

BAB III

ANALISIS DAN PERANCANGAN

III.1. Analisis Masalah

Analisa sistem pada yang berjalan bertujuan untuk mengidentifikasi serta melakukan evaluasi terhadap Implementasi Algoritma *ROT 13* dan *Vigenere Cipher* dalam pesan pada aplikasi *chat* berbasis *Android*. Adapun masalah yang terdapat pada sistem sebelumnya adalah belum adanya sebuah *system* yang menerapkan kombinasi *algoritma Rot 13* dan *Vigenere Cipher* dalam aplikasi *chatting* yang memudahkan masyarakat untuk saling berkomunikasi dengan aman.

Strategi dalam melakukan pemecahan masalah yang sedang dianalisa oleh penulis mengenai perancangan Implementasi Algoritma *ROT 13* dan *Vigenere Cipher* dalam pesan pada aplikasi *chat* berbasis *Android* adalah sebagai berikut :

1. Mengamankan pesan selama pengiriman
2. Menerapkan algoritma *ROT13* dan *Vigenere Cipher* dalam mengamankan pesan.
3. Bagaimana mengimplementasikan algoritma *Rot 13* dan *Vigenere Cipher* dalam aplikasi *chatting*?

III.2. Penerapan Metode Algoritma *ROT 13* dan *Vigenere Cipher*

Algoritma *ROT 13* dan *Vigenere Cipher* mengenkripsi dengan menggeser *Alphabet* sebanyak 13 kali dan menggunakan tabel kunci pada *vigenere cipher*. Tabel ini digunakan untuk *pseudo random* yang menggunakan

XOR dengan *plaintext* untuk menghasilkan *ciphertext*. Masing - masing elemen dalam tabel saling ditukarkan minimal sekali. Proses dekripsinya dilakukan dengan cara yang sama (karena *Xor* merupakan fungsi simetrik)

Setelah terbentuk *keystream*, kemudian *keystream* tersebut dimasukkan dalam operasi *XOR* dengan *plaintext* yang ada, dengan sebelumnya pesan dipotong-potong terlebih dahulu menjadi *byte-byte*.

III.2.1. Studi Kasus Algoritma

Berikut adalah implementasi Algoritma *ROT 13* dan *Vigenere Cipher* untuk lebih menyederhanakan dalam perhitungan manual serta untuk kebutuhan sistem yang sangat terbatas.

A. Proses Enkripsi

➤ ROT 13

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Rumus : Cipher = (Index Ke-n + 13) Mod 26

Plaintext	R	A	H	A	S	I	A
Index	17	0	7	0	18	8	0

Maka,

R	$C = (17 + 13) \text{ Mod } 26$	4	E
A	$C = (0 + 13) \text{ Mod } 26$	13	N
H	$C = (7 + 13) \text{ Mod } 26$	7	U
A	$C = (0 + 13) \text{ Mod } 26$	13	N
S	$C = (18 + 13) \text{ Mod } 26$	5	F
I	$C = (8 + 13) \text{ Mod } 26$	21	V
A	$C = (0 + 13) \text{ Mod } 26$	13	N

Hasil Enkripsi : E N U N F V N

➤ Vigenere Cipher

Plaintext	E	N	U	N	F	V	N
Index	4	13	20	15	5	21	13
Kunci	B	E	R	S	A	M	A
Index	1	4	17	18	0	12	0

Maka,

Rumus : $\text{Cipher} = (\text{Pt} + k) \text{ Mod } 26$

E	$\text{Cipher} = (4 + 1) \text{ Mod } 26$	5	F
N	$\text{Cipher} = (13 + 4) \text{ Mod } 26$	17	R
U	$\text{Cipher} = (20 + 17) \text{ Mod } 26$	11	L
N	$\text{Cipher} = (13 + 18) \text{ Mod } 26$	5	F
F	$\text{Cipher} = (5 + 0) \text{ Mod } 26$	5	F
V	$\text{Cipher} = (21 + 12) \text{ Mod } 26$	7	H
N	$\text{Cipher} = (13 + 0) \text{ Mod } 26$	13	N

Hasil Enkripsi :

R	A	H	A	S	I	A
F	R	L	F	F	H	N

B. Proses Dekripsi

➤ Vigenere Cipher

Chipertext	F	R	L	F	F	H	N
Index	5	17	11	5	5	7	13
Kunci	B	E	R	S	A	M	A
Index	1	4	17	18	0	12	0

Rumus : $= (Ci - k) \text{ Mod } 26$
 $= (Ci - k) + 26$ (Jika hasil minus)

F	$= (5 - 1) \text{ Mod } 26$	4	E
R	$= (17 - 4) \text{ Mod } 26$	13	N
L	$= (11 - 17) + 26$	20	U
F	$= (5 - 18) + 26$	13	N
F	$= (5 - 0) \text{ Mod } 26$	5	F
H	$= (7 - 12) \text{ Mod } 26$	21	V
N	$= (13 - 0) \text{ Mod } 26$	13	N

➤ ROT 13

$$\begin{aligned}\text{Rumus : } &= (C_i - 13) \bmod 26 \\ &= (C_i - 13) + 26 \text{ (Jika Hasil Minus)}\end{aligned}$$

E	$= (4 - 13) + 26$	17	R
N	$= (13 - 13) \bmod 26$	0	A
U	$= (20 - 13) \bmod 26$	7	H
N	$= (13 - 13) \bmod 26$	0	A
F	$= (5 - 13) + 26$	18	S
V	$= (21 - 13) \bmod 26$	8	I
N	$= (13 - 13) \bmod 26$	0	A

III.3. Perancangan

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.

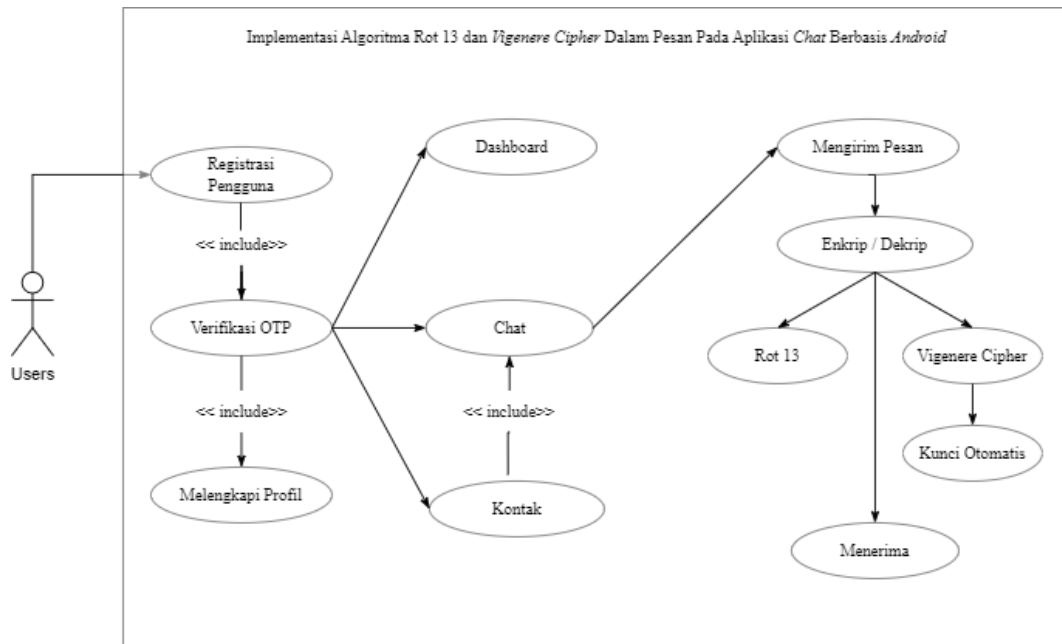
III.3.1. Desain Sistem Secara Global

Desain sistem secara global menggunakan bahasa pemodelan UML yang terdiri dari *Usecase Diagram*, *Activity Diagram* dan *Sequence Diagram*.

III.3.1.1 *Usecase Diagram*

Dalam penyusunan suatu program diperlukan suatu model data yang berbentuk diagram yang dapat menjelaskan suatu alur proses sistem yang akan dibangun. Dalam penulisan skripsi ini penulis menggunakan metode UML yang

dalam metode itu penulis menerapkan diagram *Use Case*. Maka digambarkanlah suatu bentuk diagram *Use Case* yang dapat dilihat pada gambar dibawah ini



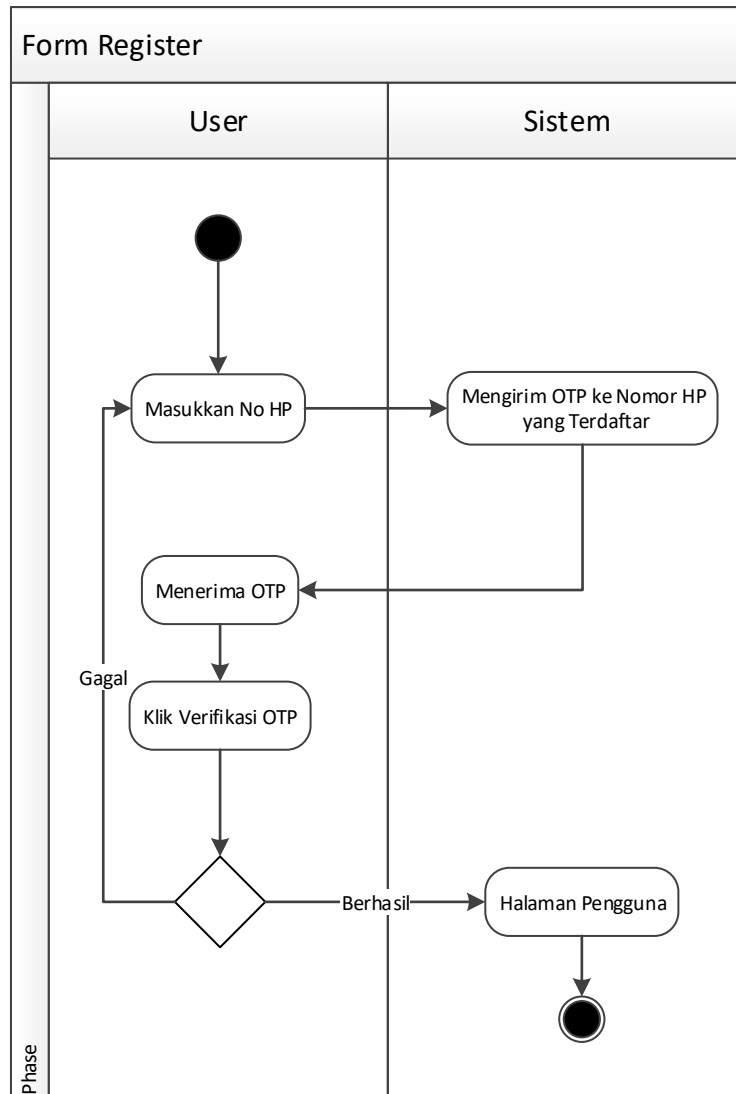
Gambar III. 1. Use Case Diagram Sistem Keamanan Aplikasi chat dengan Menggunakan Algoritma ROT 13 dan Vigenere Cipher

III.3.1.2. Activity Diagram

Bisnis proses yang telah digambarkan pada *use case diagram* dijabarkan dengan *activity diagram* :

1. Activity Diagram Register

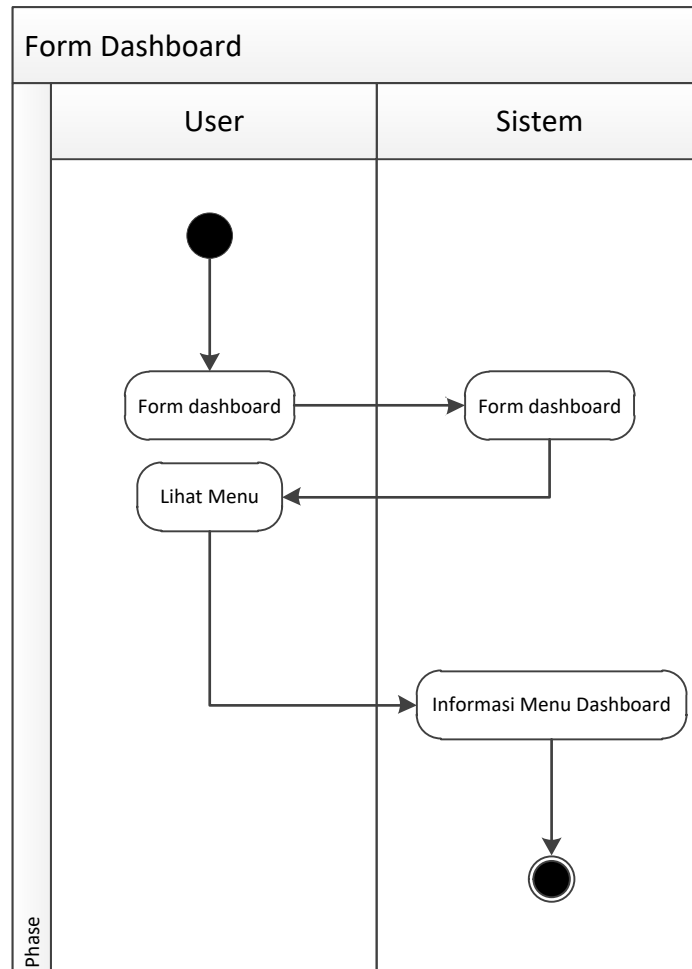
Aktivitas *register* yang dilakukan oleh user dapat diterangkan dengan langkah-langkah *state* berikut :



Gambar III. 2. Activity Diagram Register

3. Activity Diagram Dashboard

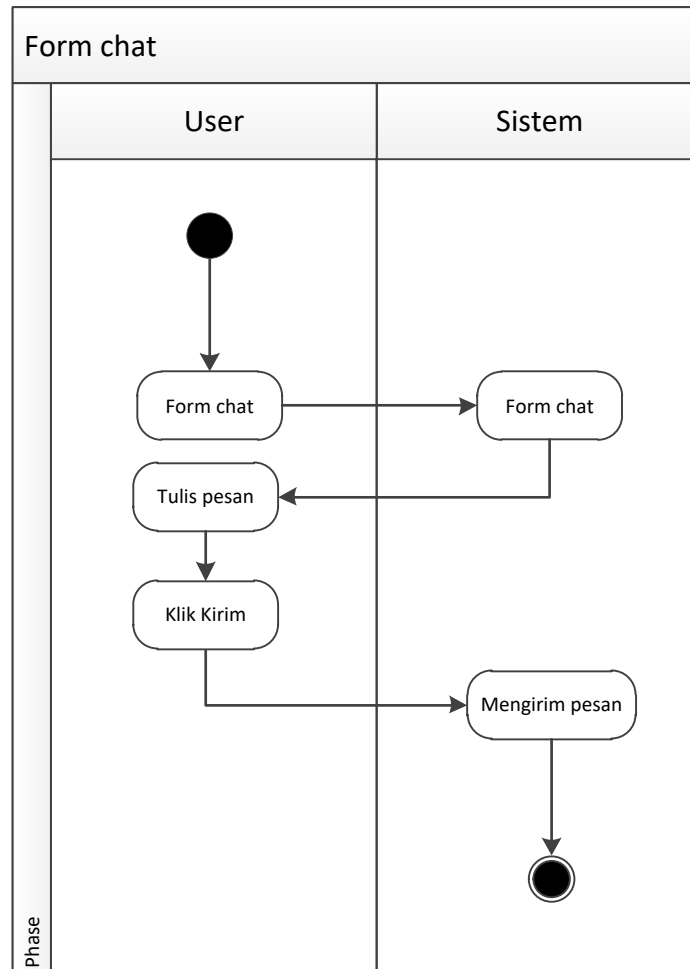
Aktivitas yang dilakukan oleh user pada form dashboard dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar berikut :



Gambar III. 3. Activity Diagram Form Dashboard

4. Activity Diagram Chat

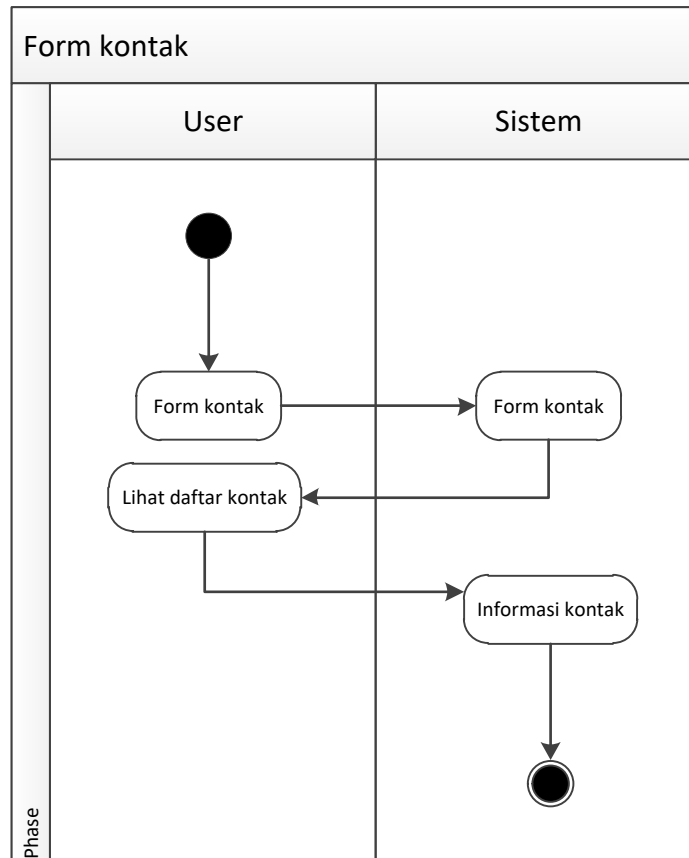
Aktivitas yang dilakukan oleh user pada form chat dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar berikut :



Gambar III. 4. Activity Diagram Form Chat

5. *Activity Diagram Kontak*

Aktivitas yang dilakukan oleh user pada form kontak dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar berikut :



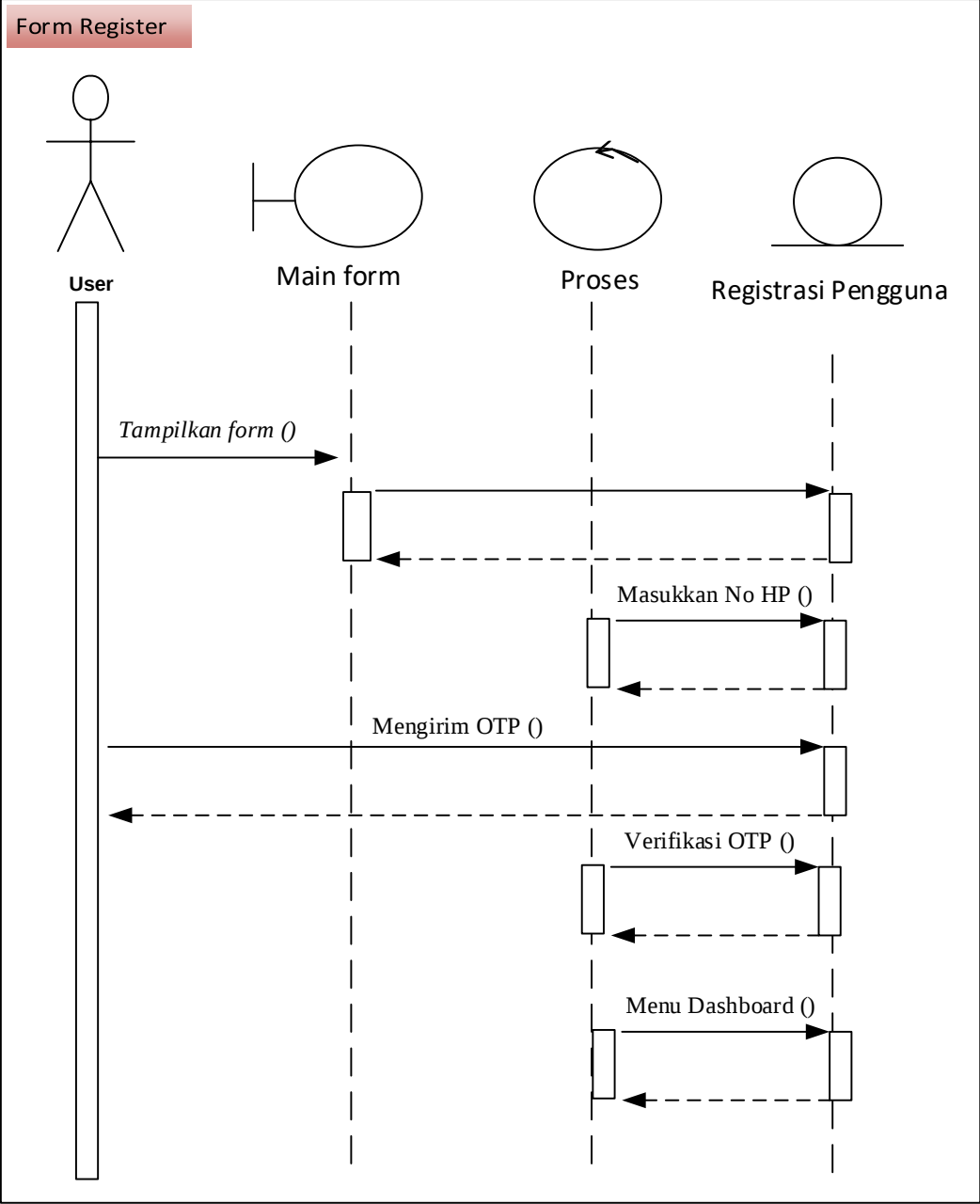
Gambar III. 5. Activity Diagram Form Kontak

III.3.13. Sequence Diagram

Sequence Diagram (diagram urutan) 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 Register

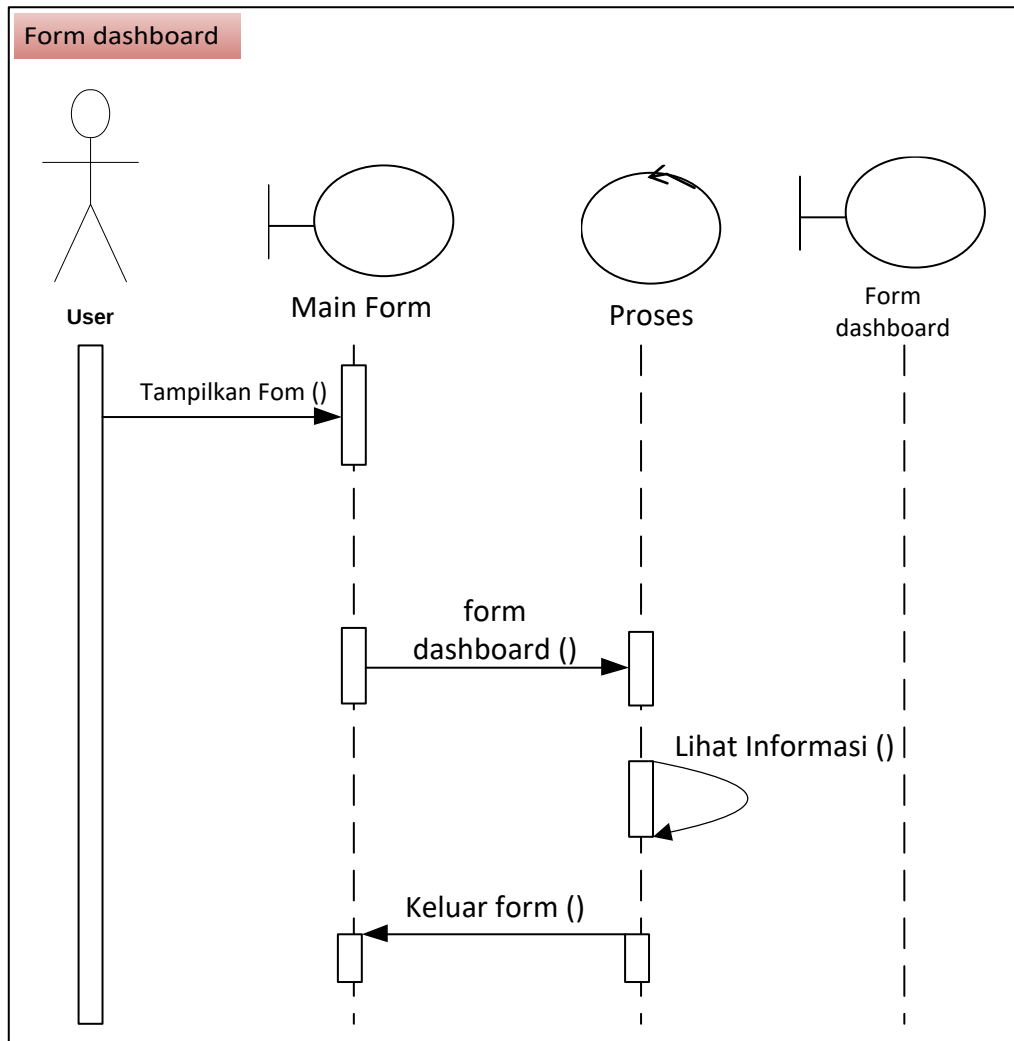
Serangkaian kegiatan sistem *register* yang dilakukan oleh user dapat diterangkan dengan langkah-langkah *state* berikut :



Gambar III. 6. Sequence Diagram Register

3. Sequence Diagram Dashboard

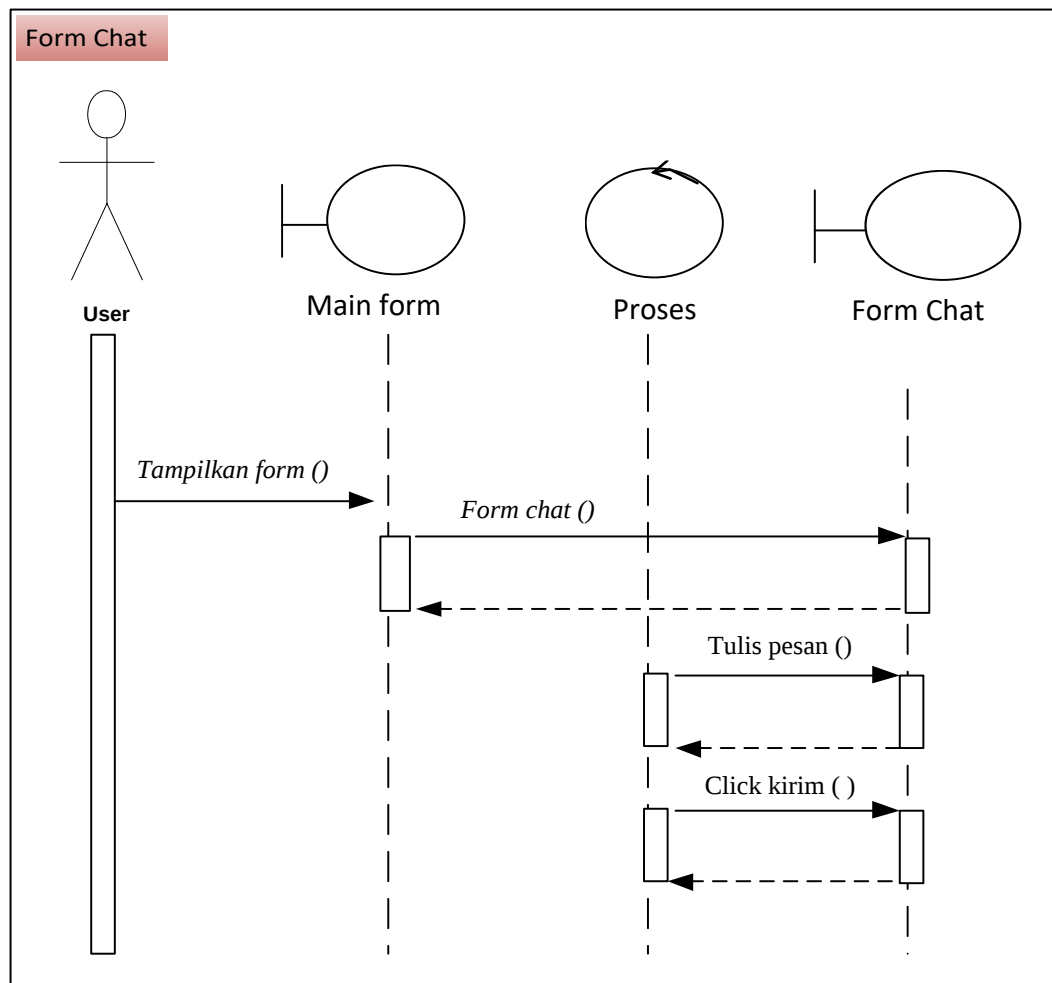
Serangkaian kegiatan sistem yang dilakukan oleh user pada form dashboard dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar berikut :



Gambar III. 7. Sequence Diagram Form Dashboard

4. Sequence Diagram Chat

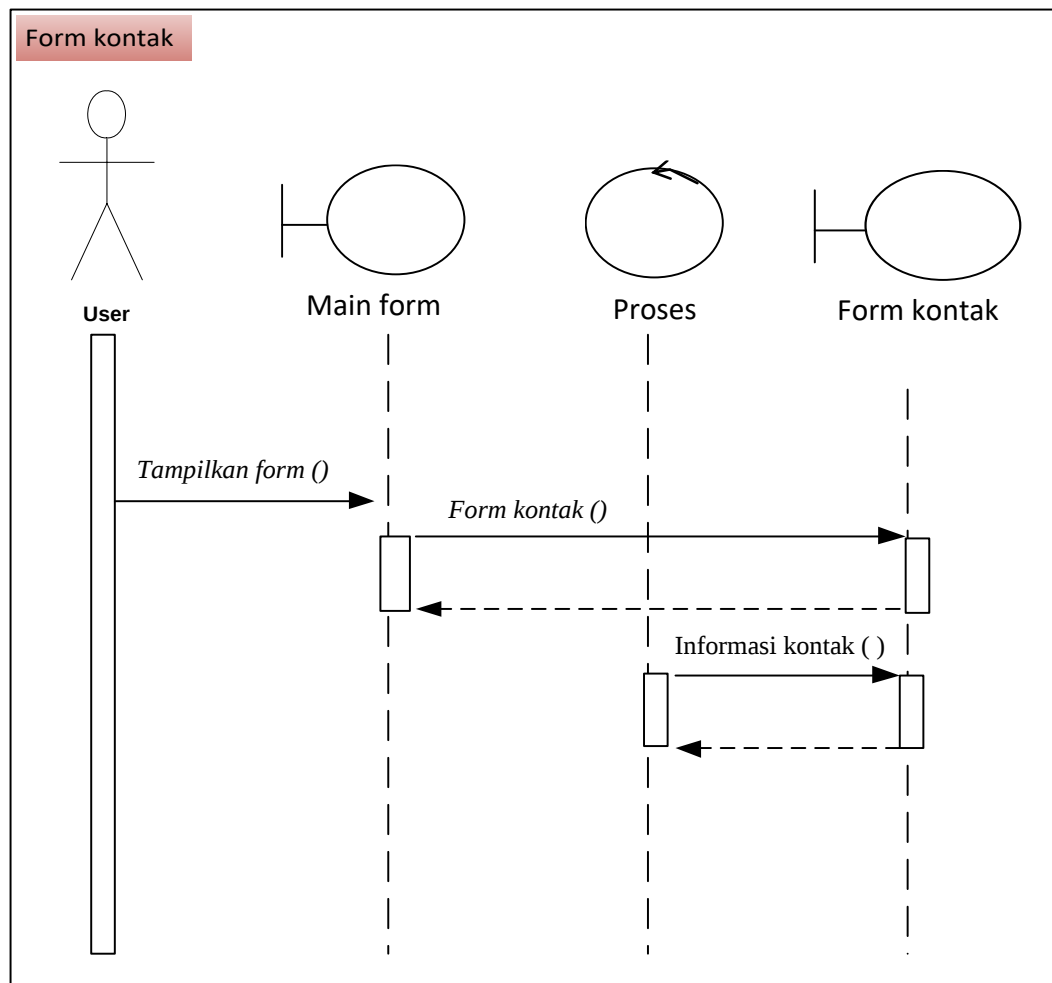
Serangkaian kegiatan sistem yang dilakukan oleh user pada form berkas pelajaran dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar berikut :



Gambar III. 8. Sequence Diagram Form Chat

5. Sequence Diagram Kontak

Serangkaian kegiatan sistem yang dilakukan oleh user pada form kontak dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar berikut :



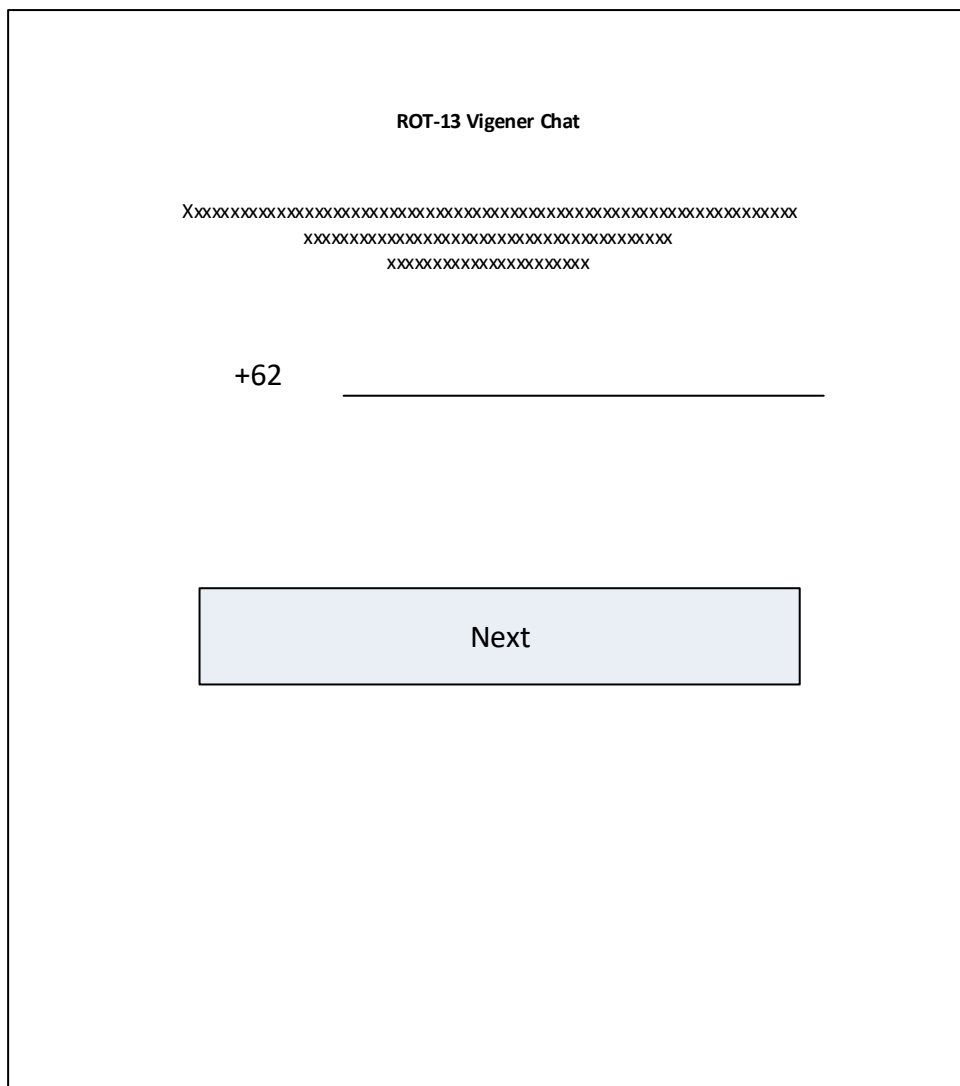
Gambar III.9. Sequence Diagram Form Kontak

III.3.3. Desain Sistem Secara Detail

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

1. Desain Tampilan *Register*

Serangkaian kegiatan sistem *register* yang dilakukan oleh user dapat diterangkan dengan langkah-langkah *state* berikut :



ROT-13 Vigenere Chat

XX
XX
XX

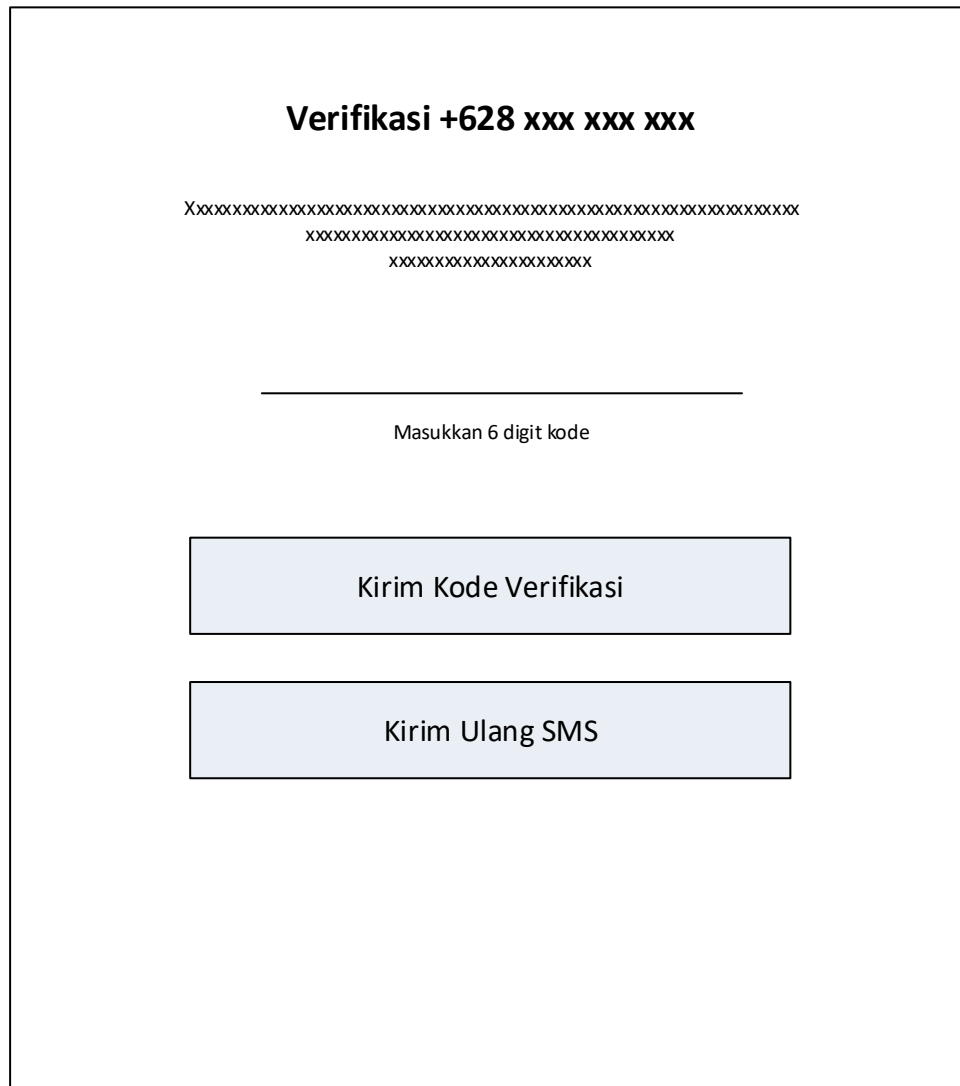
+62

Next

Gambar III. 10. Desain Tampilan Register

2. Desain Tampilan *Verifikasi OTP*

Serangkaian kegiatan sistem *verifikasi OTP* yang dilakukan oleh user dapat diterangkan dengan langkah-langkah *state* berikut :



Verifikasi +628 xxx xxx xxx

XX
XX
XX

Masukkan 6 digit kode

Kirim Kode Verifikasi

Kirim Ulang SMS

Gambar III. 11. Desain Tampilan Verifikasi OTP

3. Desain Tampilan Dashboard

Serangkaian kegiatan sistem yang dilakukan oleh user pada form dashboard dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar berikut :

ROT13 – Vigenere Chat	
Chat	Kontak
Chat 1	
Chat 2	
Chat 3	

Gambar III. 12. Desain Tampilan Form Dashboard

4. Tampilan Desain *Form Chat*

Serangkaian kegiatan sistem yang dilakukan oleh user pada form chat dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar berikut :

Info Profil

Logo

Next

Gambar III. 15. Desain Profil