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 n yang sangat besar Sistem yang dibangun nantinya akan memiliki sebuah aplikasi khusus untuk mendeskripsikan data keamanan absensi karyawan yang ada pada data absensi.

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 pertaman 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.

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 $\phi(n) = (p - 1)x (q - 1)$, 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 $Dd (Ee(m)) = Ee(Dd(c)) \equiv md \bmod n$.

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.

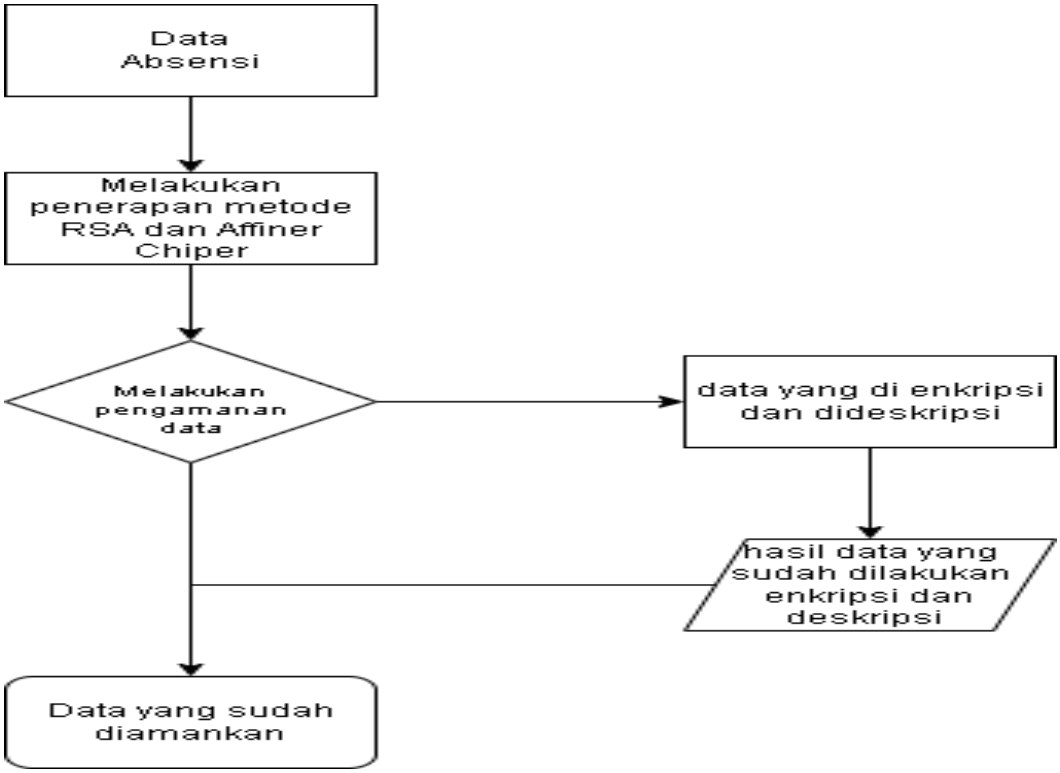
Pada dasarnya *Affine Cipher* merupakan hasil pengembangan *Caesar Cipher* yang mengalikan plaintext dengan sebuah nilai P dan menambahkannya dengan sebuah pergeseran b menghasilkan *Ciphertext* C dinyatakan dengan fungsi kongruen :

$C \equiv m\,P + b \pmod{n}$ …… (1)

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:

$P \equiv m\text{-}1(C - b) \pmod{n}$ …… (2)

Kemudian ini adalah alur dari proses pengamanan data absensi karyawan yang telah dirancang sehingga mempermudah bagaimana untuk proses pengamanan data, dapat dilihat pada Gambar III.1.



Gambar III.1. *Flowchart* penerapan metode *Affine Chiper* Dan RSA

III.3. Studi Kasus

Pada saat ini PT. Duta Jelita belum memiliki sistem aplikasi keamanan data absensi karyawan, maka dari itu ini adalah proses enkripsi dan deskripsi metode *Affine Cipher* dan RSA.

1. *Affine Cipher*

Berikut adalah contoh enkripsi menggunakan metode *Affine Cipher* :

Misalkan absensi:

Mutiara Aulia

Yang ekuivalen dengan:

7 * 12 + 10 Mod 26 = 16

7 * 20 + 10 Mod 26 = 20

7 * 19 + 10 Mod 26 = 13

7 * 8 + 10 Mod 26 = 14

7 * 0 + 10 Mod 26 = 10

7 * 17 + 10 Mod 26 = 25

7 * 0 + 10 Mod 26 = 10

7 * 0 + 10 Mod 26 = 10

7 * 20 + 10 Mod 26 = 20

7 * 11 + 10 Mod 26 = 9

7 * 8 + 10 Mod 26 = 14

7 * 0 + 10 Mod 26 = 10

Cipherteks : qunokzk kujok

2. RSA

Penerapan algoritma Algoritma *RSA*. Pada sistem ini akan mengenkripsi data absensi yang disimpan ke dalam sistem dengan menerapkan algoritma *RSA*.

Contoh Proses Enkrip :

Plainteks RSA : qunokzk

kujok

Nilai e : 7

Nilai n : 143

Konversi ASCII : 13 10 113 117 110 111 107 122 107 32 107 117 106 111 107

ASCII^e mod n : (13^7 mod 143) (10^7 mod 143) (113^7 mod 143) (117^7 mod 143) (110^7 mod 143) (111^7 mod 143) (107^7 mod 143) (122^7 mod 143) (107^7

mod 143) (32^7 mod 143) (107^7 mod 143) (117^7 mod 143) (106^7 mod 143) (111^7 mod 143) (107^7 mod 143)

Cipherteks : 117 10 9 39 33 45 68 34 68 98 68 39 50 45 68

III.4. 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 :

Cipherteks RSA : 117 10 9 39 33 45 68 34 68 98 68 39 50 45 68

Nilai d : 103
Nilai n : 143
Konversi ASCII : 10 113 117 110 111 107 122 107 32 107 117 106 111
ASCII^e mod n : (117^103 mod 143) (10^103 mod 143) (9^103 mod 143) (39^103mod 143) (33^103 mod 143) (45^103 mod 143) (68^103 mod 143) (34^103 mod
143) (68^103 mod 143) (98^103 mod 143) (68^103 mod 143) (39^103 mod 143) (50^103 mod 143) (45^103 mod 143) (68 ^103 mod 143)
Plainteks : qunokzk kujo

2. *Affine Cipher*

Untuk melakukan dekripsi, pertama-tama dihitung 7^{-1} (mod 26), yang dapat dihitung dengan memecahkan kekongruenan lanjar:

Cipherteks : qunokzk kujo

15 * (16 - 10) Mod 26 = 12
15 * (20 - 10) Mod 26 = 20
15 * (13 - 10) Mod 26 = 19
15 * (14 - 10) Mod 26 = 8
15 * (10 - 10) Mod 26 = 0
15 * (25 - 10) Mod 26 = 17
15 * (10 - 10) Mod 26 = 0
15 * (10 - 10) Mod 26 = 0
15 * (20 - 10) Mod 26 = 20
15 * (9 - 10) Mod 26 = 11
15 * (14 - 10) Mod 26 = 8

Plainteks : mutiara aulia

III.5. Perancangan

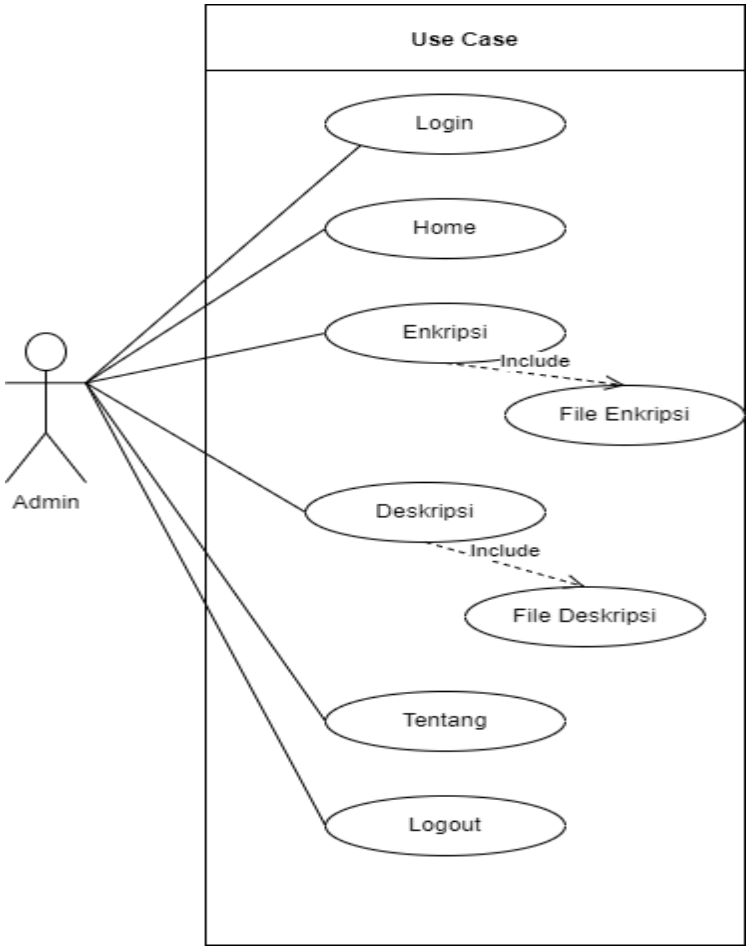
Perancangan aplikasi merupakan perancangan yang dilakukan untuk merancang sebuah aplikasi dengan menggunakan salah satu bahasa pemrograman *PHP*, dalam kasus ini penulis merancang sebuah aplikasi keamanan data keamanan absensi karyawan dengan menggunakan *PHP*.

III.6. Desain Sistem

Perancangan ini akan memberikan penjelasan mengenai rancangan aplikasi serta pembentukan dan pembangunan aplikasi kriptografi algoritma *Affine Cipher* dan *RSA* dalam mengamankan data keamanan absensi karyawan.

III.6.1. *Use Case Diagram*

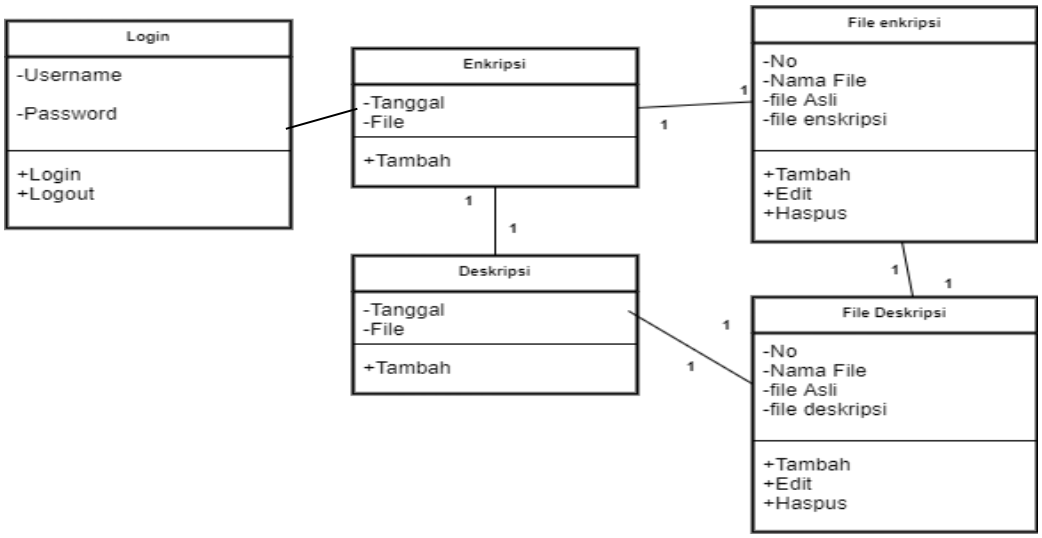
Perilaku beserta tugas-tugas dari tiap–tiap elemen maupun aktor yang terlibat dalam sistem yang akan dirancang, akan digambarkan dalam diagram *use case* yang bertujuan untuk memberikan gambaran secara umum tentang sistem yang akan dirancang pada Gambar III.2.



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

III.6.2 *Class Diagram*

Class Diagram Keamanan Data File Ms. Word *Affine Chiper* dan *RSA* dapat dilihat pada Gambar III.3.



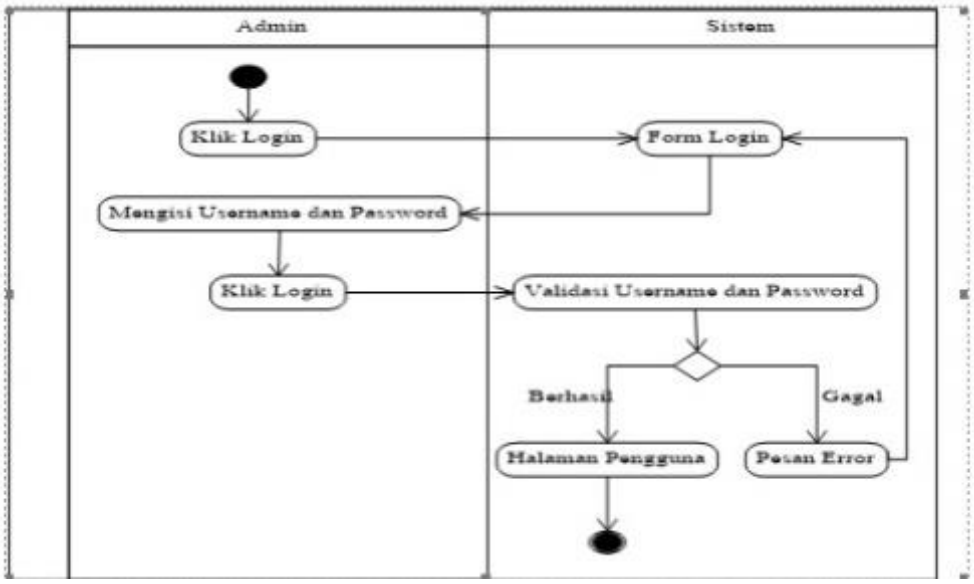
Gambar III.3. ***Class Diagram*** **Keamanan Data absensi karyawan** ***Affine Cipher*** **dan** ***RSA***

III.6.3. *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*

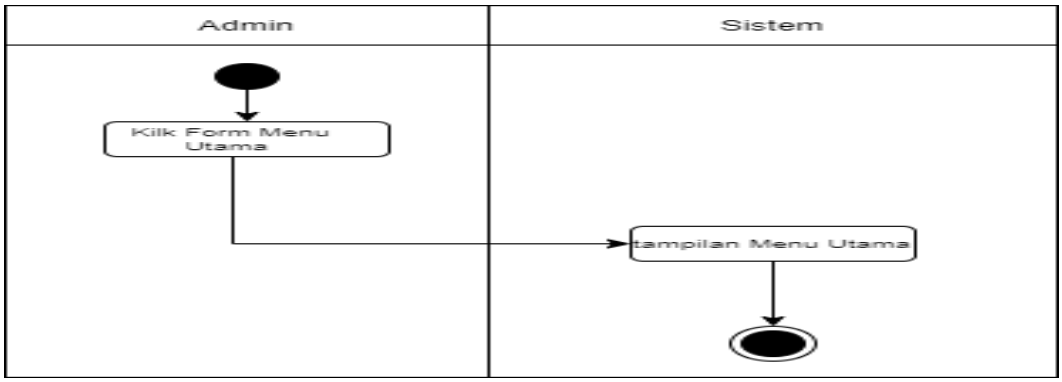
Admin melakukan *login* dengan mengisi *Username* dan *Password*, kemudian setelah diisi akan masuk ke Tampilan Menu Utama. Jika gagal akan disuruh memasukkan *Username* dan *Password* kembali.



Gambar III.4. ***Activity Login Diagram Affine Cipher dan RSA***

2. *Activity Diagram* Menu Utama

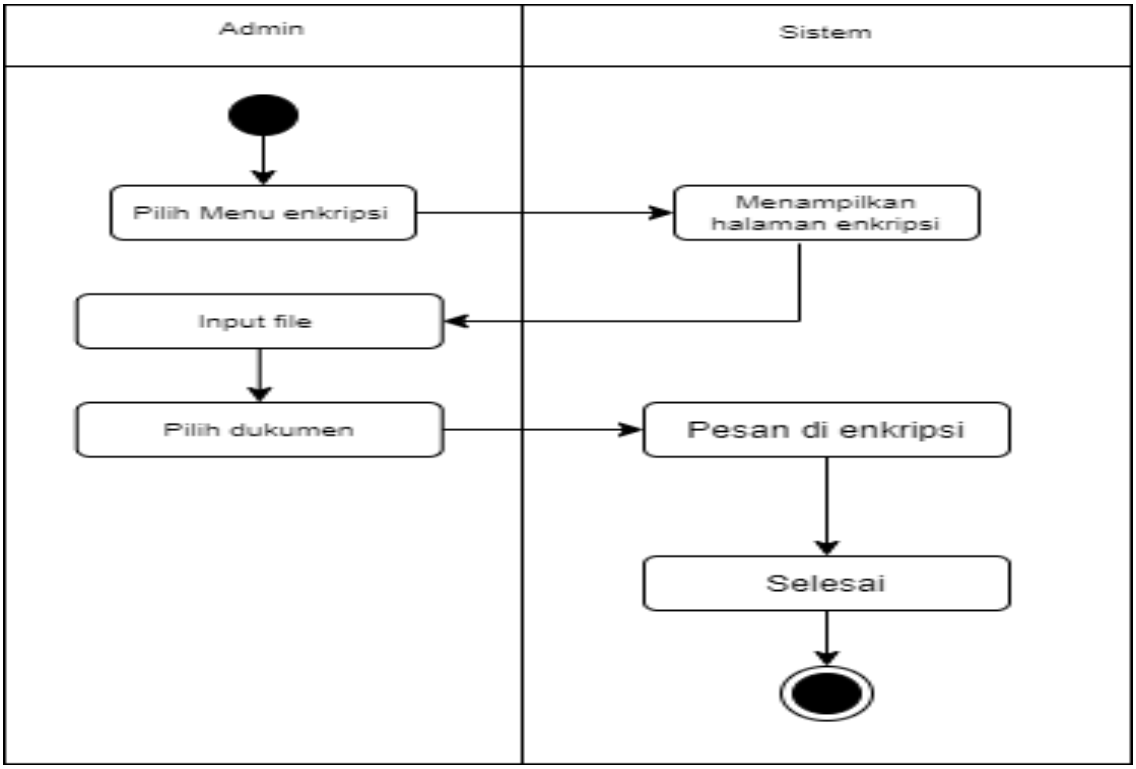
Setelah *Login* akan diarahkan ke Tampilan Menu Utama



Gambar III.5. *Activity Diagram* Menu Utama

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

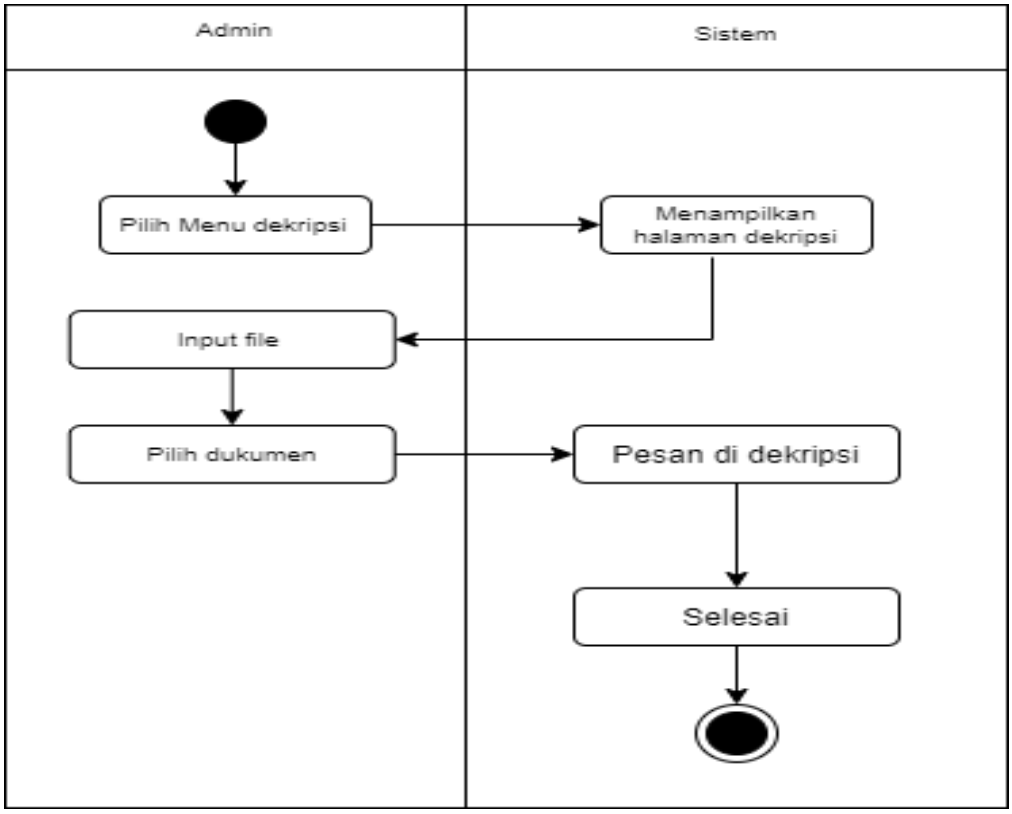
Pilih menu enkripsi lalu ke tampilan halaman enkripsi kemudian pilih file yang akan di enkripsi dan akan muncul pesan bahwa file telah dienkripsi.



Gambar III.6. *Activity* Diagram Enkripsi *Affine Cipher dan RSA*

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

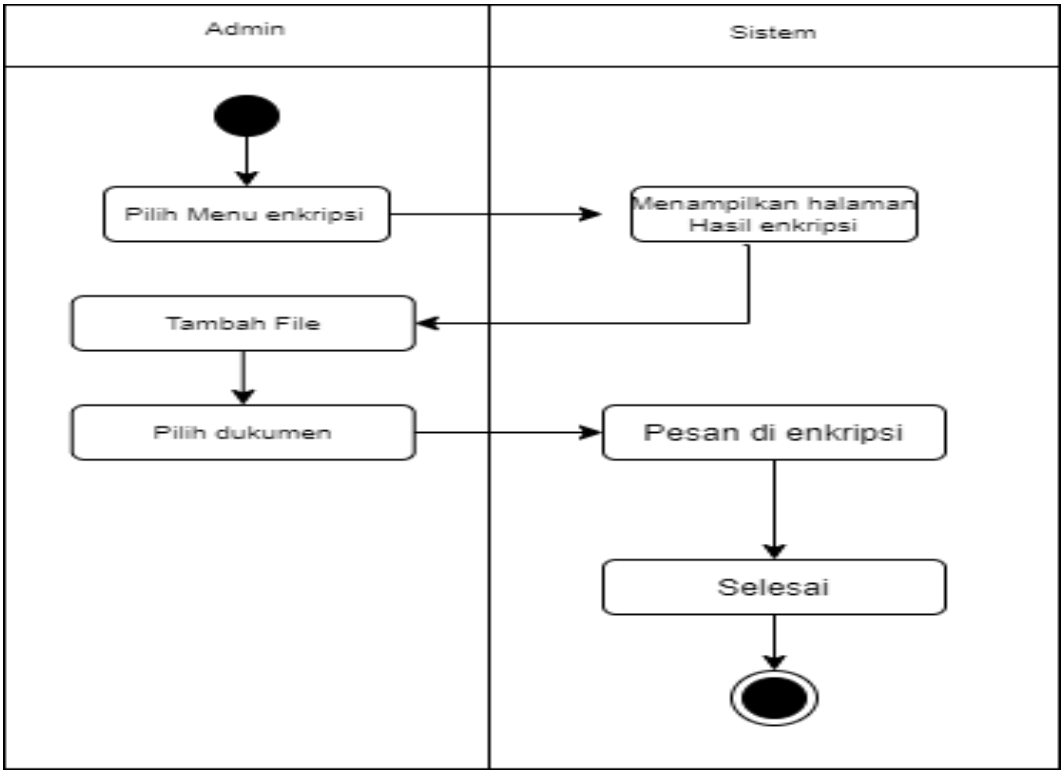
Pilih menu dekripsi lalu ke tampilan halaman dekripsi kemudian pilih file yang akan di dekripsi dan akan muncul pesan bahwa file telah didekripsi.



Gambar III.7. *Activity Diagram* Dekripsi *Affine Cipher* Dan *RSA*

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

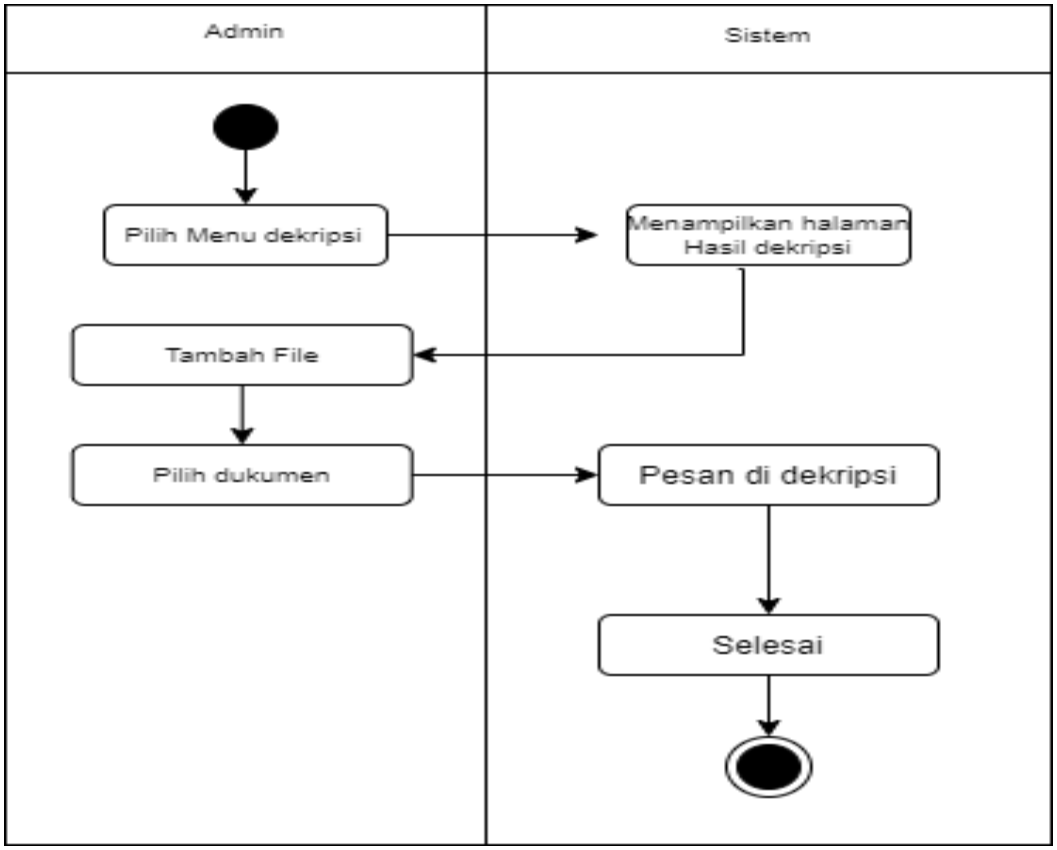
Pilih menu enkripsi lalu ke tampilan halaman file yang telah di enkripsi kemudian pilih tambah file lalu pilih dokumen yang akan di enkripsi dan akan menampilkan hasil file yang telah dienkripsi.



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

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

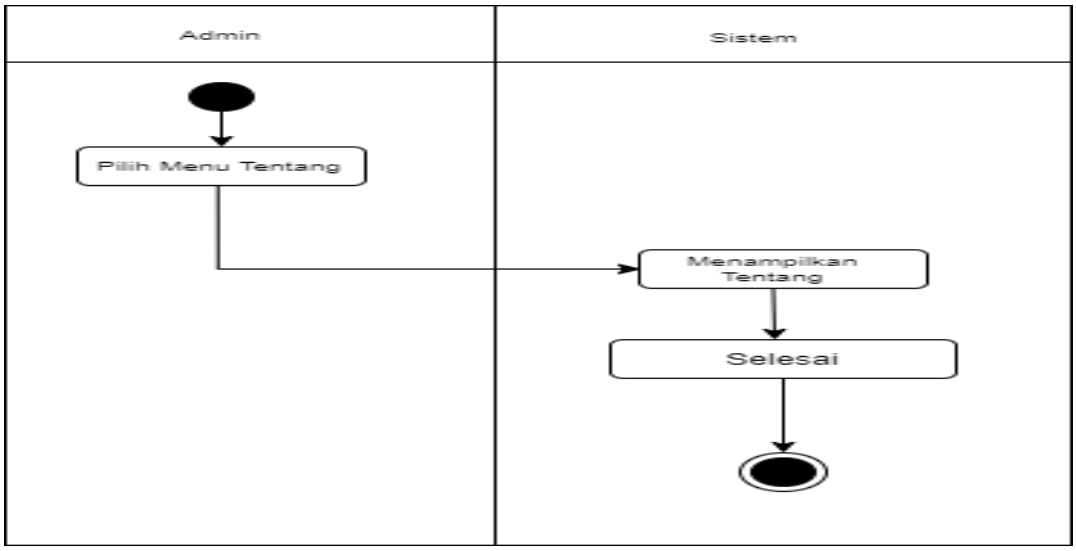
Pilih menu dekripsi lalu ke tampilan halaman file yang telah di enkripsi kemudian pilih tambah file lalu pilih dokumen yang akan di dekripsi dan akan menampilkan file yang telah didekripsi.



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

7. *Activity Diagram* Tentang

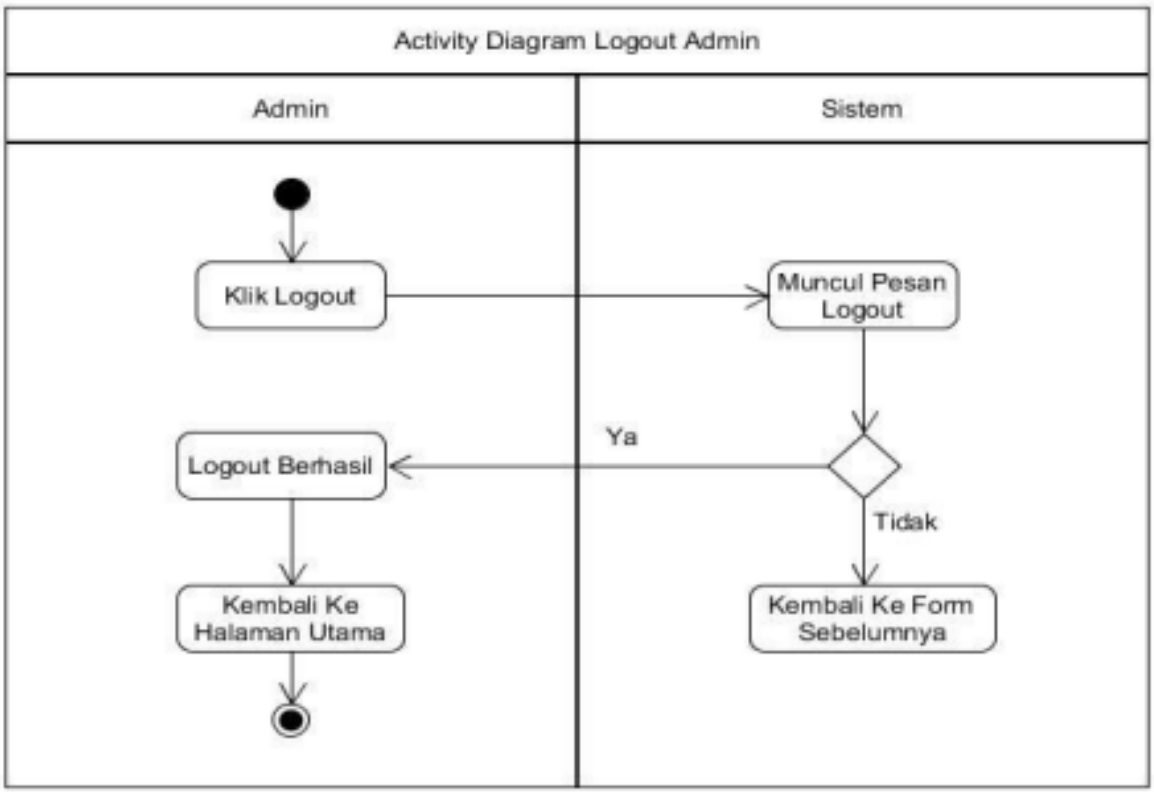
Menampilkan menu tentang algoritma kriptografi *Affine Cipher* dan *RSA*



Gambar III.10. *Activity Diagram* Tentang

8. *Activity Diagram Logout*

Menampilkan menu tentang *logout* dengan cara mengklik *logout*, lalu muncul pesan bahwa *logout* telah berhasil dan kembali ke Halaman Utama. Jika gagal maka akan kembali ke *Form* sebelumnya.



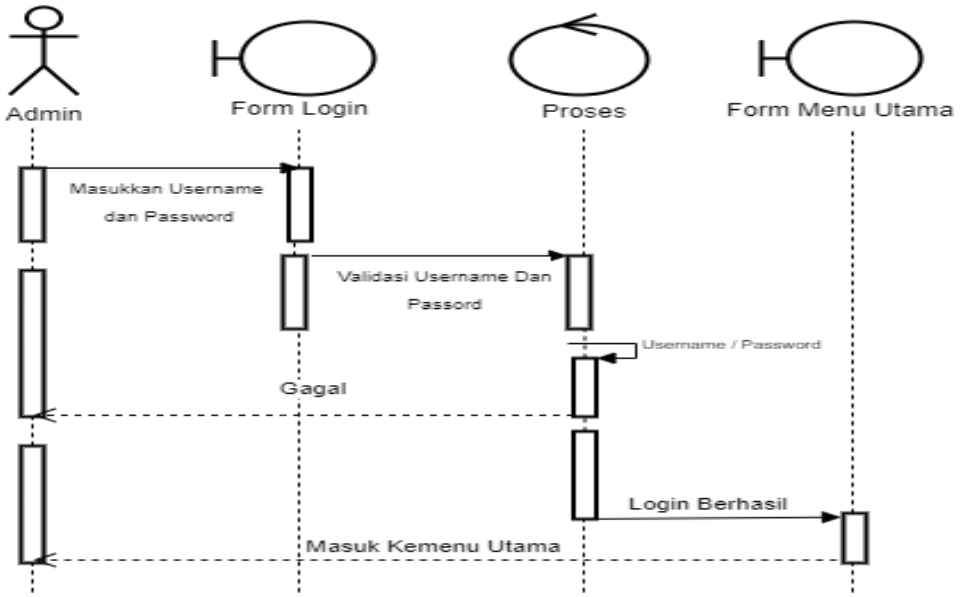
Gambar III.11. *Activity Diagram logout*

III.6.4. *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

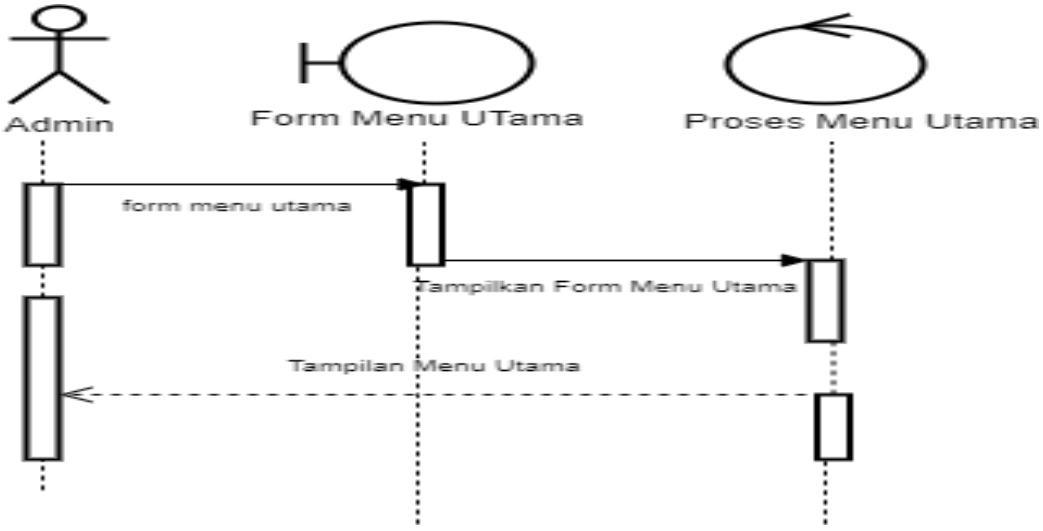
Serangkaian kerja melakukan *login* dapat dilihat pada Gambar III.12.



Gambar III.12. *Sequence Diagram Login*

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

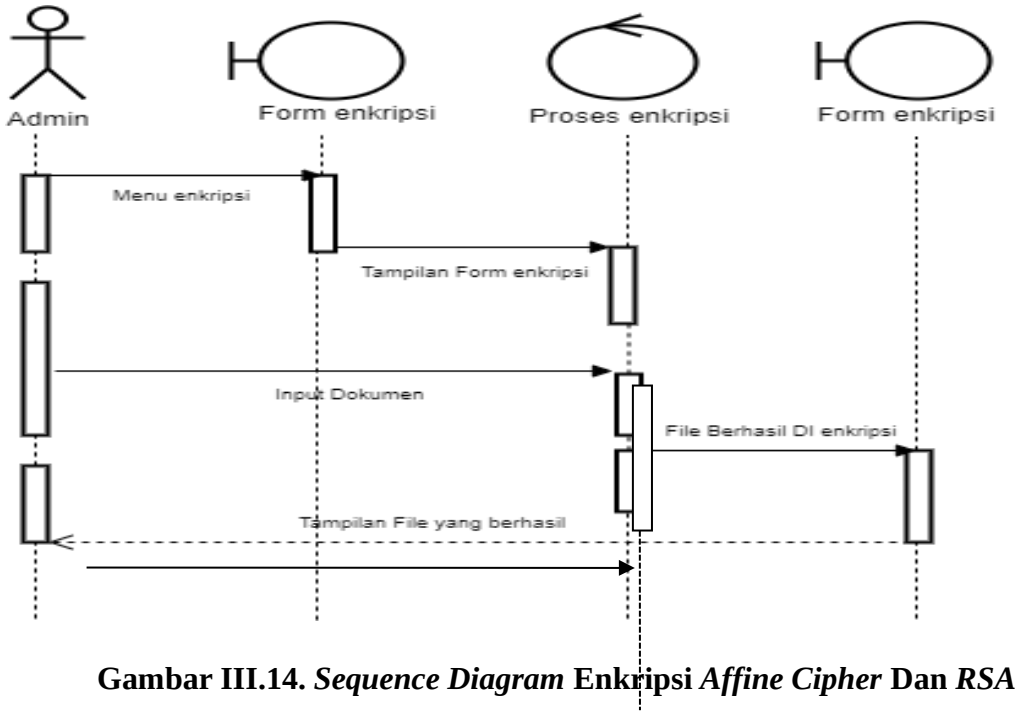
Serangkaian kerja melakukan Menu Utama *Affine Cipher* dan *RSA* dapat dilihat pada Gambar III.13.



Gambar III.13. *Sequence Diagram* Menu Utama *Affine Cipher Dan RSA*

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

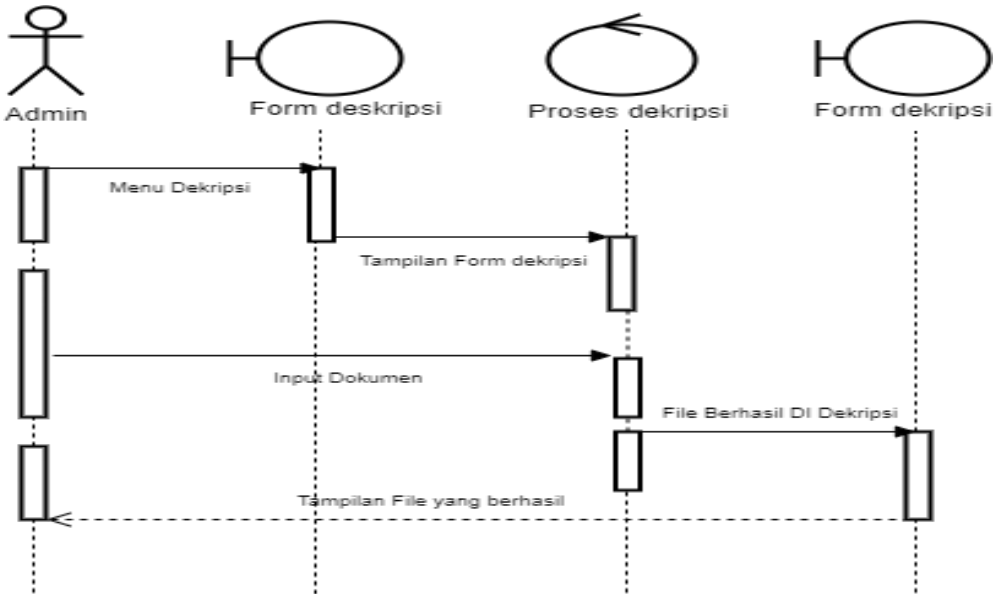
Serangkaian kerja melakukan enkripsi *Affine Cipher* dan *RSA* dapat dilihat pada Gambar III.14.



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

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

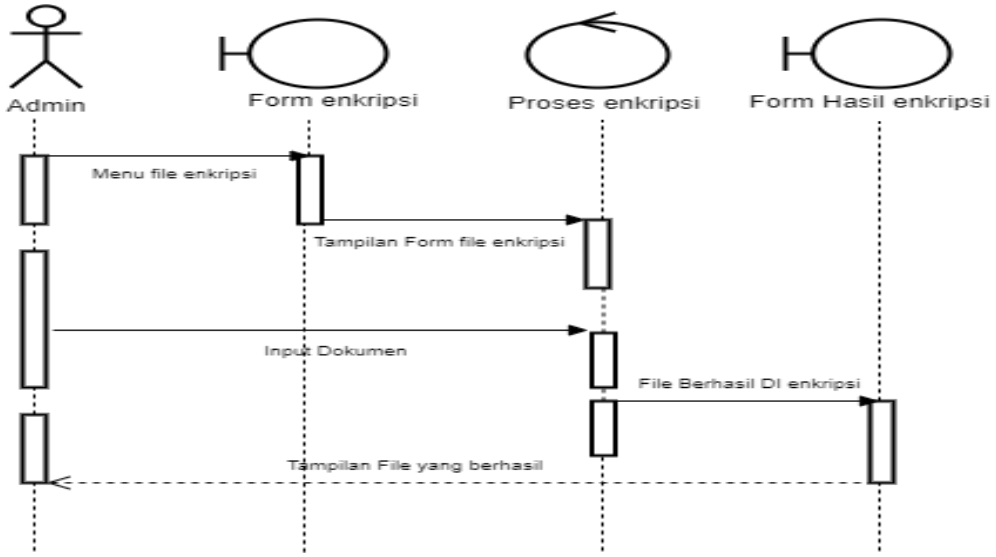
Serangkaian kerja melakukan dekripsi *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.15.



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

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

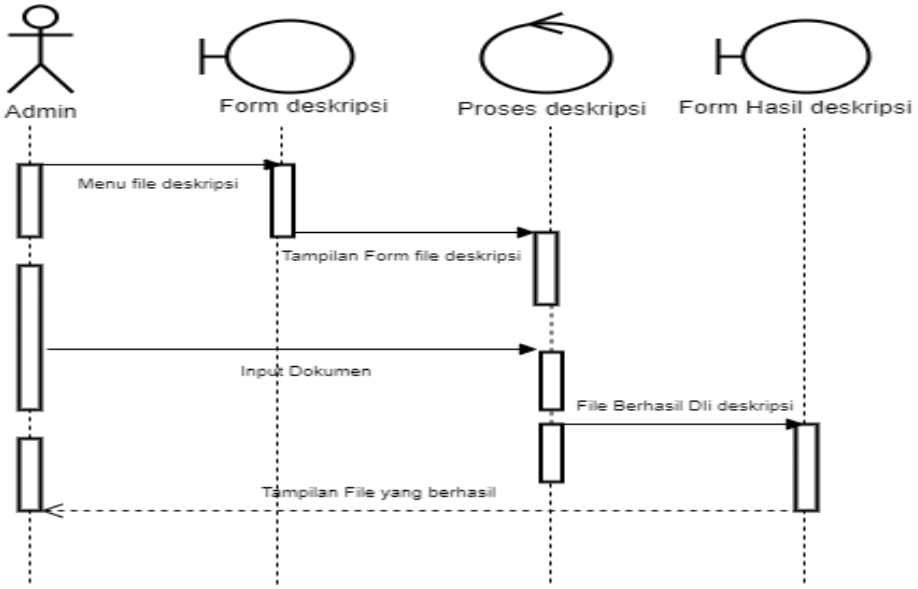
Serangkaian kerja melakukan hasil Enkripsi *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.16.



Gambar III.16. *Sequence Diagram* Hasil Enkripsi *Affine Cipher* Dan *RSA*

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

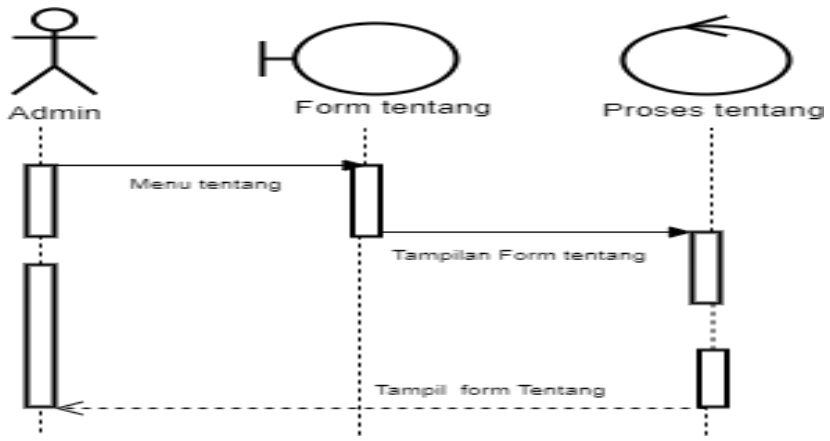
Serangkaian kerja melakukan Hasil Deskripsi *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.17.



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

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

Serangkaian kerja melakukan Tentang *Affine Cipher* Dan *RSA* dapat dilihat pada Gambar III.18.

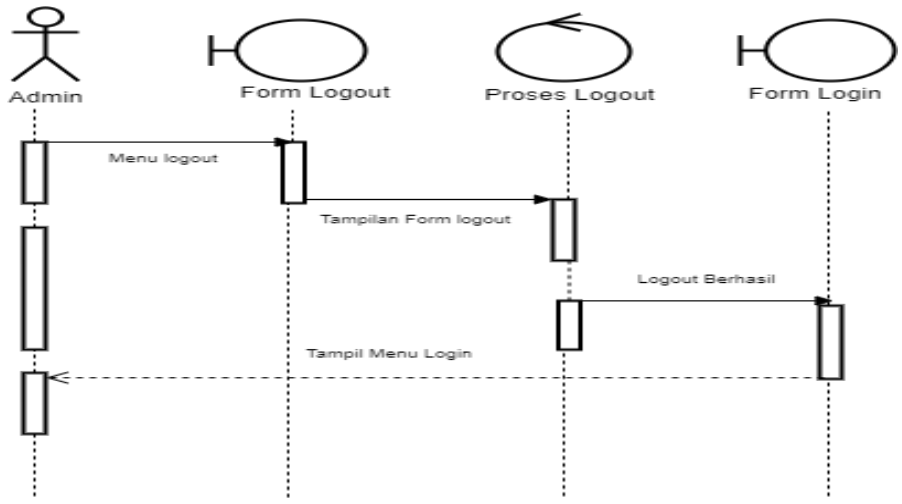


Gambar III.18. *Sequence Diagram* Tentang *Affine Cipher* Dan *RSA*

---

8. Sequence Diagram Logout

Serangkaian kerja melakukan *logout* dapat dilihat pada Gambar III.19.



Gambar III.19. *Sequence Diagram Logout*

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	-	-

3. File_deskripsi

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

Nama Database : dbadmin

Nama Tabel : file_dekripsi

Primary Key : id

Foreign Key : -

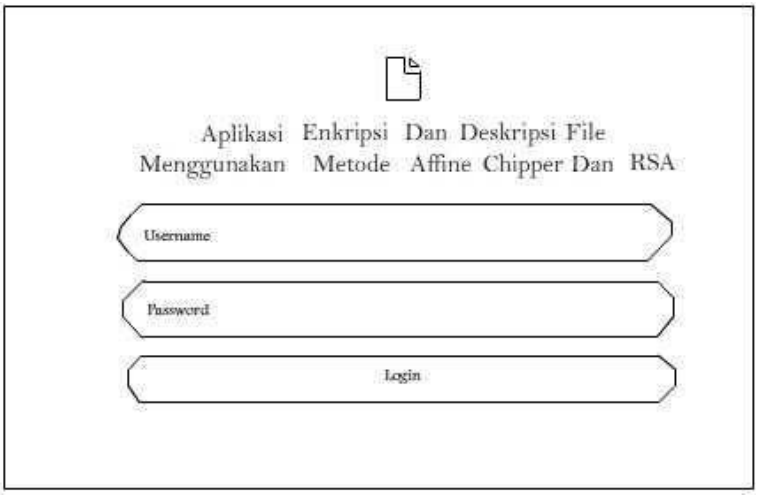
Tabel III.3. Tabel Deskripsi

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*

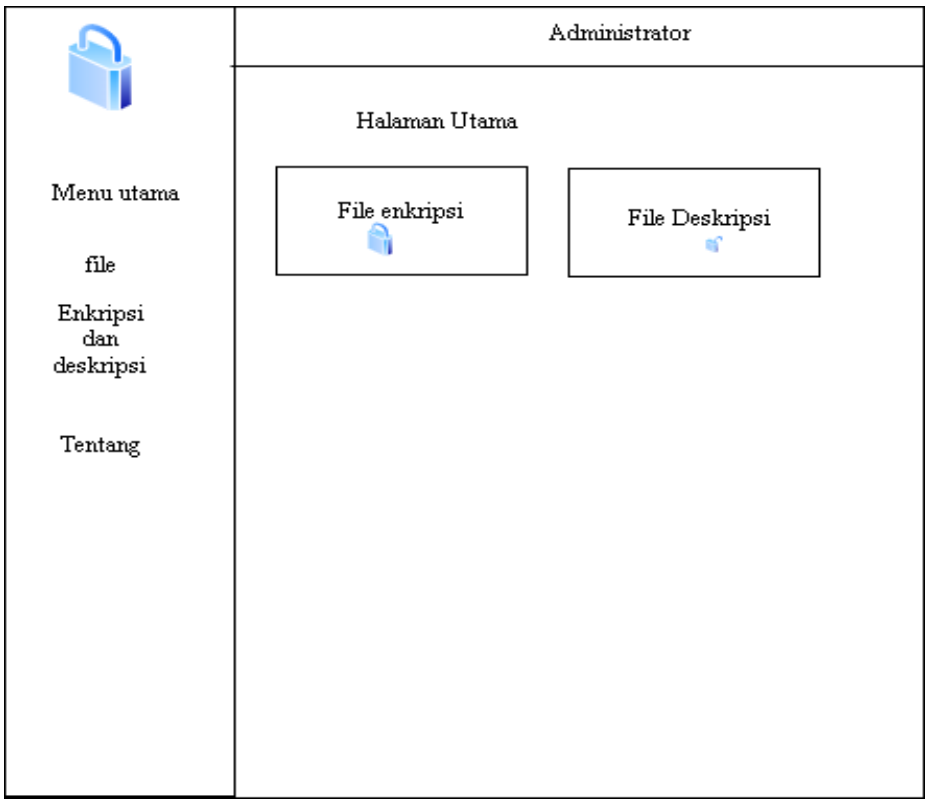
Perancangan *form login* ini terdiri dari satu buah gambar, satu buah *checkbox*, empat buah *label*, dua buah *button* dan dua buah *textfield*. Untuk lebih jelasnya, perancangan *form login* dapat dilihat pada Gambar III.20.



Gambar III.20. Perancangan *Form Login*

III.8.2. Perancangan *Form* Utama

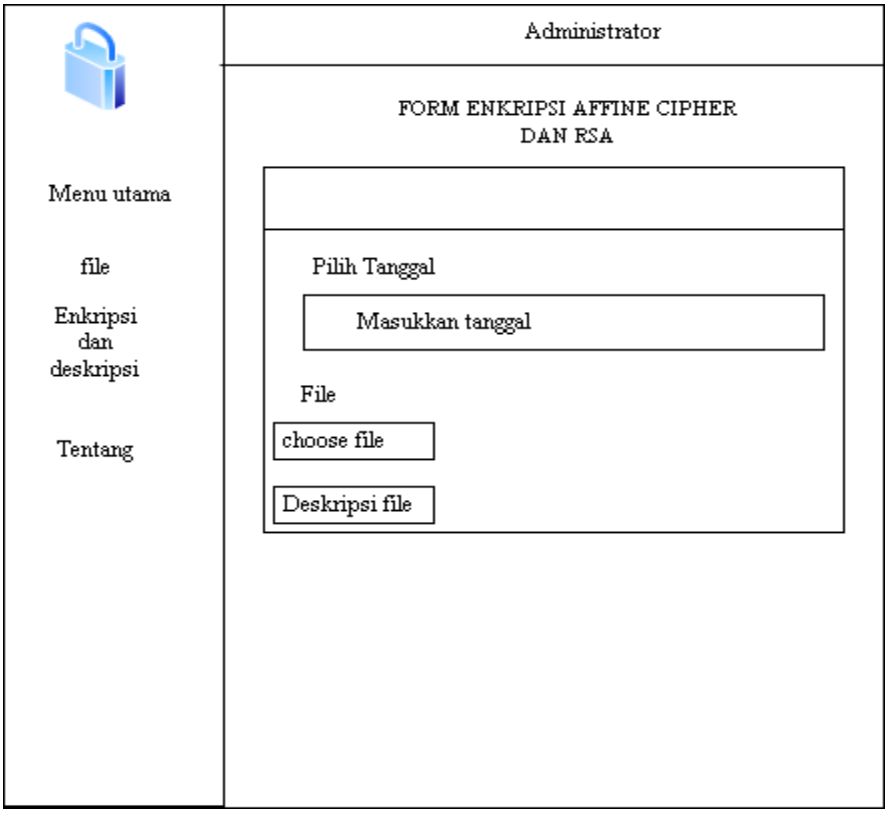
Perancangan *Form* Utama ini terdiri dari empat buah *menu bar*. Untuk lebih jelasnya, perancangan *Form* Utama dapat dilihat pada Gambar III.21.



Gambar III.21. Perancangan *Form* Utama

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

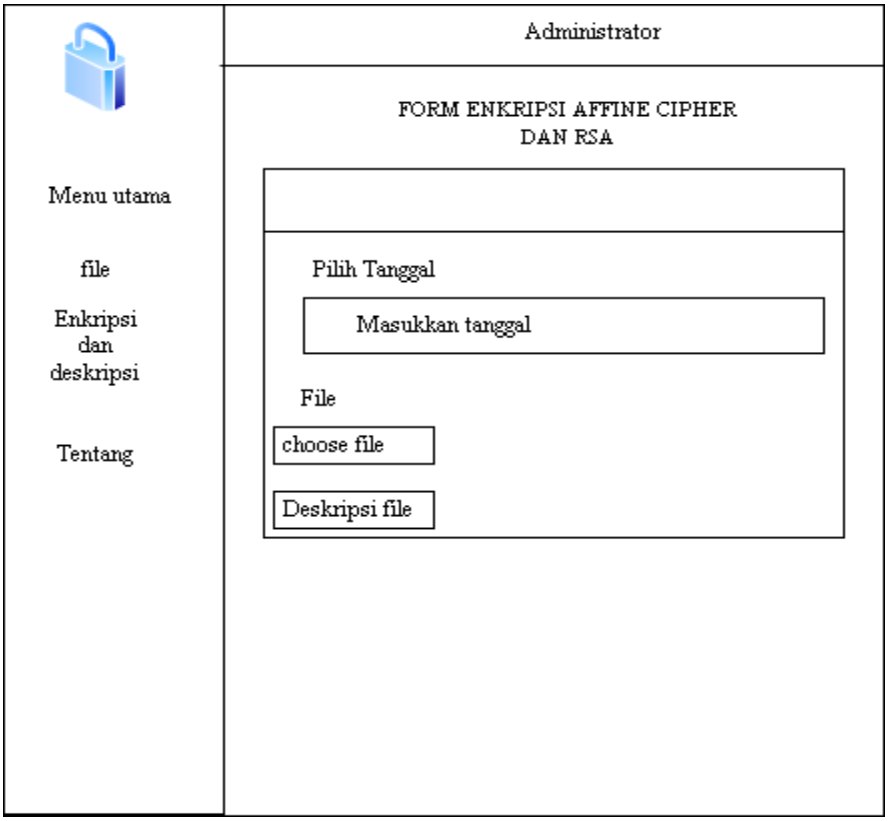
Perancangan *form* Enkripsi *Affine Cipher* Dan *RSA*, untuk lebih jelasnya, perancangan *form* Enkripsi dapat dilihat pada Gambar III.22.



Gambar III.22. Perancangan *Form* Enkripsi *Affine Cipher dan RSA*

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

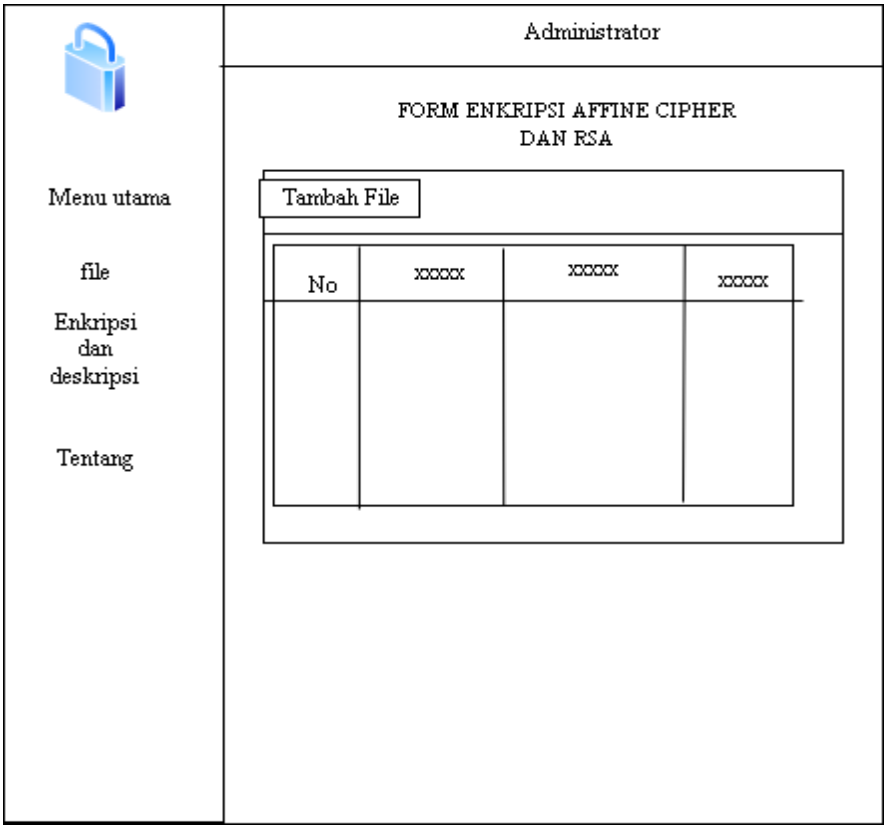
Perancangan *form* Dekripsi *Affine Cipher* Dan *RSA*, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar III.23.



Gambar III.23. Perancangan *Form* Dekripsi *Affine Cipher* Dan *RSA*

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

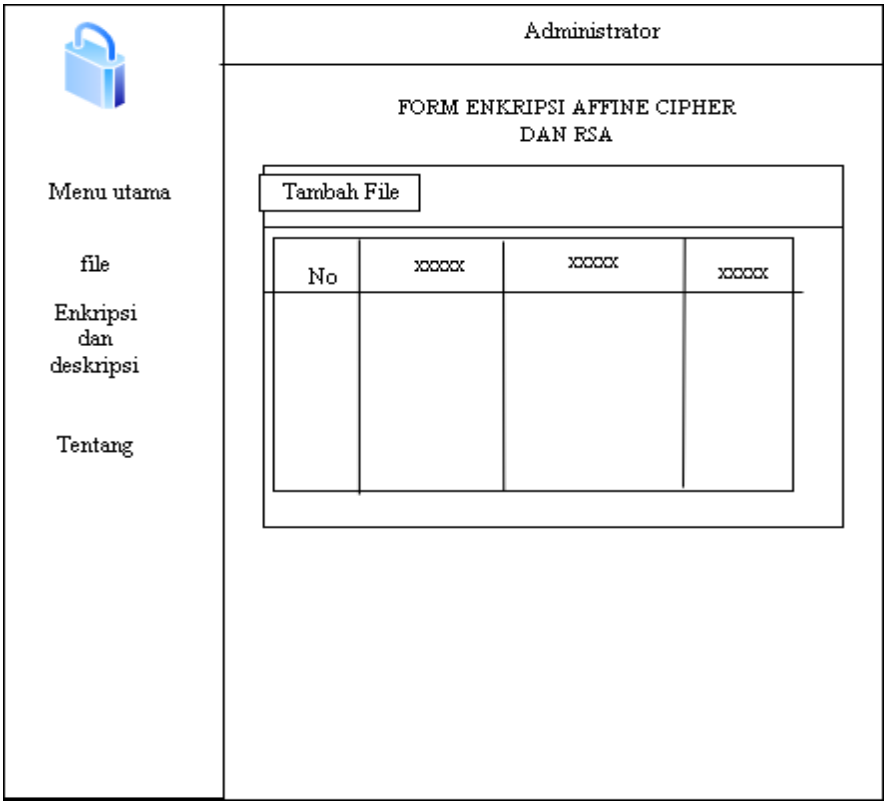
Perancangan *form* Enkripsi *Affine Cipher* Dan *RSA*, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar III.24.



Gambar III.24. Perancangan *Form* Data Enkripsi *Affine Cipher* Dan *RSA*

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

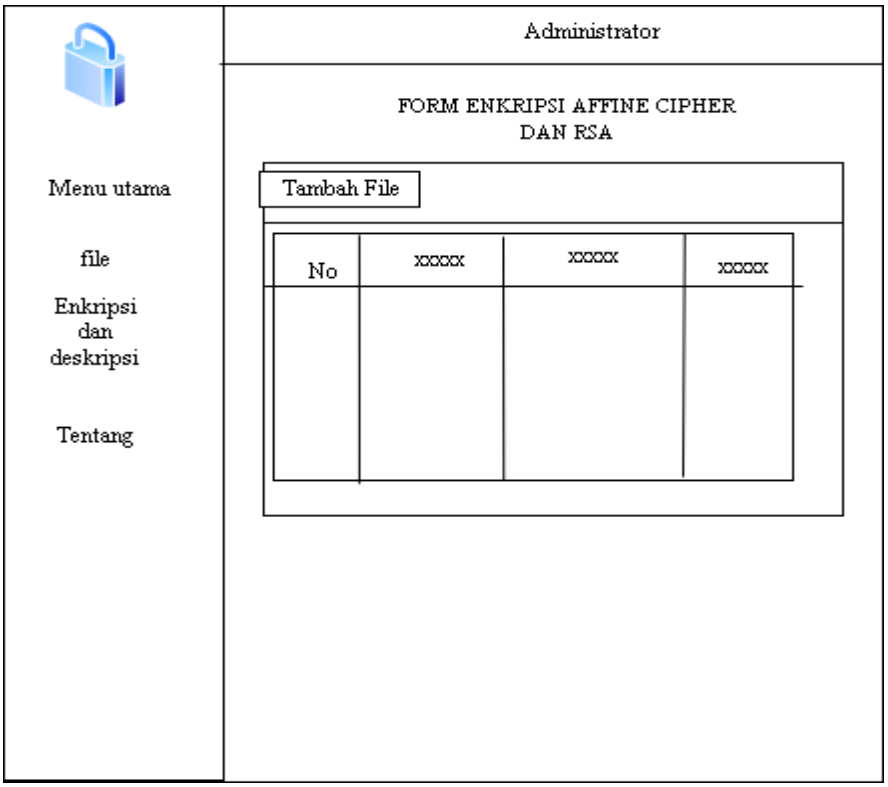
Perancangan *form* Dekripsi *Affine Cipher* Dan *RSA*, untuk lebih jelasnya perancangan *form* Dekripsi dapat dilihat pada Gambar III.25.



Gambar III.25. Perancangan *Form* Data Deskripsi *Affine Cipher* Dan *RSA*

III.8.7. Perancangan *Form* Tentang

Perancangan *form* Tentang, untuk lebih jelasnya, perancangan *form* Dekripsi dapat dilihat pada Gambar III.26.



Gambar III.26. Perancangan *Form* Tentang