

BAB III

ANALISA DAN DESAIN SISTEM

III.1. Analisa Masalah

Seiring maraknya terjadi kasus kebocoran data, peningkatan pengguna internet dan *e-commerce* yang kian meningkat semenjak terjadinya pandemi COVID-19 membuat sistem keamanan internet menjadi rentan. Banyak *website* yang diretas oleh oknum tidak bertanggung jawab, termasuk *website e-commerce* Bhinneka.com yang merupakan situs *e-commerce* Indonesia. Data pengguna Bhinneka.com dan 10 perusahaan lainnya yang serupa juga dijual bebas di sebuah pasar gelap web, sehingga tercatat setidaknya terdapat 73,2 juta data diri pengguna e-commerce dan data perusahaan lainnya terjual bebas dengan harga mencapai USD 18 ribu per-datanya.⁹ Melihat hal ini tentu harus menjadi perhatian besar bahwa sudah saatnya pengesahan RUU Perlindungan Data Pribadi harus dilakukan.

Melihat permasalahan yang ada menjadikan pertimbangan bagi penulis untuk memilih sebuah algoritma yang akan digunakan dalam penyusunan tugas akhir ini, penulis memilih *Algoritma stream cipher* dan *playfair cipher* karena dapat di implementasikan untuk pengamanan *database*. *Algoritma stream cipher* dan *playfair cipher* ini cukup mudah untuk dijelaskan dan sudah digunakan secara luas pada beberapa aplikasi dan algoritmanya sudah dinyatakan cukup aman untuk diterapkan.

III.2. Penerapan Metode

Metode yang digunakan pada penelitian ini adalah metode *Stream Cipher* dan metode *Playfair Cipher*. Berikut ini adalah rumus dan contoh dari metode *Stream Cipher* dan metode *Playfair Cipher*

III.2.1. Metode *Stream Cipher*

Berikut ini adalah rumus enkripsi dan dekripsi metode *Stream Cipher* beserta contohnya:

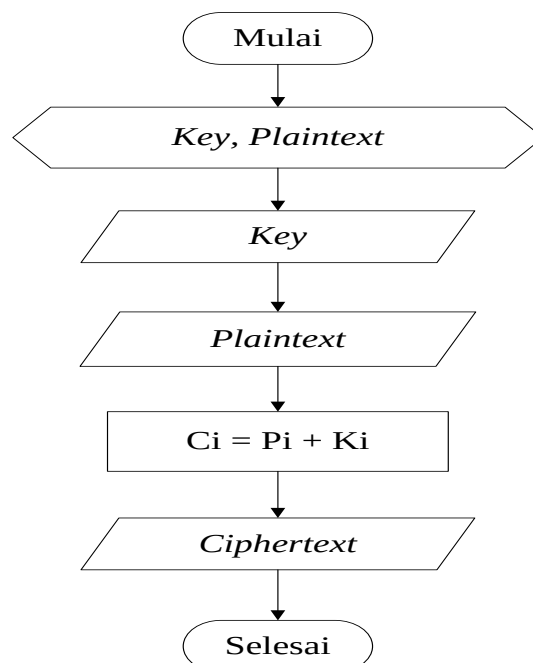
1. Enkripsi Metode *Stream Cipher*

Berikut rumus enkripsi metode *Stream Cipher* beserta contohnya:

Rumus:

$$C_i = (P_i + K_i) \bmod 256$$

Flowchart enkripsi metode *Stream Cipher* dapat dilihat sebagai berikut:



Gambar III.1. Flowchart Enkripsi Metode *Stream Cipher*

Contoh proses Enkripsi:

Plaintext : AFFIF dan INFORMATIKA

Kunci : 12345

Solusi:

Ubah *plaintext* ke dalam kode *ASCII*:

A = 65

F = 70

F = 70

I = 73

F = 70

I = 73

N = 78

F = 70

O = 79

R = 82

M = 77

A = 65

T = 84

I = 73

K = 75

A = 65

Ubah kunci ke dalam kode *ASCII*:

1 = 49

$$2 = 50$$

$$3 = 51$$

$$4 = 52$$

$$5 = 53$$

Gunakan rumus Enkripsi:

$$P1 = (A + 1) \bmod 256$$

$$= (65 + 49) \bmod 256$$

$$= 114 \bmod 256 = 114 = r$$

$$P2 = (F + 2) \bmod 256$$

$$= (70 + 50) \bmod 256$$

$$= 120 \bmod 256 = 120 = x$$

$$P3 = (F + 3) \bmod 256$$

$$= (70 + 51) \bmod 256$$

$$= 121 \bmod 256 = 121 = y$$

$$P4 = (I + 4) \bmod 256$$

$$= (73 + 52) \bmod 256$$

$$= 125 \bmod 256 = 125 = \}$$

$$P5 = (F + 5) \bmod 256$$

$$= (70 + 53) \bmod 256$$

$$= 123 \bmod 256 = 123 = \{$$

$$P6 = (I + 1) \bmod 256$$

$$= (73 + 49) \bmod 256$$

$$= 122 \bmod 256 = 122 = z$$

$$\begin{aligned}
 P7 &= (N + 2) \bmod 256 \\
 &= (78 + 50) \bmod 256 \\
 &= 128 \bmod 256 = 128 = \epsilon
 \end{aligned}$$

$$\begin{aligned}
 P8 &= (F + 3) \bmod 256 \\
 &= (70 + 51) \bmod 256 \\
 &= 121 \bmod 256 = 121 = y
 \end{aligned}$$

$$\begin{aligned}
 P9 &= (O + 4) \bmod 256 \\
 &= (79 + 52) \bmod 256 \\
 &= 131 \bmod 256 = 131 = f
 \end{aligned}$$

$$\begin{aligned}
 P10 &= (R + 5) \bmod 256 \\
 &= (82 + 53) \bmod 256 \\
 &= 135 \bmod 256 = 135 = \ddagger
 \end{aligned}$$

$$\begin{aligned}
 P11 &= (M + 1) \bmod 256 \\
 &= (77 + 49) \bmod 256 \\
 &= 126 \bmod 256 = 126 = \sim
 \end{aligned}$$

$$\begin{aligned}
 P12 &= (A + 2) \bmod 256 \\
 &= (65 + 50) \bmod 256 \\
 &= 115 \bmod 256 = 115 = s
 \end{aligned}$$

$$\begin{aligned}
 P13 &= (T + 3) \bmod 256 \\
 &= (84 + 51) \bmod 256 \\
 &= 135 \bmod 256 = 135 = \ddagger
 \end{aligned}$$

$$\begin{aligned}
 P14 &= (I + 4) \bmod 256 \\
 &= (73 + 52) \bmod 256
 \end{aligned}$$

$$= 125 \bmod 256 = 125 = \}$$

$$P_{15} = (K + 5) \bmod 256$$

$$= (75 + 53) \bmod 256$$

$$= 128 \bmod 256 = 128 = \epsilon$$

$$P_{16} = (A + 1) \bmod 256$$

$$= (65 + 49) \bmod 256$$

$$= 114 \bmod 256 = 114 = r$$

Ciphertext:	r	x	y	}	{	z	€	y	f	‡	~	s	‡	}	€	r
-------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

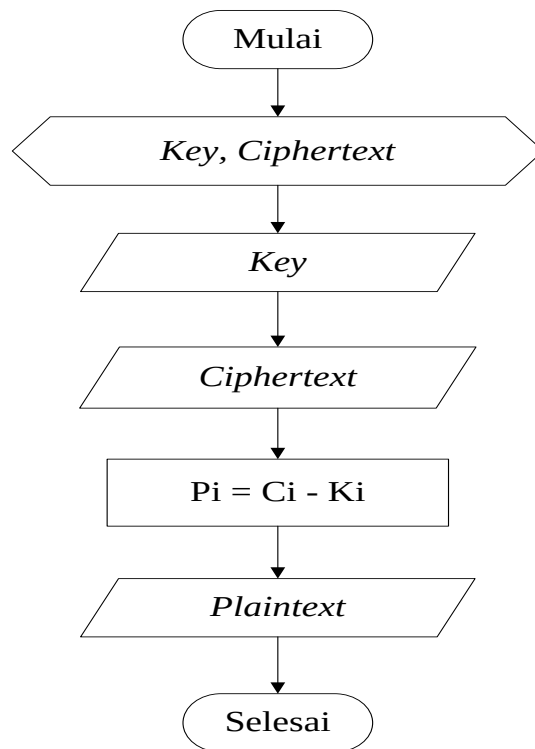
2. Dekripsi Metode *Stream Cipher*

Berikut ini adalah rumus dekripsi metode *Stream Cipher* beserta contohnya:

Rumus dekripsi *Stream Cipher*:

$$P_i = (C_i - K_i) \bmod 256$$

Flowhart dekripsi metode *Stream Cipher* dapat dilihat sebagai berikut:



Gambar III.2. Flowchart Dekripsi Metode Stream Cipher

Contoh Proses Dekripsi:

$$\begin{aligned}
 C1 &= (r - 1) \bmod 256 \\
 &= (114 - 49) \bmod 256 \\
 &= 65 \bmod 256 = 65 = A
 \end{aligned}$$

$$\begin{aligned}
 C2 &= (x - 2) \bmod 256 \\
 &= (120 - 50) \bmod 256 \\
 &= 70 \bmod 256 = 70 = F
 \end{aligned}$$

$$\begin{aligned}
 C3 &= (y - 3) \bmod 256 \\
 &= (121 - 51) \bmod 256 \\
 &= 70 \bmod 256 = 70 = F
 \end{aligned}$$

$$\begin{aligned}
 C4 &= (z - 4) \bmod 256 \\
 &= (125 - 52) \bmod 256
 \end{aligned}$$

$$= 73 \bmod 256 = 73 = I$$

$$C5 = (\{ - 5) \bmod 256$$

$$= (123 - 53) \bmod 256$$

$$= 70 \bmod 256 = 70 = F$$

$$C6 = (z - 1) \bmod 256$$

$$= (122 - 49) \bmod 256$$

$$= 73 \bmod 256 = 73 = I$$

$$C7 = (\epsilon - 2) \bmod 256$$

$$= (128 - 50) \bmod 256$$

$$= 78 \bmod 256 = 78 = N$$

$$C8 = (y - 3) \bmod 256$$

$$= (121 - 51) \bmod 256$$

$$= 70 \bmod 256 = 70 = F$$

$$C9 = (f - 4) \bmod 256$$

$$= (131 - 52) \bmod 256$$

$$= 79 \bmod 256 = 79 = O$$

$$C10 = (\ddagger - 5) \bmod 256$$

$$= (135 - 53) \bmod 256$$

$$= 82 \bmod 256 = 82 = R$$

$$C11 = (\sim - 1) \bmod 256$$

$$= (126 - 49) \bmod 256$$

$$= 77 \bmod 256 = 77 = M$$

$$C12 = (s - 2) \bmod 256$$

$$= (115 - 50) \bmod 256$$

$$= 65 \bmod 256 = 65 = A$$

$$C13 = (\ddagger - 3) \bmod 256$$

$$= (135 - 51) \bmod 256$$

$$= 84 \bmod 256 = 84 = T$$

$$C14 = (\} - 4) \bmod 256$$

$$= (125 - 52) \bmod 256$$

$$= 73 \bmod 256 = 73 = I$$

$$C15 = (\text{€} - 5) \bmod 256$$

$$= (128 - 53) \bmod 256$$

$$= 75 \bmod 256 = 75 = K$$

$$C16 = (r - 1) \bmod 256$$

$$= (114 - 49) \bmod 256$$

$$= 65 \bmod 256 = 65 = A$$

Plaintext: AFFIF dan INFORMATIKA

III.2.2. Metode *Playfair Cipher*

Tahapan-tahapan yang digunakan untuk melakukan proses enkripsi dan dekripsi menggunakan metode *Playfair Cipher* dapat dilakukan dengan aturan sebagai berikut:

1. Cara mengubah pesan menjadi sandi adalah sebagai berikut:
 - a. Mengganti huruf J (bila ada) dengan huruf I
 - b. Menulis pesan dalam pasangan huruf

- c. Jika terdapat pasangan huruf yang sama, maka harus disisipkan huruf Z di tengahnya
- d. Jika jumlah huruf ganjil, maka harus ditambahkan huruf Z di akhir kunci

2. Proses enkripsi

- a. Jika terdapat dua huruf pada baris kunci yang sama maka masing-masing huruf diganti dengan huruf di kanannya (pada kunci yang sudah diperluas).
- b. Jika terdapat dua huruf pada kolom kunci yang sama maka masing-masing huruf diganti dengan huruf di bawahnya (pada kunci yang sudah diperluas).
- c. Jika dua huruf tidak terdapat pada baris atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan.

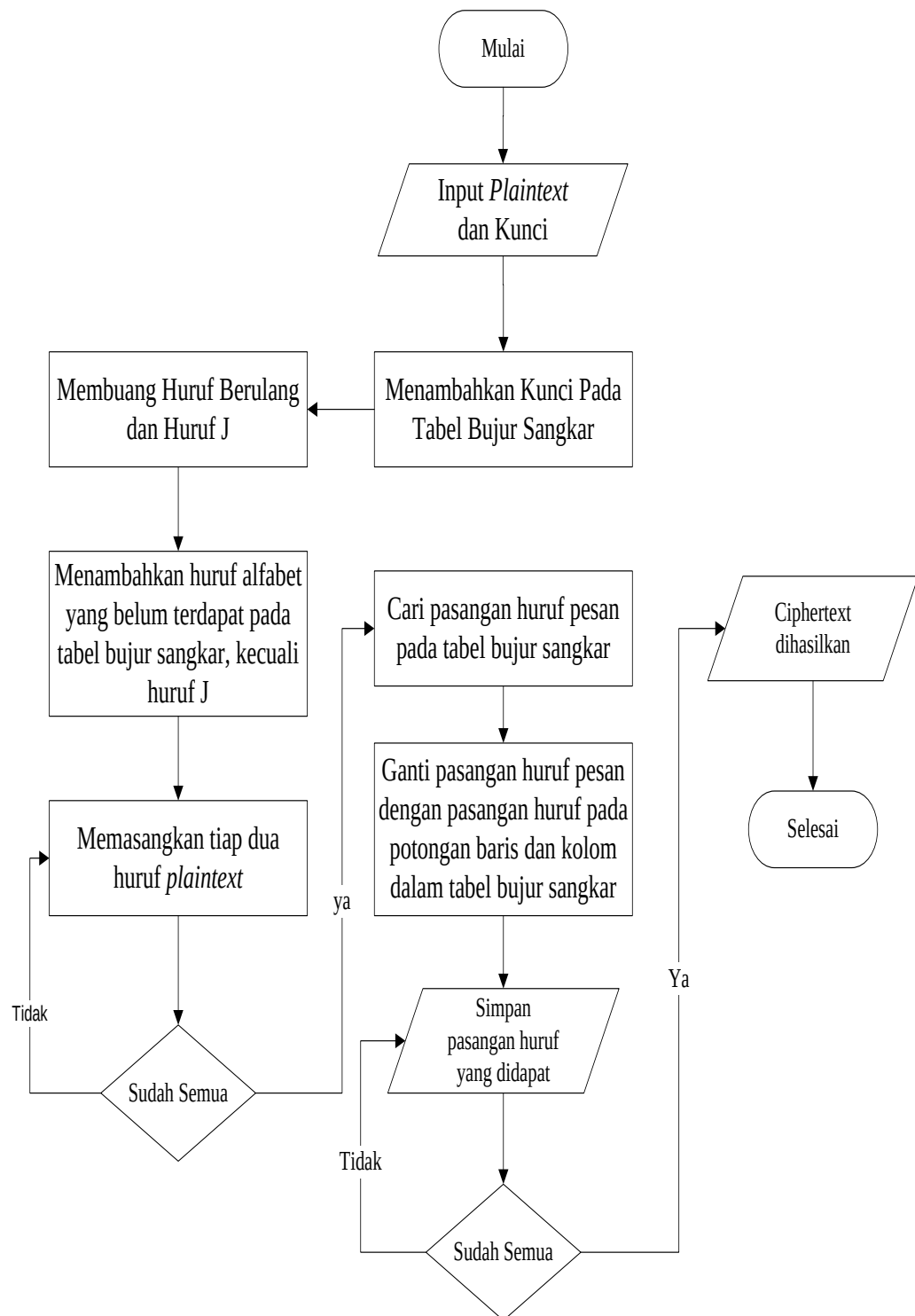
3. Proses Dekripsi

- a. Jika terdapat dua huruf pada baris kunci yang sama maka masing-masing huruf diganti dengan huruf di kirinya (pada kunci yang sudah diperluas).
- b. Jika terdapat dua huruf pada kolom kunci yang sama maka masing-masing huruf diganti dengan huruf di atasnya (pada kunci yang sudah diperluas).
- c. Jika dua huruf tidak terdapat pada baris atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada perpotongan baris huruf kedua dengan kolom huruf pertama.

- d. Jika terdapat huruf yang berada di antara dua huruf yang sama (tidak sesuai pada tempatnya), maka huruf tersebut dapat dihilangkan.

4. *Flowchart* Enkripsi Metode *Playfair Cipher*

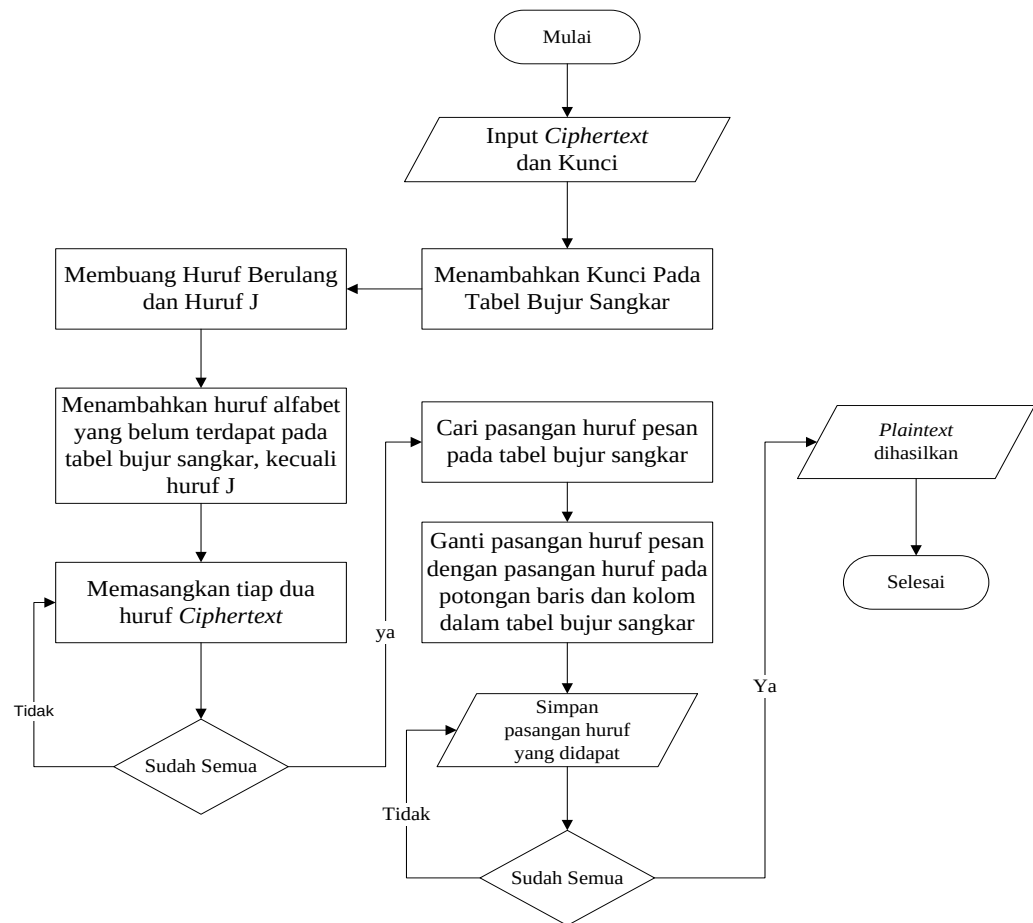
Flowchart Enkripsi Metode *Playfair Cipher* dapat dilihat sebagai berikut:



Gambar III.3. Flowchart Enkripsi Metode Playfair Cipher

5. Flowchart Dekripsi Metode Playfair Cipher

Flowchart Enkripsi Metode Playfair Cipher dapat dilihat sebagai berikut:



Gambar III.5. Flowchart Dekripsi Metode Playfair Cipher

6. Contoh Kasus Proses Enkripsi

Proses Enkripsi adalah proses *Plaintext* (PesanAsli) menjadi *Ciphertext* (PesanTersandi).

Berikut contoh penyelesaiannya:

Diketahui:

Plaintext = INFORMATIKA

Kunci = AFFIF HUDA

Terlebih dahulu susun hurufnya, huruf yang sudah ada tidak dituliskan lagi “AFIHUD” kemudian jika terdapat huruf J maka diganti dengan huruf I. Selanjutnya tambahkan huruf yang tidak terdapat pada kunci

“BCEGKLMNOPQRSTUVWXYZ” menjadi “AFIHUDBCEGKLMNOPQRST VWXYZ”.

Tabel III.1. Tabel Kunci Bujur Sangkar

A	F	I	H	U
D	B	C	E	G
K	L	M	N	O
P	Q	R	S	T
V	W	X	Y	Z

Selanjutnya kunci diperluas untuk masuk kedalam proses enkripsi:

Tabel III.2. Perluasan Tabel Kunci Bujur Sangkar

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Selanjutnya pasangkan *plaintext* dimana jika terdapat huruf J, maka langsung lakukan pasangan huruf dan apabila huruf yang sama, sisipkan huruf Z, Jika sudah dipasangkan “IN FO RM AT IK AZ” lakukan proses *plaintext*

Tabel III.3. Enkrip IN menjadi HM

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.4. Enkrip FO menjadi LU

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.5. Enkrip RM menjadi RX

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.6. Enkrip AT menjadi PU

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.7. Enkrip IK menjadi AM

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.8. Enkrip AZ menjadi UV

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Ciphertext yang dihasilkan dari proses enkripsi *plaintext* “**IN FO RM AT
IK AZ**” adalah “**HM LU RX PU AM UV**”.

5. Contoh Kasus Proses Dekripsi

Proses dekripsi menggunakan metode *Playfair* dapat dilakukan sebagai berikut:

Flowchart Dekripsi metode *Playfair Cipher* dapat dilihat sebagai berikut:

Ciphertext : HMLURXPUAMUV

Kunci : AFFIF HUDA

Proses pembuatan tabel kunci bujur sangkar dengan cara yang digunakan pada proses enkripsi, sehingga dapat dilihat pada tabel III.9.

Tabel III.9. Perluasan Tabel Kunci Bujur Sangkar

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Kemudian lakukan proses dekripsi dengan cara mengubah *ciphertext* ke dalam bentuk pasangan menjadi “**HM LU RX PU AM UV**”.

Tabel III.10. Dekripsi HM menjadi IN

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.11. Dekripsi LU menjadi FO

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.12. Dekripsi RX menjadi RM

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.13. Dekripsi PU menjadi AT

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.14. Dekripsi AM menjadi IK

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

Tabel III.15. Dekripsi UV menjadi AZ

A	F	I	H	U	A
D	B	C	E	G	D
K	L	M	N	O	K
P	Q	R	S	T	P
V	W	X	Y	Z	V
A	F	I	H	U	

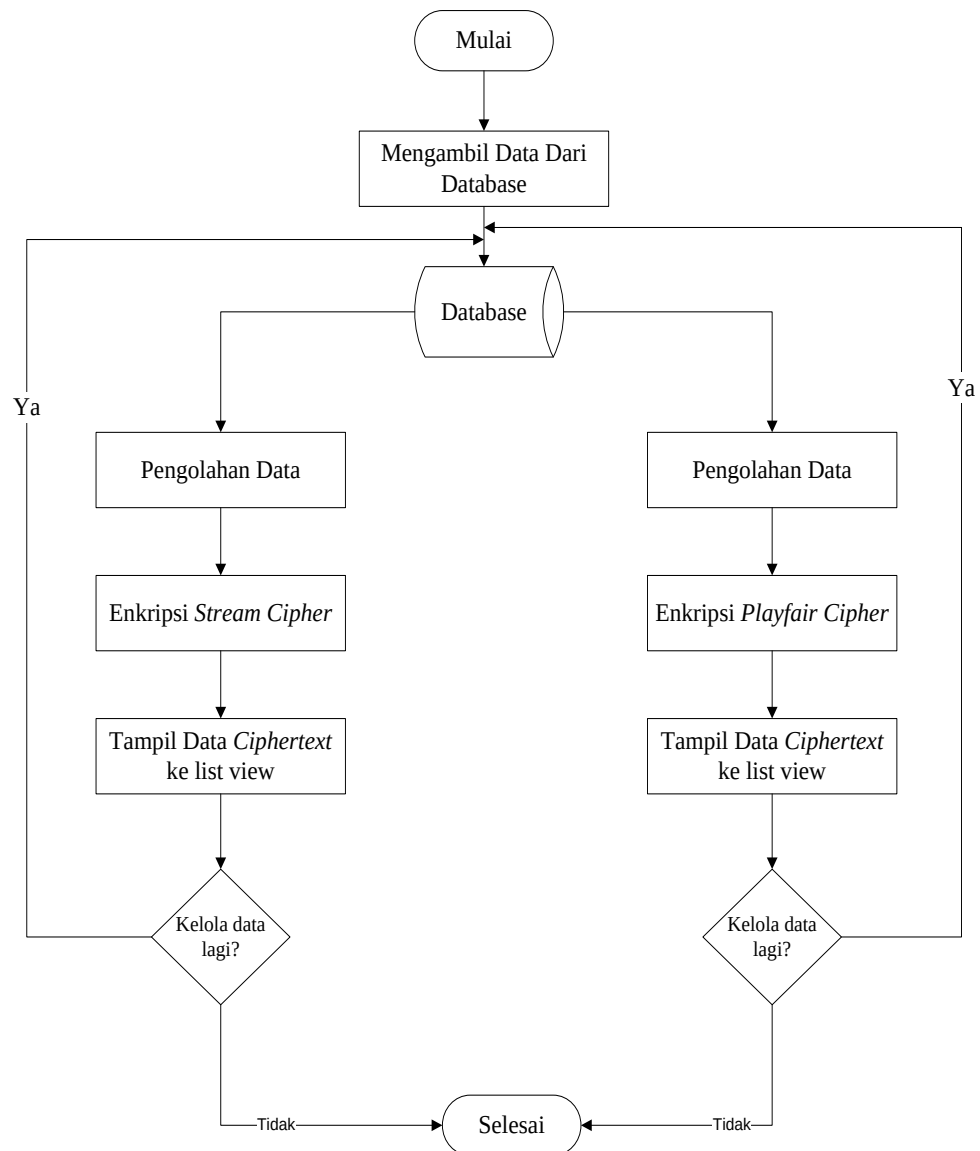
Plaintext yang dihasilkan dari proses dekripsi “**HM LU RX PU AM UV**” adalah “**IN FO RM AT IK AZ**”.

III.2.3. *Flowchart* Rancangan Program

Adapun *Flowchart* rancangan program keamanan *database* menggunakan metode *Stream Cipher* dan metode *Playfair Cipher* sebagai berikut:

1. Enkripsi *Flowchart* Rancangan Program

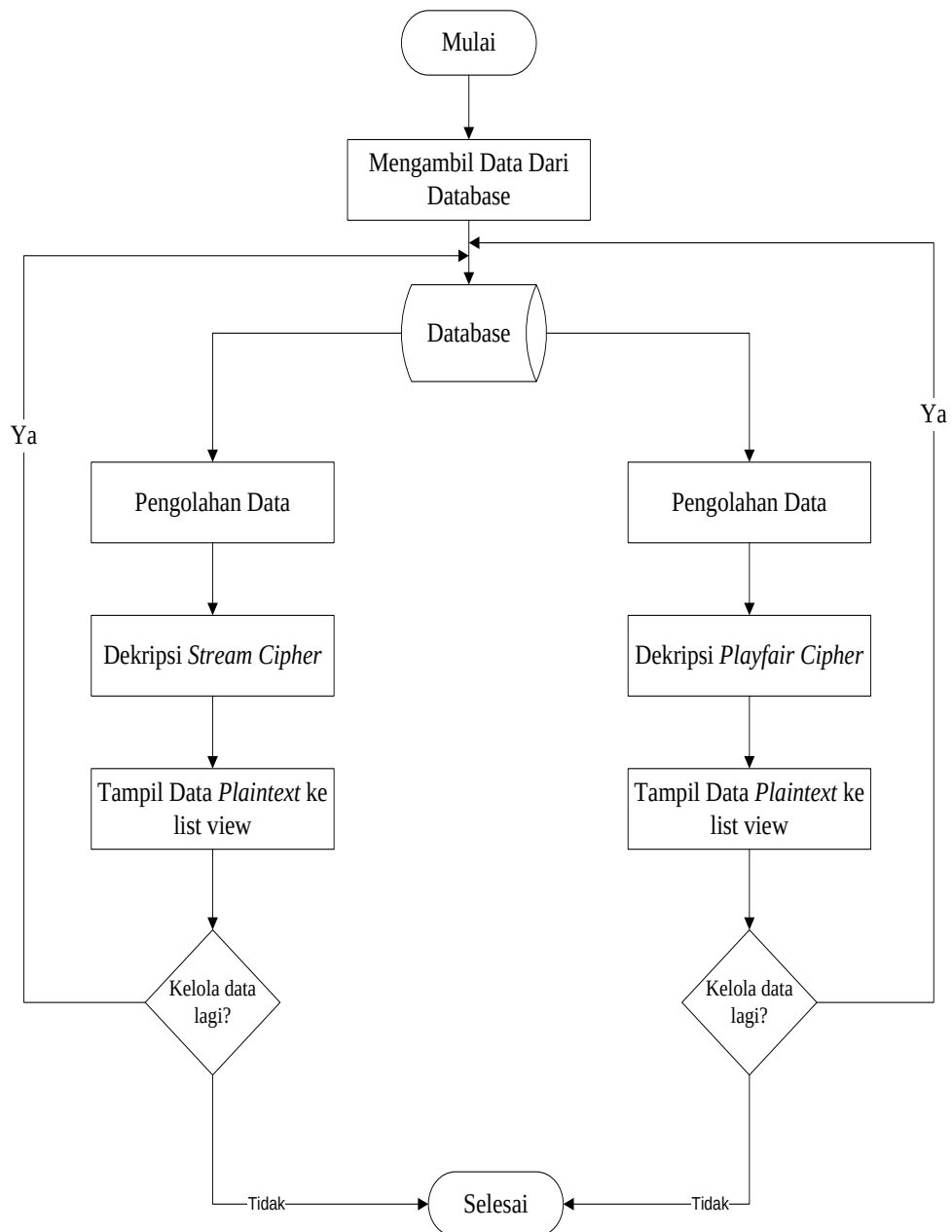
Adapun Enkripsi *Flowchart* Rancangan Program dapat dilihat pada gambar sebagai berikut:



Gambar III.5. Flowchart Enkripsi Rancangan Program Keamanan Database

2. Dekripsi Flowchart Rancangan Program

Adapun *Flowchart* Dekripsi Rancangan Program dapat dilihat pada gambar sebagai berikut:



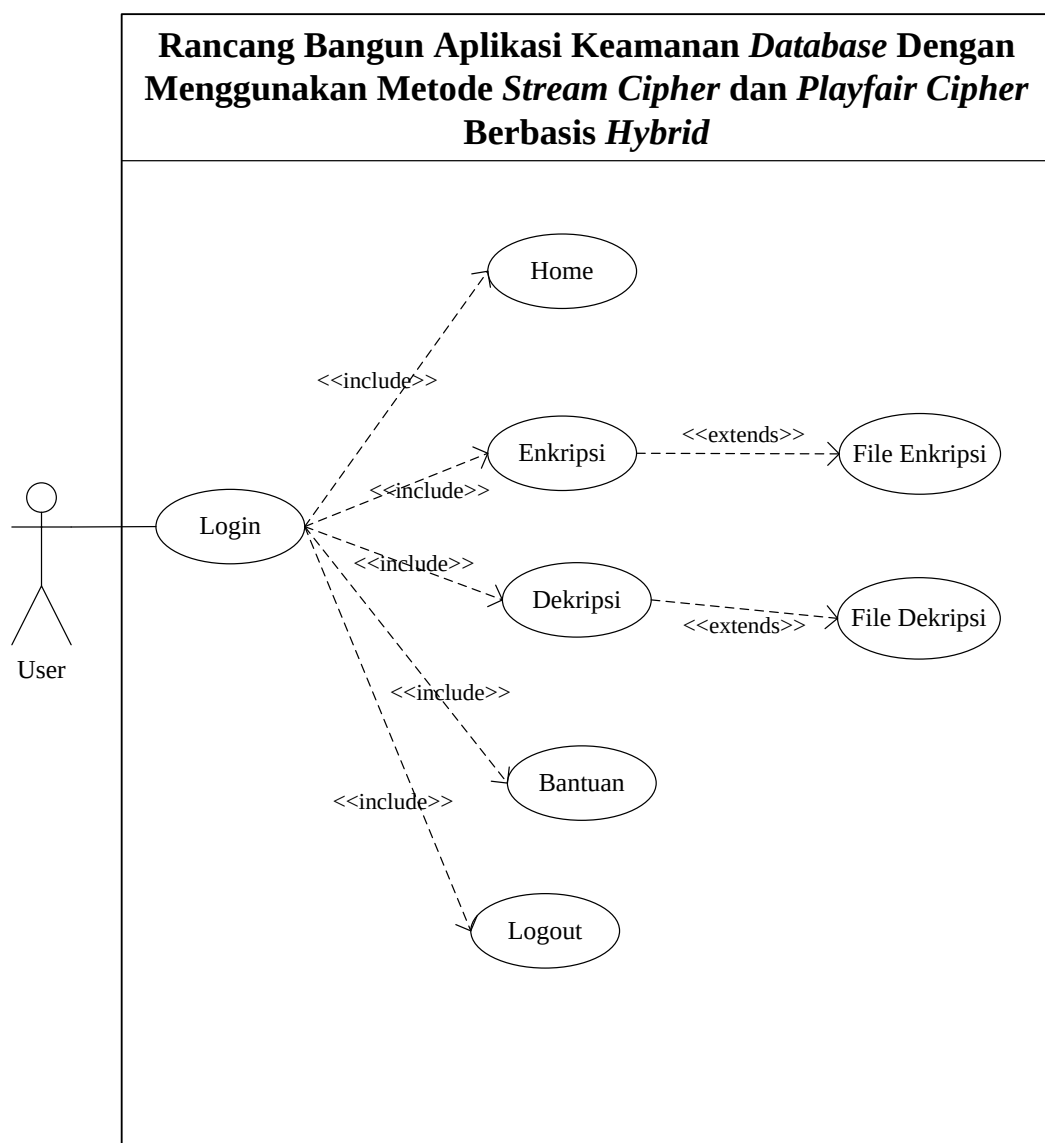
Gambar III.6. Flowchart Dekripsi Rancangan Program Keamanan Database

III.3. Desain Sistem

Tahap desain sistem mempunyai maksud dan tujuan untuk memenuhi kebutuhan kepada pemakai sistem dan untuk memberikan gambaran yang jelas serta rancang bangun yang lengkap tentang sistem yang akan dibangun.

III.3.1. Use Case Diagram

Use Case menjelaskan urutan kegiatan yang dilakukan aktor dan sistem untuk mencapai suatu tujuan tertentu. Sebuah *Use Case* mempresentasikan sebuah interaksi antara aktor dengan sistem dan menggambarkan fungsional yang diharapkan dari sebuah sistem perbandingan. Diagram *Use Case* tersebut dapat dilihat pada gambar III.7.



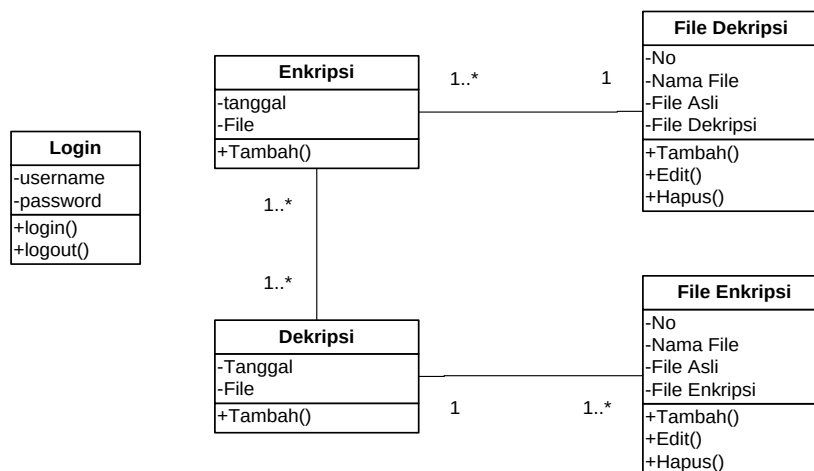
Gambar III.7. Use Case Diagram Rancang Bangun Aplikasi Keamanan Database Dengan Menggunakan Metode Stream Cipher dan Playfair Cipher Berbasis Hybrid

Keterangan *Use Case* Rancang Bangun Aplikasi Keamanan *Database* Dengan Menggunakan Metode *Stream Cipher* dan *Playfair Cipher* Berbasis *Hybrid*:

1. *User* melakukan *login* terlebih dahulu.
2. Setelah *login* menampilkan halaman *home*
3. *User* menginput data dan setelah diinput data tersebut di enkripsikan menggunakan metode *Stream Cipher* dan *Playfair Cipher*
4. *User* menginput data yang telah di enkripsi dan setelah itu data tersebut di Dekripsikan menggunakan metode *Stream Cipher* dan *Playfair Cipher*
5. Jika *User* belum memahami cara-cara menggunakan aplikasi, maka user bisa membuka form bantuan.
6. Jika *User* ingin keluar dari aplikasi, maka *user* bisa mengklik menu *logout*.

III.3.2. Class Diagram

Rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat pada Gambar III.8 berikut:



Gambar III.8. Class Diagram Rancang Bangun Aplikasi Keamanan Database Dengan Menggunakan Metode *Stream Cipher* dan *Playfair Cipher* Berbasis Android

Keterangan *Class Diagram* berikut:

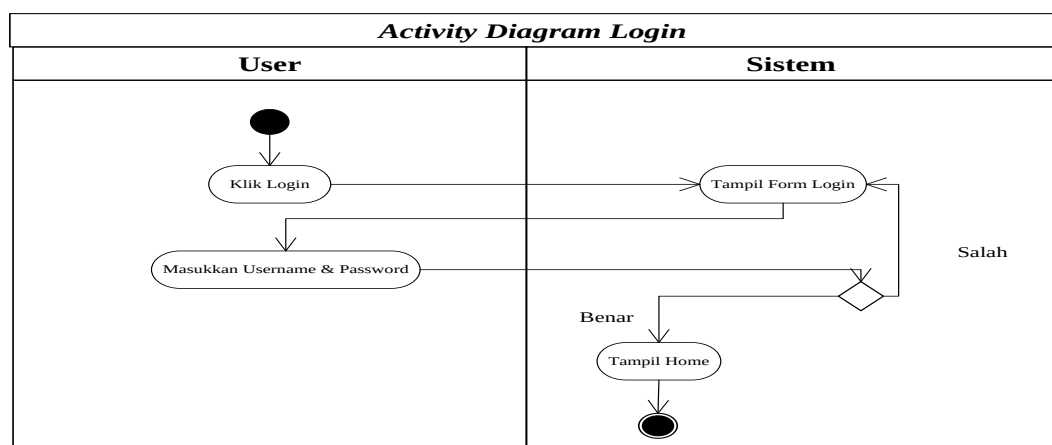
1. Tabel *Login* untuk membuat akun agar user bisa menggunakan aplikasi
2. Tabel Enkripsi untuk data yang akan di input kedalam *database* yang akan di enkripsikan menggunakan metode *Stream Cipher* dan metode *Playfair Cipher*
3. Tabel Dekripsi untuk data yang telah di enkripsikan kemudian di dekripsikan menggunakan metode *Stream Cipher* dan metode *Playfair Cipher*
4. *File Dekripsi* adalah hasil dari enkripsi isi *database*
5. *File Enkripsi* adalah hasil dari dekripsi isi *database*

III.3.3. Activity Diagram

Bisnis proses yang telah digambarkan pada *Use Case Diagram* di atas dijabarkan dengan *Activity Diagram* :

1. Activity Diagram Login

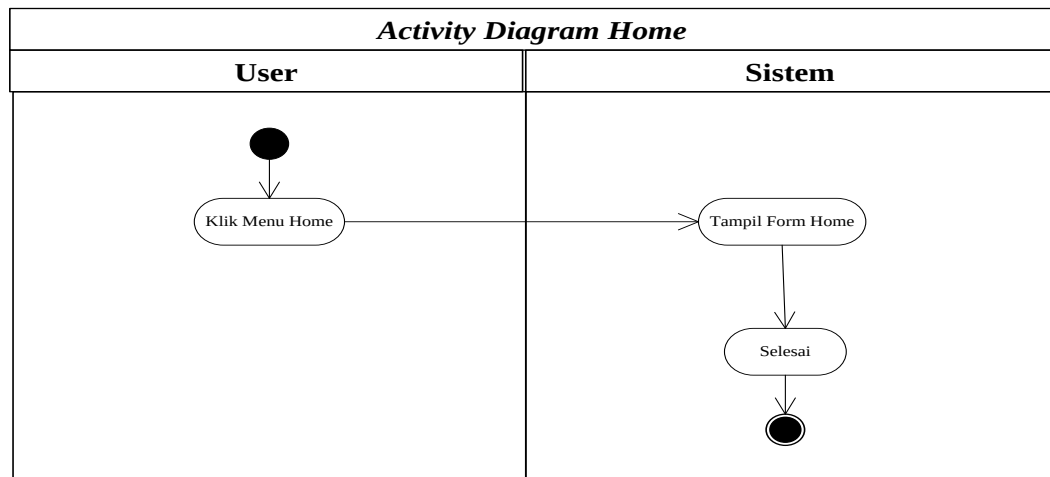
Activity Diagram Login menggambarkan user yang melakukan login untuk masuk kedalam sistem dapat dilihat pada gambar III.9 berikut:



Gambar III.9. Activity Diagram Login

2. Activity Diagram Home

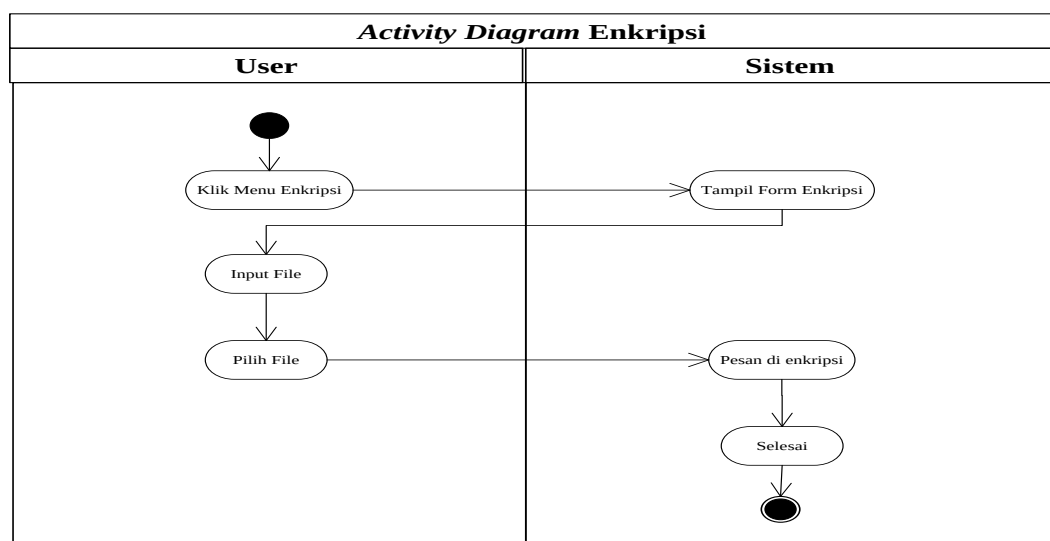
Activity Diagram Home menggambarkan user yang masuk kedalam menu utama atau home untuk menjalankan sistem dapat dilihat pada gambar III.10 berikut:



Gambar III.10 Activity Diagram Home

3. Activity Diagram Enkripsi

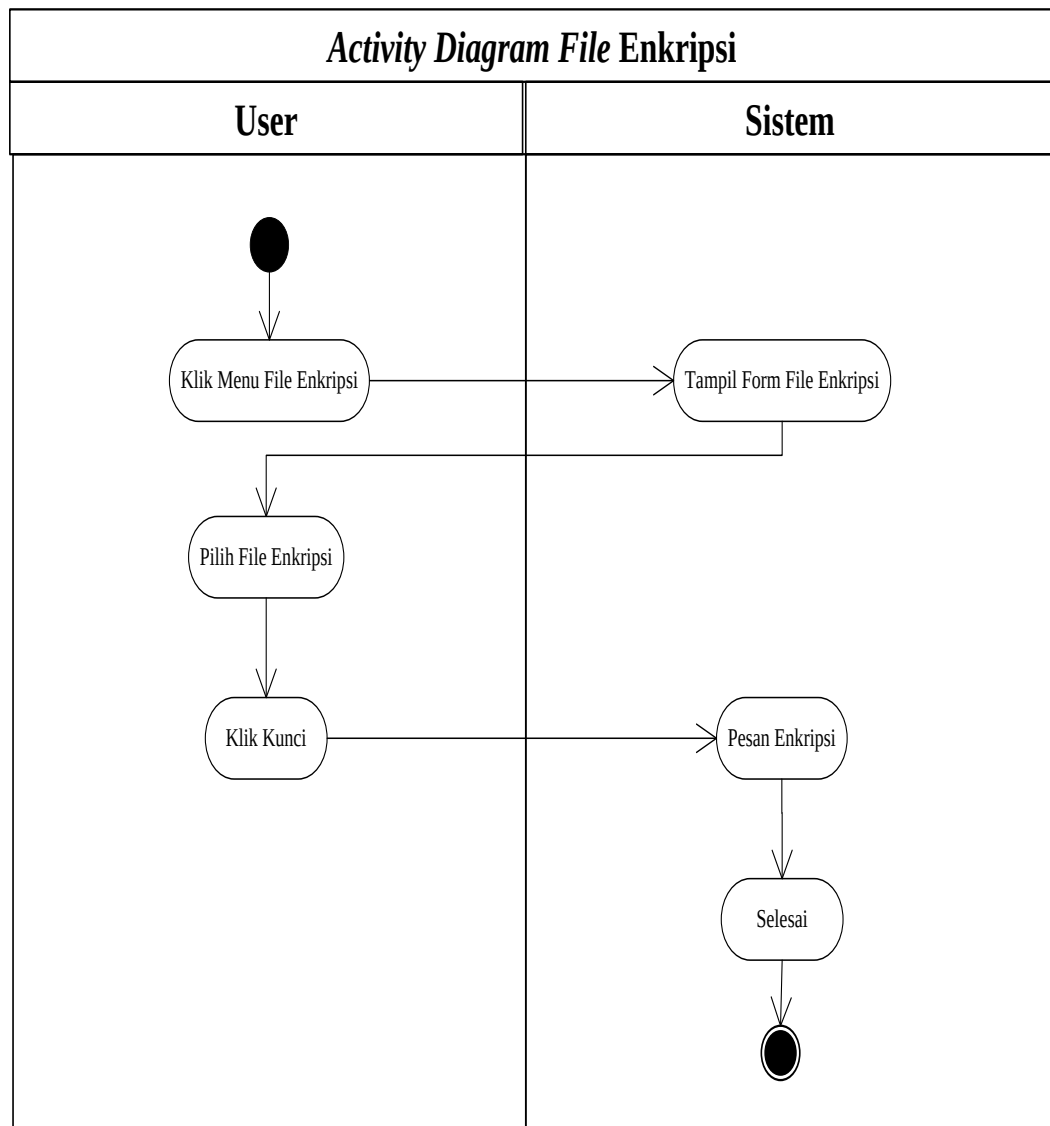
Activity Diagram Enkripsi halaman ini user melakukan pengamanan data enkripsi dapat dilihat pada gambar III.11 berikut:



Gambar III.11 Activity Diagram Enkripsi

4. Activity Diagram File Enkripsi

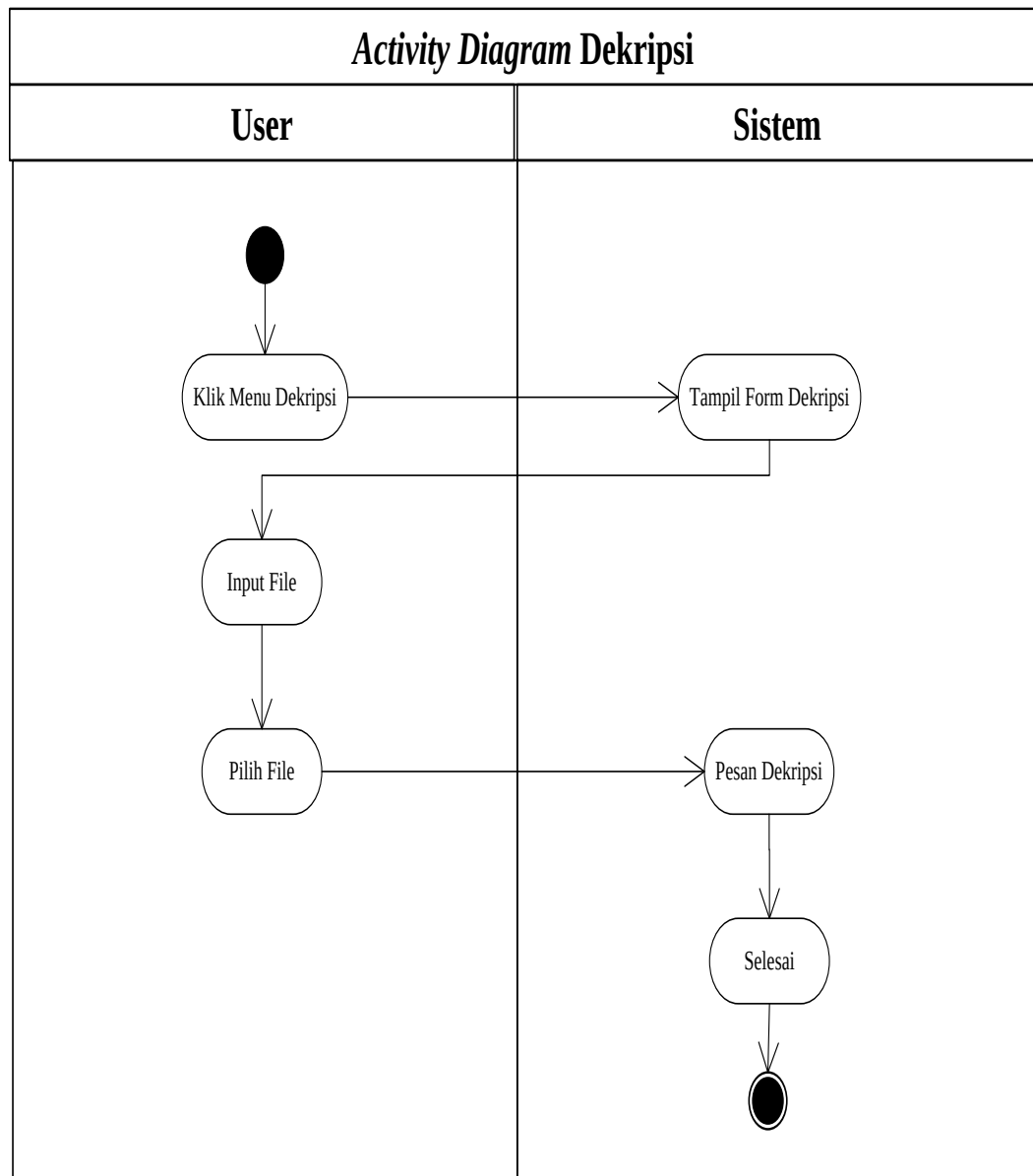
Activity Diagram File Enkripsi halaman ini user memilih file yang akan dilakukan enkripsi dapat dilihat pada gambar III.12 berikut:



Gambar III.12. Activity Diagram File Enkripsi

5. Activity Diagram Dekripsi

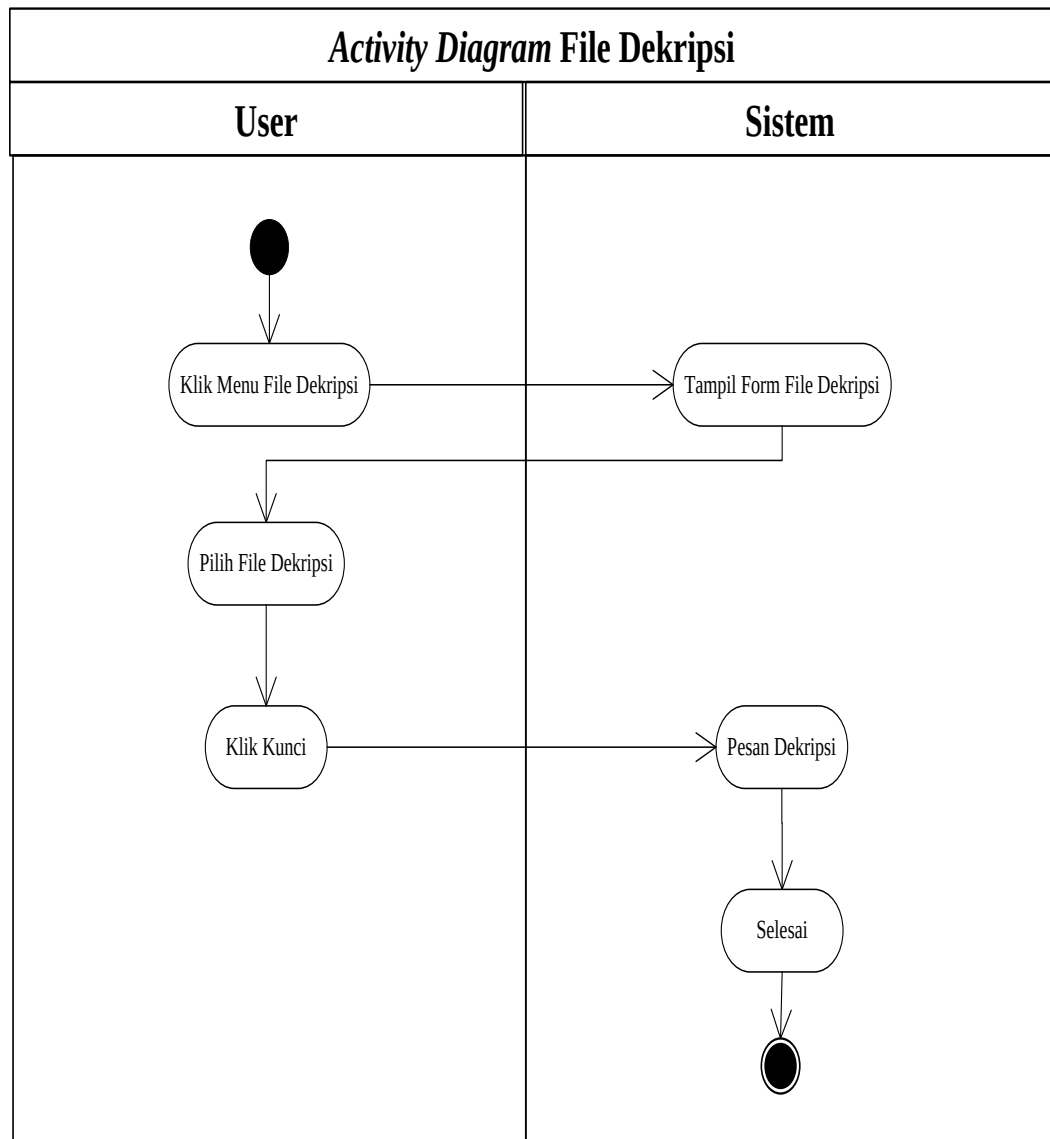
Activity Diagram Dekripsi halaman ini user melakukan pembukaan kunci keamanan file dapat dilihat pada gambar III.13 berikut:



Gambar III.13. Activity Diagram Dekripsi

6. Activity Diagram File Dekripsi

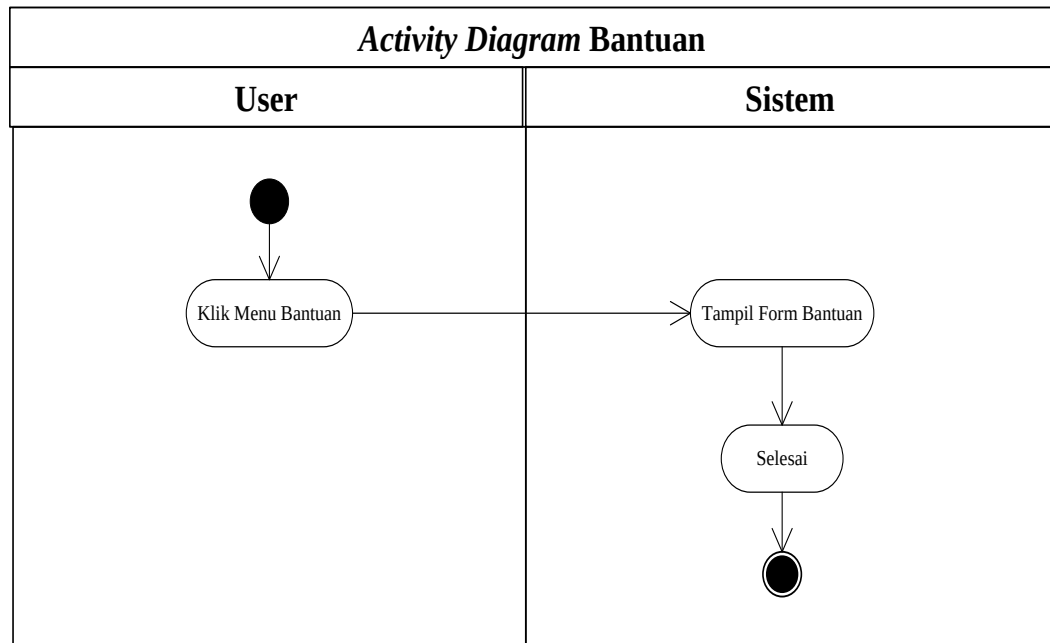
Activity diagram file Deskripsi halaman ini user mengambil file yang sudah dilakukan enkripsi oleh user untuk melakukan proses deskripsi file dapat dilihat pada gambar III.14 berikut:



Gambar III.14 Activity Diagram File Enkripsi

7. Activity Diagram Bantuan

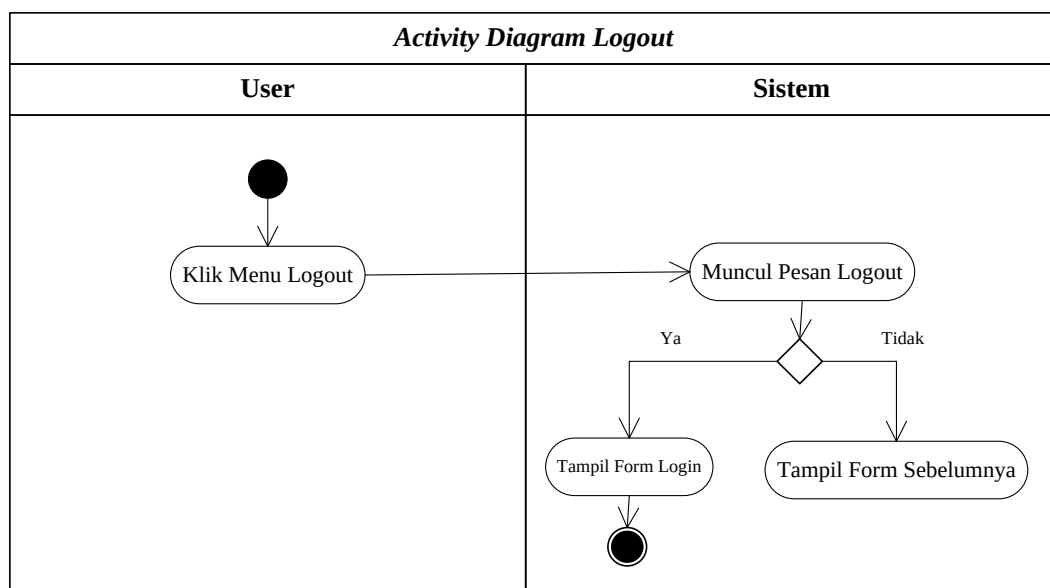
Activity Diagram Bantuan pada halaman ini user bisa memilih bantuan untuk mengetahui cara kerja sistem yang akan dijalankan dapat dilihat pada gambar III.15 berikut:



Gambar III.15 Activity Diagram Bantuan

8. Activity Diagram Logout

Activity Diagram Logout pada halaman ini user melakukan *logout* atau keluar dari sistem setelah menjalankan proses sistem atau dapat dilihat pada gambar III.16 berikut:



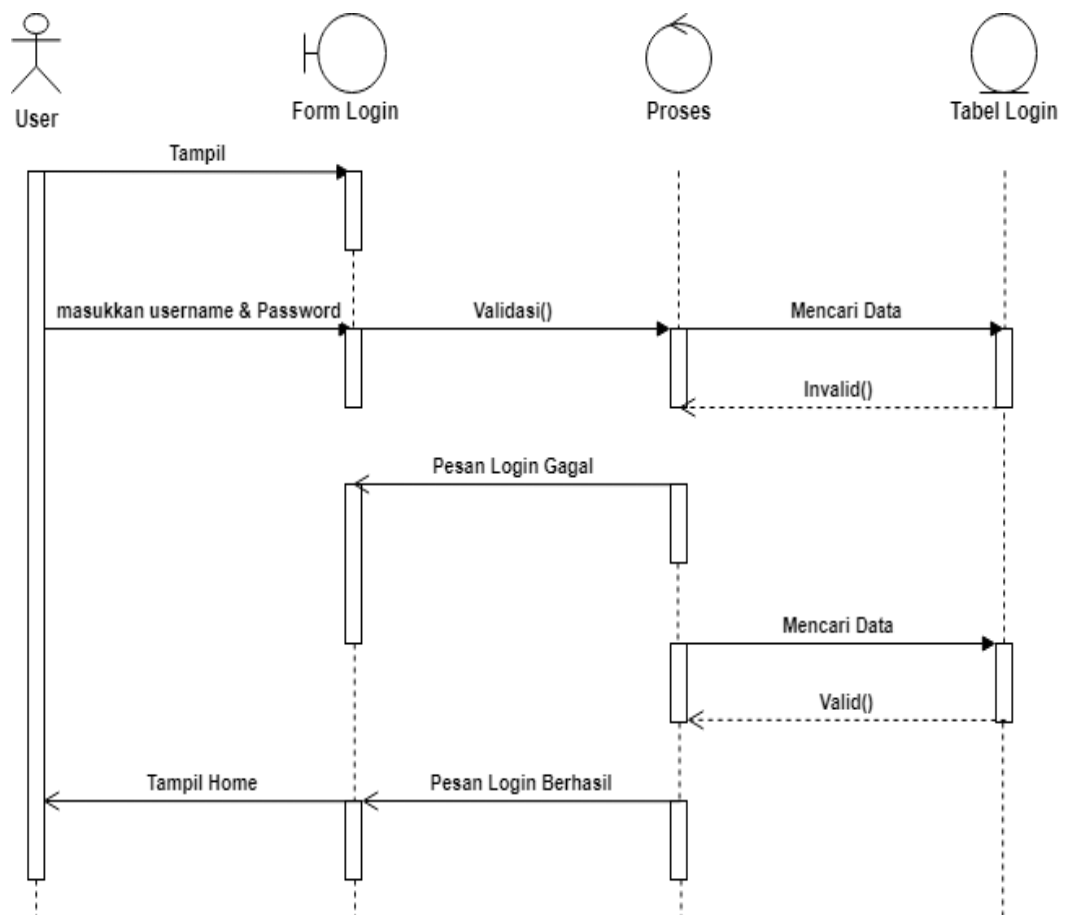
Gambar III.16. Activity Diagram Logout

III.3.4. Sequence Diagram

Rangkaian kegiatan pada setiap terjadi pada sistem digambarkan pada *Sequence diagram* berikut:

1. SequenceDiagram Login

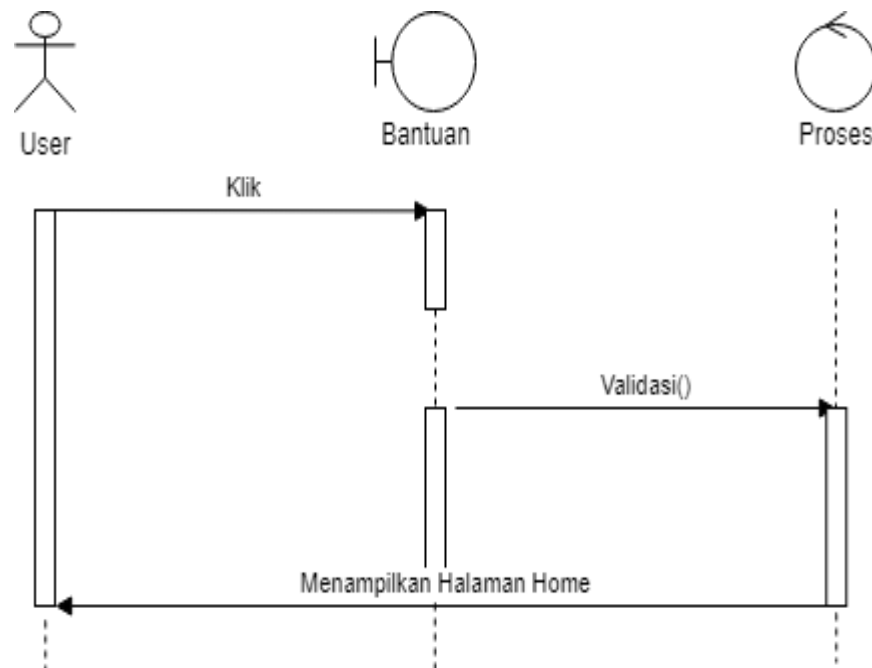
Sequence Diagram Login ini adalah alur proses melakukan login user dapat dilihat pada gambar III.17 berikut:



Gambar III.17. Sequence Diagram Login

2. Sequence Diagram Home

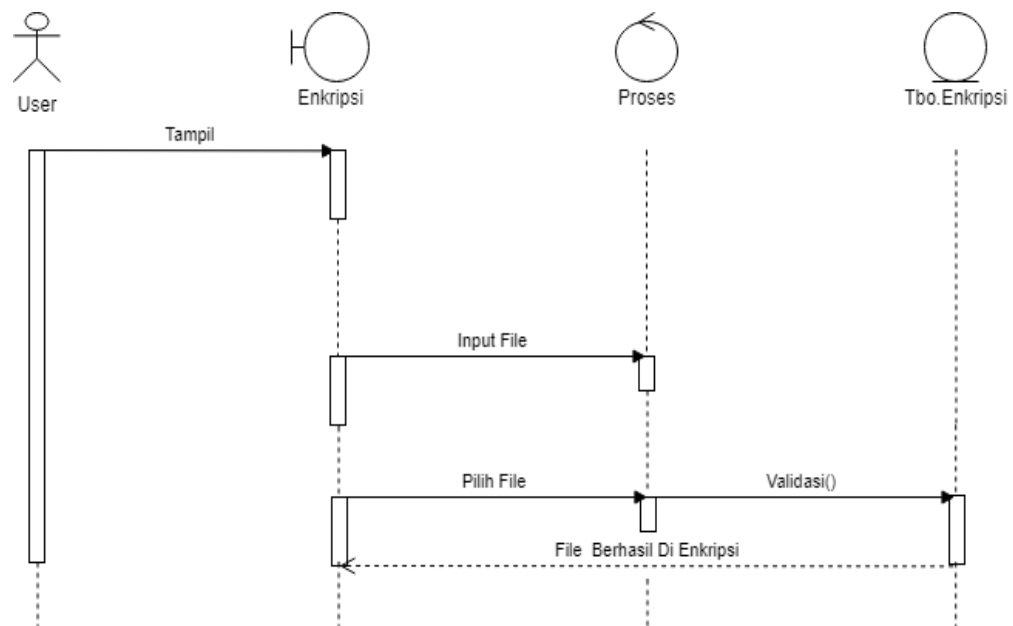
Sequence Diagram Home ini adalah alur proses melakukan home dapat dilihat pada gambar III.18 berikut:



Gambar III.18. Sequence Diagram Home

3. Sequence Diagram Enkripsi

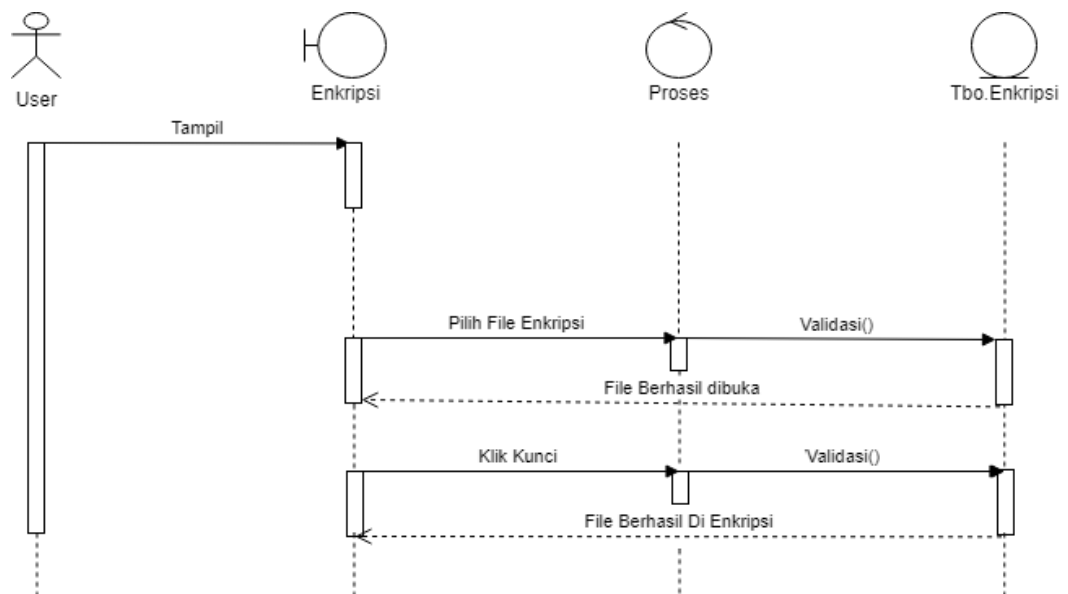
Sequence Diagram Enkripsi ini adalah alur proses melakukan enkripsi dapat dilihat pada gambar III.19 berikut:



Gambar III.19. Sequence Diagram Enkripsi

4. Sequence Diagram File Enkripsi

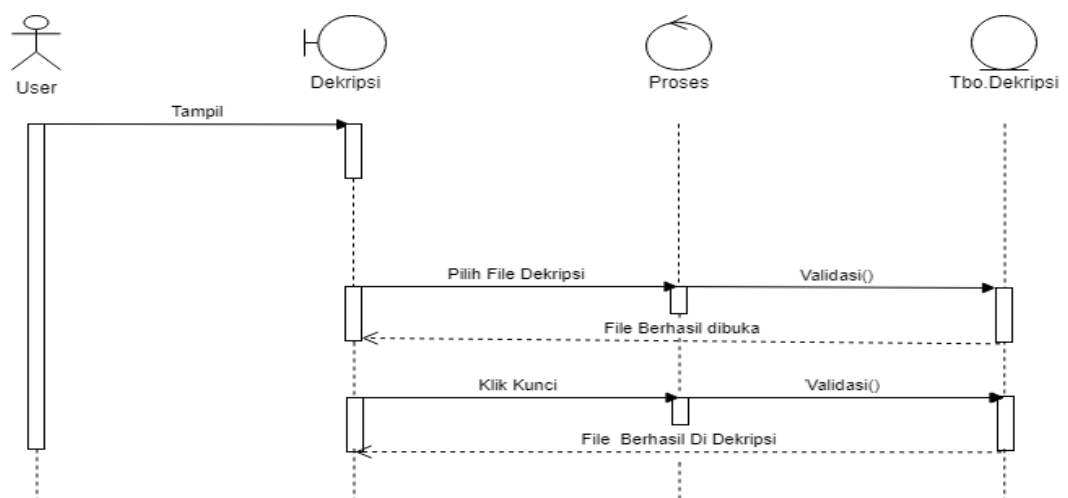
Sequence Diagram File Enkripsi ini adalah alur proses melakukan file enkripsi dapat dilihat pada gambar III.20 berikut:



Gambar III.20. Sequence Diagram File Enkripsi

5. Sequence Diagram Dekripsi

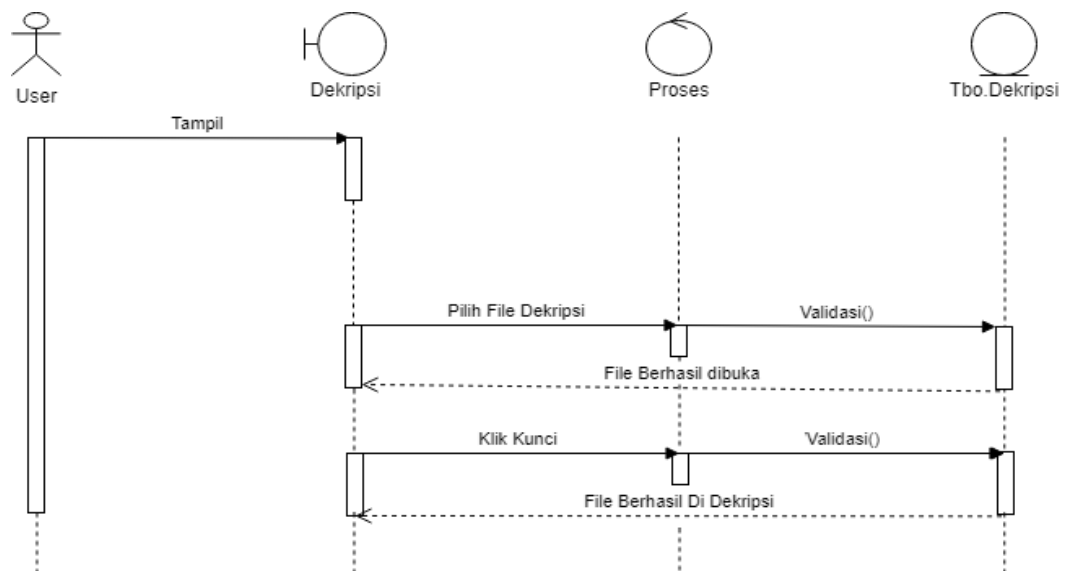
Sequence Diagram Dekripsi ini adalah alur proses melakukan Deskripsi dapat dilihat pada gambar III.21 berikut:



Gambar III.21. Sequence Diagram Dekripsi

6. Sequence Diagram File Dekripsi

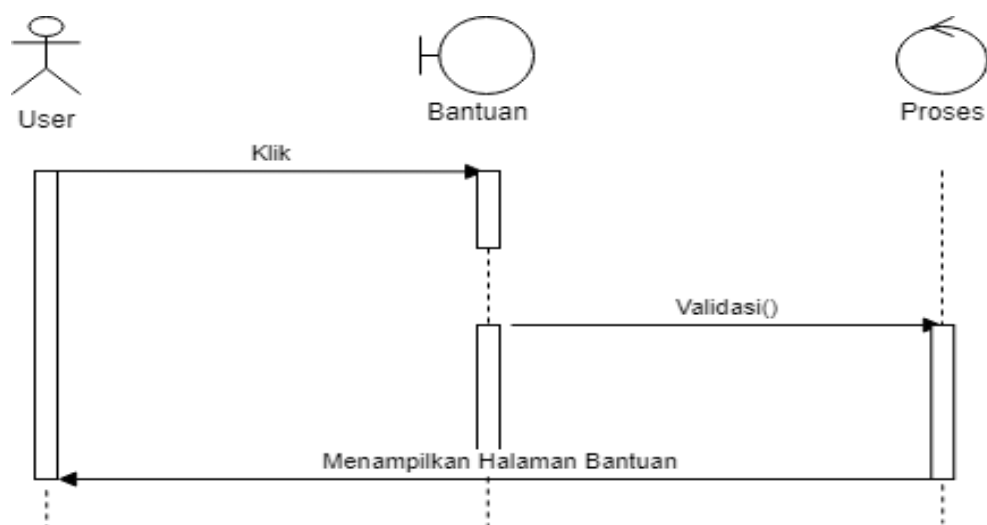
Sequence Diagram File Dekripsi ini adalah alur proses melakukan file deskripsi dapat dilihat pada gambar III.22 berikut:



Gambar III.22 Sequence Diagram File Dekripsi

7. Sequence Diagram Bantuan

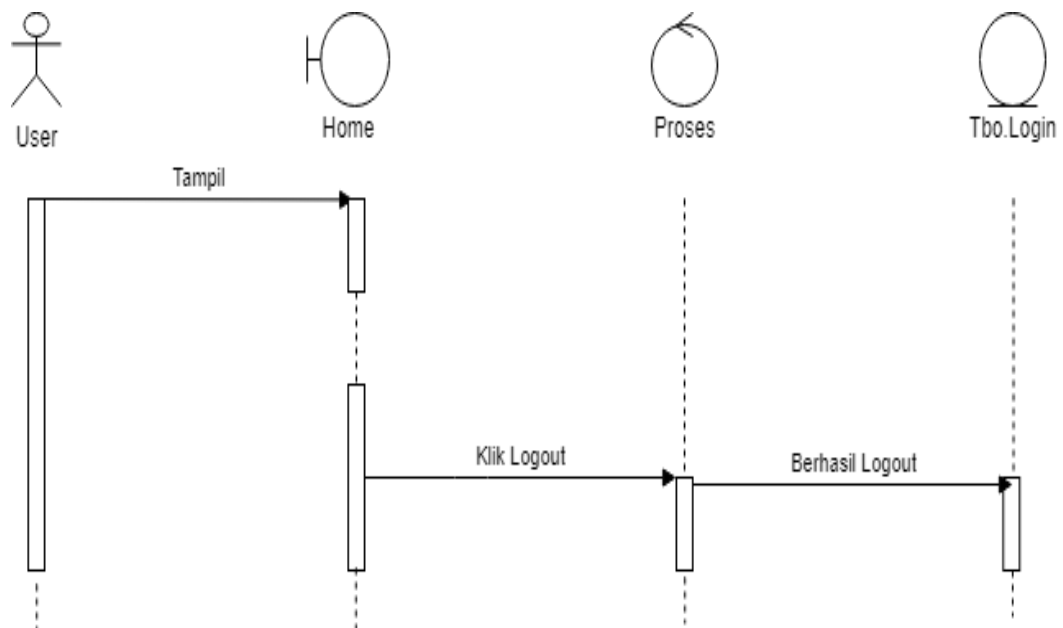
Sequence Diagram Bantuan ini adalah alur proses melakukan form bantuan dapat dilihat pada gambar III.23 berikut:



Gambar III.23. Sequence Diagram Bantuan

8. Sequence Diagram Logout

Sequence Diagram Logout ini adalah alur proses melakukan *logout* yang dilakukan oleh *user* dapat dilihat pada gambar III.24 berikut:



Gambar III.24. Sequence Diagram Logout

III.4. Desain Tabel

Merancang struktur tabel pada basis data sistem yang akan dibuat, berikut ini merupakan rancangan struktur tabel tersebut:

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.16. Tabel Admin

No	Nama Field	Tipe Data	Ukuran	Kunci
1.	Kd_admin	Varchar	50	<i>Primary Key</i>
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.17. Tabel Enkripsi

No	Nama Field	Tipe Data	Ukuran	Kunci
1.	id	Varchar	50	<i>Primary Key</i>
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 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.18. Tabel Deskripsi

No	Nama Field	Tipe Data	Ukuran	Kunci
1.	Id	Varchar	50	<i>Primary Key</i>
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	-	-

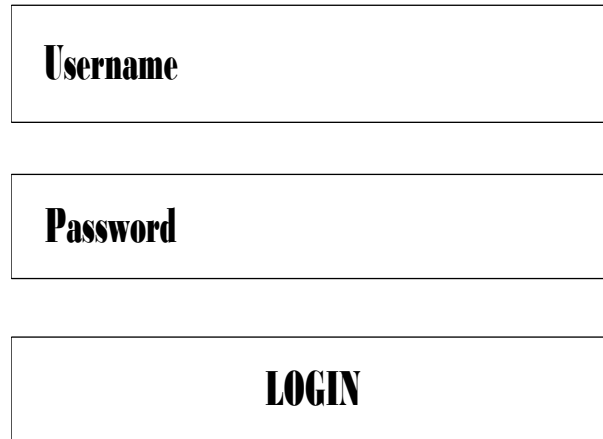
III.4. Desain User Interface

Tahap perancangan berikutnya yaitu desain sistem secara detail yang meliputi desain halaman *user* sebagai berikut:

1. Perancangan Desain 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.25 sebagai berikut:

Silahkan Login

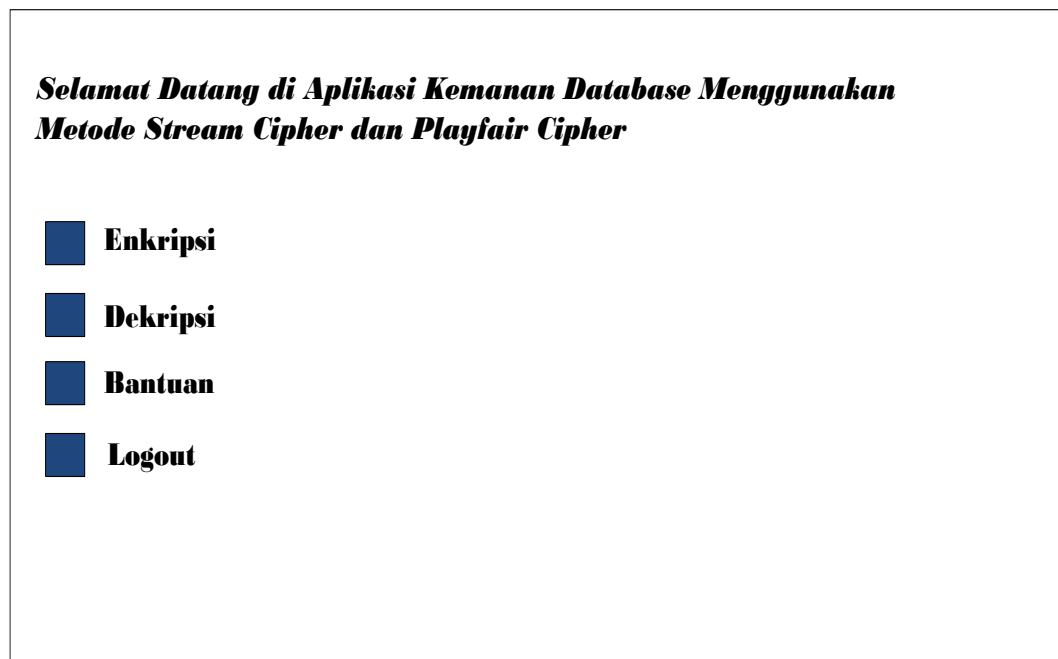


The login form consists of three vertically stacked rectangular boxes. The top box contains the text 'Username', the middle box contains 'Password', and the bottom box contains the text 'LOGIN' in all caps.

Gambar III.25. Perancangan Desain Login

2. Perancangan Desain Home

Perancangan *form Home* ini terdiri dari empat buah *menu bar*. Untuk lebih jelasnya, perancangan *form Home* dapat dilihat pada Gambar III.26 sebagai berikut:



The home form is enclosed in a large rectangular border. At the top, it features a bold welcome message: 'Selamat Datang di Aplikasi Keamanan Database Menggunakan Metode Stream Cipher dan Playfair Cipher'. Below this message, there is a vertical list of four menu items, each preceded by a small blue square icon: 'Enkripsi', 'Dekripsi', 'Bantuan', and 'Logout'.

Gambar III.26. Perancangan Desain Home

3. Perancangan *Desain* Enkripsi

Perancangan *form* Enkripsi, untuk lebih jelasnya, perancangan *form* Enkripsi yang berisi form tanggal, nama file, dan proses enkripsi dapat dilihat pada Gambar III.27 sebagai berikut:

Home File Bantuan Logout		Form Enkripsi Metode Stream Cipher dan Playfair Cipher Tanggal Nama File File Choose File Enkripsi
---	--	--

Gambar III.27. Perancangan *Desain* Enkripsi

4. Perancangan *Desain* File Enkripsi

Perancangan *form* File Enkripsi, untuk lebih jelasnya, perancangan *form* Enkripsi berisi file yang sudah dilakukan enkripsi dan terdapat tanggal, nama file, maupun jenis file yang sudah dilakukan enkripsi dapat dilihat pada Gambar III.28 sebagai berikut:

Form Data File Enkripsi

Tanggal	Nama File	Jenis File	File	Aksi
xxx	xxx	xxx	xxx	Dekripsi

Gambar III.28. Perancangan *Desain* Data File Enkripsi

5. Perancangan *Desain* Dekripsi

Perancangan *form* Dekripsi, untuk lebih jelasnya, pserancangan *form* Dekripsi memiliki tanggal, nama *file* dan proses deskripsi dapat dilihat pada Gambar III.29 sebagai berikut:

Home
File
Bantuan
Logout

Form Dekripsi Metode Stream Cipher dan Playfair Cipher

Tanggal

Nama File

File

Gambar III.29. Perancangan *Desain* Dekripsi

6. Perancangan *Desain File* Dekripsi

Perancangan *form File* Dekripsi, untuk lebih jelasnya, perancangan *form* Dekripsi yang terdapat tanggal, nama *file*, dan jenis file yang sebelumnya kita lakukan enkripsi dapat dilihat pada Gambar III.30 sebagai berikut:

12:00

Form Data File Dekripsi

Tanggal	Nama File	Jenis File	File	Aksi
xxx	xxx	xxx	xxx	Enkripsi

Gambar III.30. Perancangan *Desain Data File* Dekripsi