BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisis Masalah

Dalam kehidupan sehari-hari sering ditemukan masalah yang berhubungan dengan keuangan. Mengatur keuangan merupakan persoalan klasik di kehidupan. Ada beberapa orang yang sering kali mengalami yang namanya krisis keuangan, misalnya selalu merasa kurang dengan penghasilan atau uang bulanan. Krisis keuangan terjadi pada umumnya bukan karena kurangnya penghasilan tapi seringkali karena pengaturan keuangan yang tidak tepat. Dari hal tersebut di dapat kesimpulan bahwa untuk meningkatkan efisiensi dalam pengelolaan catatan keuangan untuk menghindari masalah krisis dapat dilakukan dengan baik menggunakan sebuah aplikasi pencatatan keuangan pribadi.

Berdasarkan masalah yang di temukan tersebut, dilakukan wawancara terhadap 12 orang responden yang sudah bekerja dikisaran waktu antara 4 sampai dengan 27 tahun dengan memberikan pertanyaan sebagai berikut :

1. Bagaimana mereka melakukan pengelolaan keuangan pribadinya?
2. Apakah mereka mencatatnya atau tidak ?
3. Bagaimana cara pencatatan keuangan pribadi dilakukan ?
4. Kesulitan apa saja yang ditemukan dalam proses mencatat keuangan pribadi harian ?

Dari pertanyaan tersebut ditemukan kesimpulan bahwa 8 orang responden diantaranya melakukan pencatatanya secara manual pada sebuah buku dan 4 orang lainnya tidak mencatat pengeluarannya. Cara pencatatan seperti itu terkadang memunculkan masalah seperti tidak efisiennya proses pencatatan karena susahnya pengelompokan pengeluaran berdasarkan kategori berbeda, tidak efesiensi dalam melakukan pencarian pengeluaran pada hari, minggu atau bulan tertentu. Masalah lain yang ditemukan adalah responden menyatakan bahwa data keuangan pribadi adalah suatu hal yang bersifat rahasia sehingga sebisa mungkin catatan keuangan pribadi tersebut tidak boleh diketahui oleh orang lain.

Dari hal tersebut di dapat kesimpulan bahwa untuk meningkatkan efisiensi dalam pengelolaan catatan keuangan dapat dilakukan dengan baik menggunakan sebuah aplikasi pencatatan keuangan pribadi. Selain meningkatkan efisiensi dalam proses pengelolaan catatan keuangan pribadi harian, dengan menggunakan aplikasi dapat mempermudah dalam pencarian catatan berdasarkan hari, minggu atau bulan. Dengan menggunakan sebuah aplikasi dapat juga diterapkan sebuah metode yang dapat merahasiakan data pengelolaan keuangan pribadi dengan memanfaatkan algoritma RC4. Cara kerjanya adalah data pengelolaan keuangan pribadi disandikan kedalam bentuk lain sehingga hanya dapat diketahui isinya oleh orang yang menyandikannya saja menggunakan kunci yang di tentukan oleh pengguna.

III.2. Strategi Pemecahan Masalah

Beberapa strategi pemecahan masalah dalam rancang bangun aplikasi keamanan data catatan keuangan harian pribadi menggunakan algoritma RC4 berbasis android ini adalah sebagai berikut:

1. Aplikasi ini dirancang agar dapat digunakan secara *mobile* pada perangkat dengan sistem operasi android.
2. Aplikasi ini digunakan untuk melakukan pencatatan pengeluaran pribadi seperti pengeluaran untuk rumah tangga, makan, kantor, transportasi, hobi dan lainnya.
3. Pada aplikasi ini akan diterapkan algoritma RC4 yang bertujuan untuk menyandikan catatan keuangan pribadi sehingga tidak dapat diketahui isinya oleh orang lain.
4. Dengan menggunakan aplikasi ini pengguna dapat melihat laporan pengeluaran berdasarkan harian, mingguan, bulanan dan keseluruhan pengeluaran.

III.3. Analisa Kebutuhan Sistem

Pembuatan aplikasi ini membutuhkan serangkaian peralatan yang dapat mendukung kelancaran proses rancang bangun aplikasi keamanan data catatan keuangan harian pribadi menggunakan algoritma RC4 berbasis android. Berikut ini aspek-aspek yang di butuhkan.

III.3.1. Kebutuhan Perangkat Keras (*Hardware*)

Hardware merupakan komponen yang terlihat secara fisik, yang saling bekerjasama dalam pengolahan data. Spesifikasi *minimum hardware* yang digunakan adalah sebagai berikut :

III.3.1.1. PC

PC yang dapat digunakan untuk merancang aplikasi pada penelitian ini memiliki spesifikasi minimum sebagai berikut :

a. Prosesor Intel *Core* i3
b. RAM 4 GB

III.3.1.2. *Smartphone*

Smartphone yang akan digunakan untuk uji coba aplikasi yang dihasilkan dari penelitian ini memiliki spesifikasi minimum sebagai berikut :

a. Android OS 5.0
b. Ram 1 GB

III.3.2. Kebutuhan Perangkat Lunak (*Software*)

Software adalah intruksi atau program-program komputer yang dapat digunakan oleh komputer dengan memberikan fungsi serta penampilan yang diinginkan. Dalam hal ini *software* yang digunakan dalam perancangan aplikasi adalah:

a. Sistem Operasi *Microsoft* Windows 7

b. Android Studio

III.4. Penerapan Algoritma RC4

Misalnya, Implementasikan algoritma RC4 menggunakan mode 4 *byte* untuk mengenkripsi *plaintext* DEDI dengan kunci 13.

1. Inisialisasi *array* S-box dengan panjang 4 *byte* sehingga *array* S-box *array* S berbentuk S[0]=0, S[1]=1, S[2]=2, S[3]=3.

Index	0	1	2	3
S	0	1	2	3

2. Inisialisasi *array* kunci (S-box lain). Karena pada contoh digunakan algoritma RC4 dengan mode 4 byte, kunci K diulang sampai panjang 4 *byte* sehingga kunci K= [1313], S-box *array* kunci berbentuk K[0]=1, K[1]=3, K[2]=1, K[3]=3.

Index	0	1	2	3
K	1	3	1	3

3. Lakukan permutasi terhadap nilai-nilai di dalam *array* S dengan cara menukarkan isi *array* S[i] dengan S[j] dengan mode 4 prosesnya berikut :

   j = 0

   For i = 0 to 3

   j = (j + S[i] + K[i]) mod 4

isi S[i] dan isi S[j] ditukar.

Dengan menggunakan algoritma tersebut, untuk nilai i = 0 sampai i = 3 didapatkan nilai *array* S berikut:

Iterasi pertama, untuk nilai i = 0

j = (j + S[i] + K[i]) mod 4

j = (j + S[0] + K[0]) mod 4

j = (0 + 0 + 1) mod 4

j = 1

Dilakukan penukaran isi *array* S[0] dan S[1] sehingga *array* S berbentuk :

Index	0	1	2	3
S	1	0	2	3

Iterasi kedua untuk nilai j = 1 dan i = 1

j = (j + S[i] + K[i]) mod 4

j = (1 + S[1] + K[1]) mod 4

j = (1 + 0 + 3) mod 4

j = 0

Dilakukan penukaran isi *array* S[1] dan S[0] sehingga *array* S berbentuk :

Index	0	1	2	3
S	0	1	2	3

Iterasi ketiga untuk nilai j = 0 dan i = 2

j = (j + S[i] + K[i]) mod 4

j = (0 + S[2] + K[2]) mod 4

j = (0 + 2 + 1) mod 4

j = 3

Dilakukan penukaran isi *array* S[2] dan S[3] sehingga *array* S berbentuk :

Index	0	1	2	3
S	0	1	3	2

Iterasi keempat untuk nilai j = 3 dan i = 3

j = (j + S[i] + K[i]) mod 4

j = (3 + S[3] + K[3]) mod 4

j = (3 + 2 + 3) mod 4

j = 0

Dilakukan penukaran isi *array* S[3] dan [0] sehingga *array* S berbentuk :

Index	0	1	2	3
S	2	1	3	0

4. Untuk mendapatkan *ciphertext*, terlebih dahulu bangkitkan *keystream* sebanyak 3 *byte*, proses membangkitkan kunci enkripsi pada mode 4 *byte* sebagai berikut :

   i = j = 0

   i = (i + 1) mod 4

   i = (j + S[i]) mod 4

isi S[i] dan S[j] ditukar

t = (S[i] + S[j]) mod 4

K = S[t]

Dengan menggunakan algoritma tersebut, bisa membangkitkan 4 buah kunci proses enkripsi sebagai berikut:

Iterasi pertama, untuk nilai i = j = 0, maka

i = (i + 1) mod 4

i = (0 + 1) mod 4

i = 1

j = (j + S[i]) mod 4

j = (0 + S[1]) mod 4

j = (0 + 1) mod 4

j = 1

Menukarkan isi S[1] dan S[1] sehingga *array* S berbentuk :

Index	0	1	2	3
S	2	1	3	0

t = (S[1] + S[1]) mod 4

t = (1 + 1) mod 4

t = 2

K = S[t] = S[2] = 3

Iterasi kedua, untuk nilai i = 1 dan j = 1 maka

i = (i + 1) mod 4

i = (1 + 1) mod 4

i = 2

j = (j + S[i]) mod 4

j = (1 + S[2]) mod 4

j = (1 + 3) mod 4

j = 0

Menukarkan isi S[2] dan S[0] sehingga *array* S berbentuk :

Index	0	1	2	3
S	3	1	2	0

t = (S[2] + S[0]) mod 4

t = (2+ 3) mod 4

t = 1

K = S[t] = S[1] = 1

Iterasi ketiga, untuk nilai i = 2 dan j = 0 maka

i = (i + 1) mod 4

i = (2 + 1) mod 4

i = 3

j = (j + S[i]) mod 4

j = (0 + S[3]) mod 4

j = (0 + 0) mod 4

j = 0

Menukarkan isi S[3] dan S[0] sehingga *array* S berbentuk :

Index	0	1	2	3
S	0	1	2	3

t = (S[3] + S[0]) mod 4

t = (3+ 0) mod 4

t = 3

K = S[t] = S[3] = 3

Iterasi keempat, untuk nilai i = 3 dan j = 0 maka

i = (i + 1) mod 4

i = (3 + 1) mod 4

i = 0j = (j + S[i]) mod 4

j = (0 + S[0]) mod 4

j = (0 + 0) mod 4

j = 0

Menukarkan isi S[0] dan S[0] sehingga *array* S berbentuk :

Index	0	1	2	3
S	0	1	2	3

t = (S[0] + S[0]) mod4

t = (0+ 0) mod 4

t = 0

K = S[t] = S[0] = 0

Maka dari hasil pembangkitan kunci tersebut di dapat hasil kuncinya adalah

Iterasi pertama, untuk nilai i = j = 0, maka

K = S[t] = S[2] = 3

Iterasi kedua, untuk nilai i = 1 dan j = 1, maka

K = S[t] = S[0] = 1

Iterasi ketiga, untuk nilai i = 2 dan j = 0, maka

K = S[t] = S[3] = 3

Iterasi keempat, untuk nilai i = 3 dan j = 0, maka

K = S[t] = S[0] = 0

Maka hasil dari pembangkit kunci tersebut di dapat : 3130 lalu di konversikan ke desimal, ke simbol dan ke biner.

Keystream				
Desimal	3	1	3	0
Symbol	ETX	SOH	ETX	NUL
Biner	00000011	00000001	00000011	00000000

5. Proses enkripsinya *plaintext* di XOR-kan dengan kunci. Untuk *plaintext* DEDI dan kunci 3130 dari hasil pembangkitan kunci maka di XOR-kan dalam bentuk kode biner 8 *byte*.

Plaintext				
Desimal	68	69	68	73
Symbol	D	E	D	I
Biner	01000100	01000101	01000100	01001001

Keystream				
Desimal	3	1	3	0
Symbol	ETX	SOH	ETX	NUL
Biner	00000011	00000001	00000011	00000000
K ⊕ P (Biner)				
Keystream	00000011	00000001	00000011	00000000
Plaintext	01000100	01000101	01000100	01001001

K ⊕ P	01000111	01000100	01000111	01001001
Ciphertext (Simbol)	**G**	**D**	**G**	**I**
Ciphertext (Desimal)	**71**	**68**	**71**	**73**

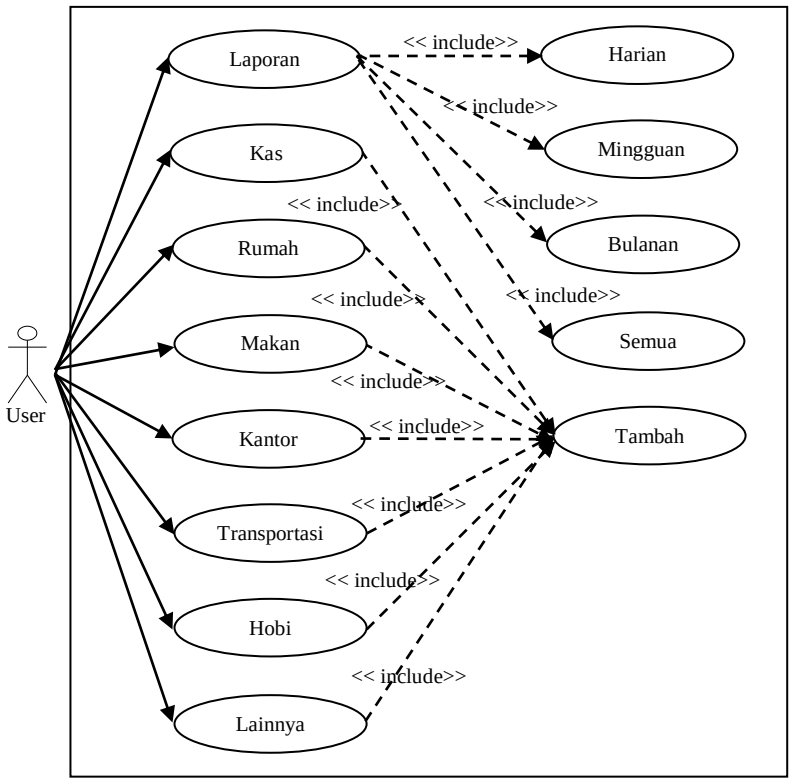
Maka didapat *ciphertext* hasil enkripsi implementasi algoritma RC4 mengunakan mode 4 byte yaitu GDGI. (Dedi Putra Oloan Simamora ; 2017 : 330-332)

III.5. Desain Sistem

Rancang bangun aplikasi keamanan data catatan keuangan harian pribadi menggunakan algoritma RC4 berbasis android dibangun dengan menggunakan perangkat lunak Android Studio. Perancangan sistem yang dirancang terdiri dari *use case diagram, activity diagram* dan *sequence diagram* serta desain antarmuka aplikasi dan penjelasan dari desain yang dirancang. Berikut adalah perancangannya :

III.5.1. *Use Case Diagram*

Use case mendiskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang akan dibuat. *Use case* digunakan untuk mengetahui fungsi yang ada didalam sistem informasi tersebut. Berikut adalah *use case diagram* dari sistem yang dirancang :



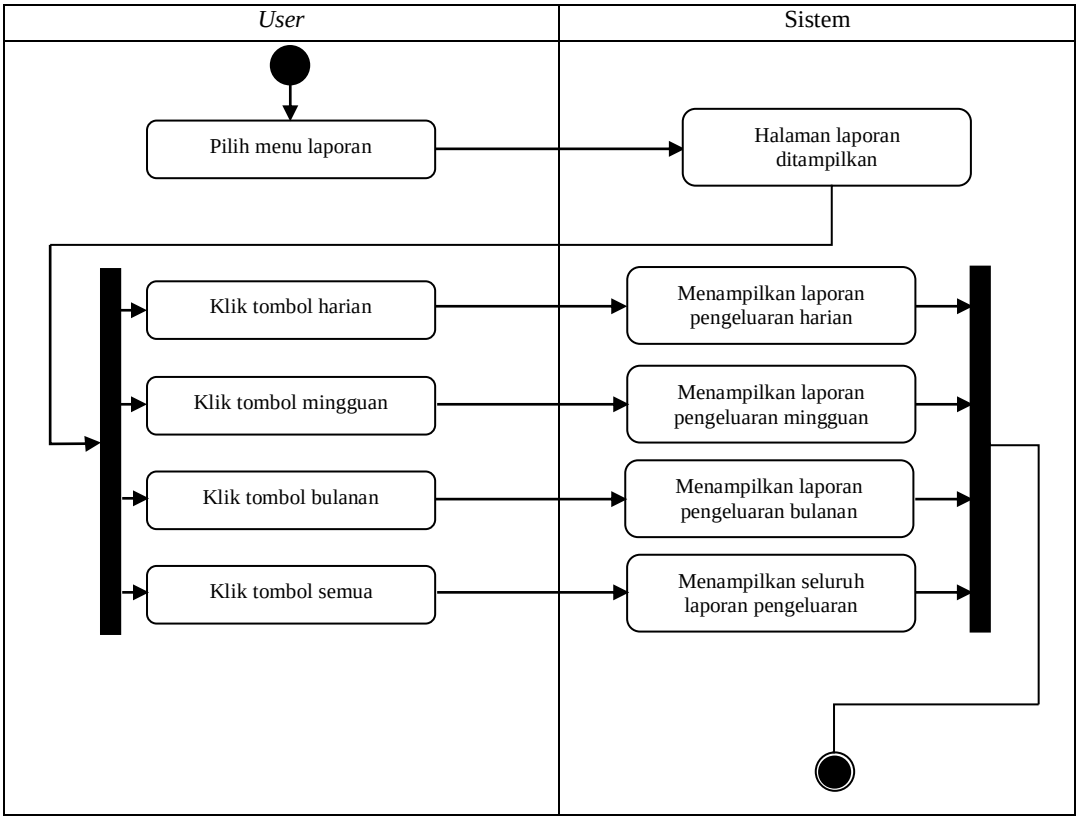
Gambar III.1. *Use Case Diagram*

III.5.2. *Activity Diagram*

Activity diagram menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir. *Activity diagram* yang terdapat pada aplikasi yaitu sebagai berikut :

III.5.2.1. *Activity Diagram* Laporan

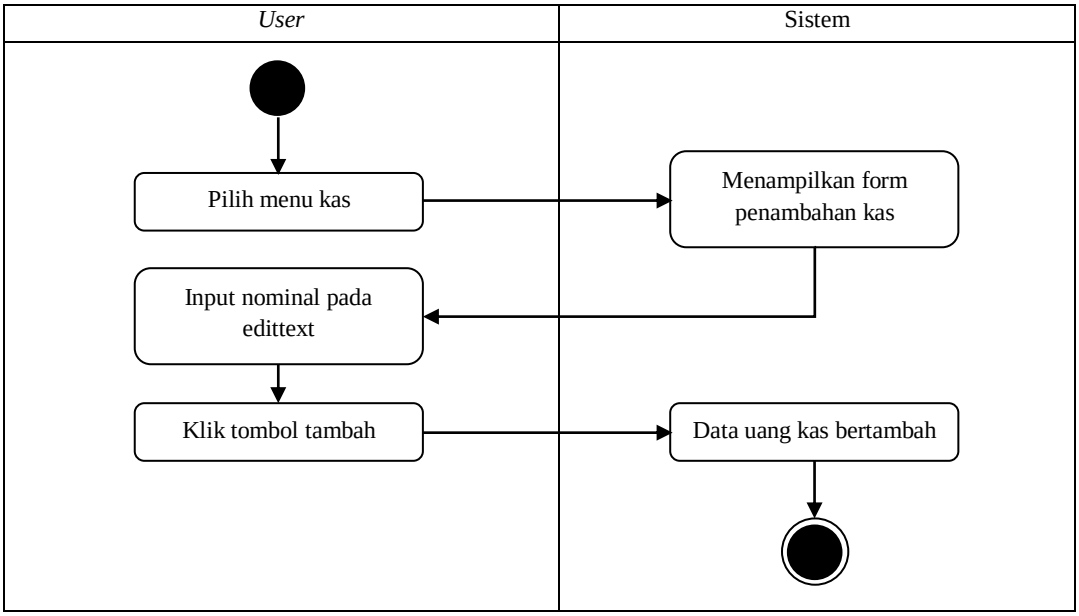
Activity diagram laporan menggambarkan alir aktifitas yang dilakukan saat akan melihat laporan pengeluaran keuangan pribadi. *Activity Diagram* laporan dapat dilihat pada gambar III.2.



Gambar III.2. *Activity Diagram* Laporan

III.5.2.2. *Activity Diagram* Kas

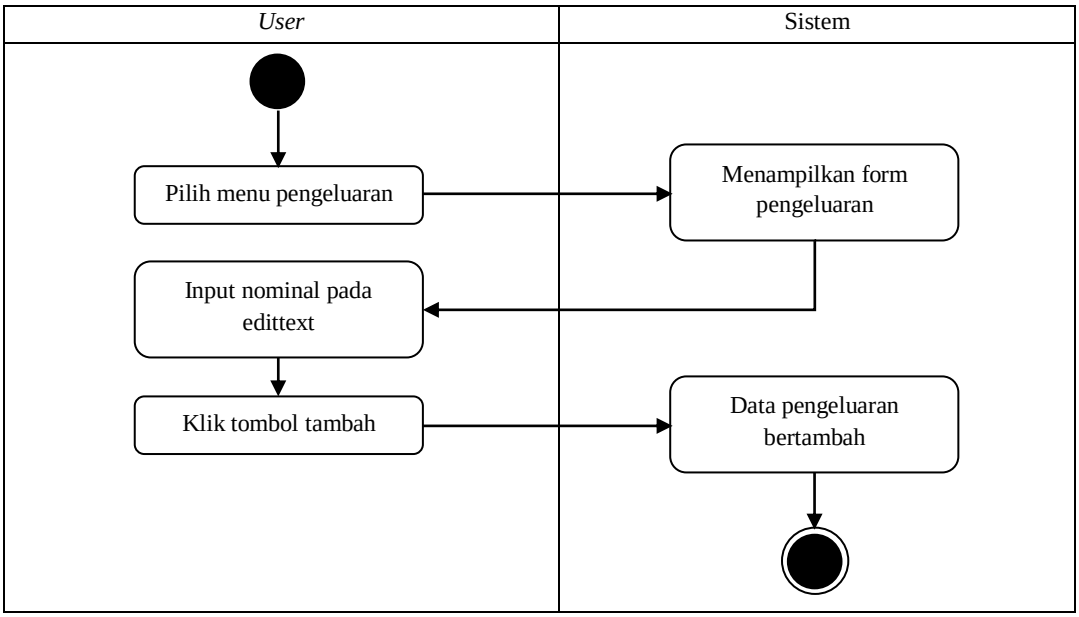
Activity diagram kas menggambarkan alir aktifitas yang dapat dilakukan pada saat memilih *menu* kas. *Menu* kas digunakan untuk menambahkan data uang pribadi. *Activity Diagram* kas dapat dilihat pada gambar III.3.



Gambar III.3. *Activity Diagram* Kas

III.5.2.3. *Activity Diagram* Jenis-Jenis Pengeluaran

Activity diagram jenis-jenis pengeluaran menggambarkan alir aktifitas yang dapat dilakukan pada saat memilih *menu* pengeluaran seperti rumah, makan, kantor, transportasi, hobi dan lainnya . *Menu* jenis-jenis pengeluaran digunakan untuk menambahkan daftar pengeluaran rumah, makan, kantor, transportasi, hobi dan lainnya. *Activity Diagram* jenis-jenis pengeluaran dapat dilihat pada gambar III.4



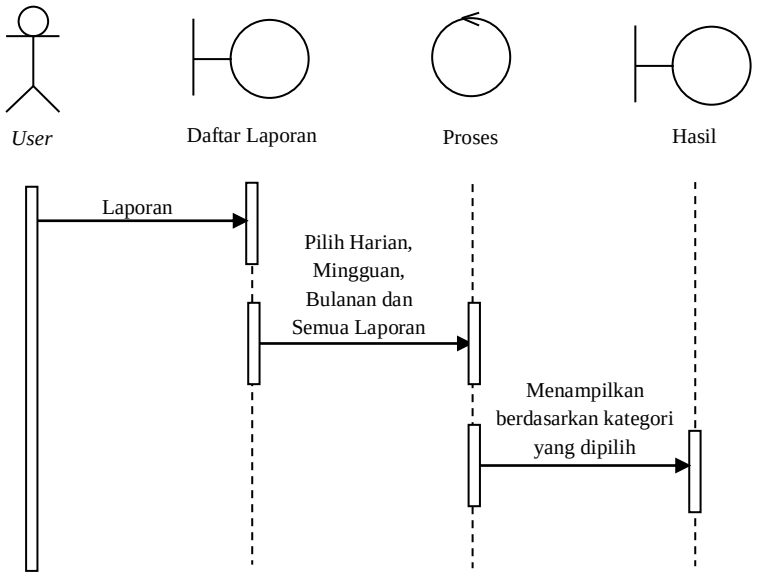
Gambar III.4. *Activity Diagram* Jenis-Jenis Pengeluaran

III.5.3. *Sequence Diagram*

Sequence diagram pada aplikasi yang akan dibuat yaitu : *Sequence diagram* laporan, kas, rumah, makan, kantor, transportasi, hobi dan lain-lain.

III.5.3.1. *Sequence Diagram* Laporan

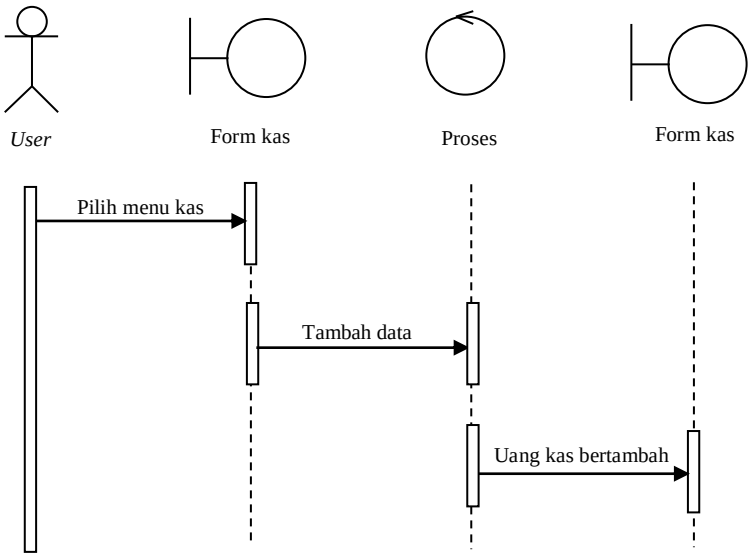
Sequence diagram laporan menggambarkan interaksi yang terjadi pada saat memilih *menu* laporan. *Sequence diagram* laporan ditunjukkan pada gambar III.10.



Gambar III.5 *Sequence Diagram* Laporan

III.5.3.2. *Sequence Diagram* Kas

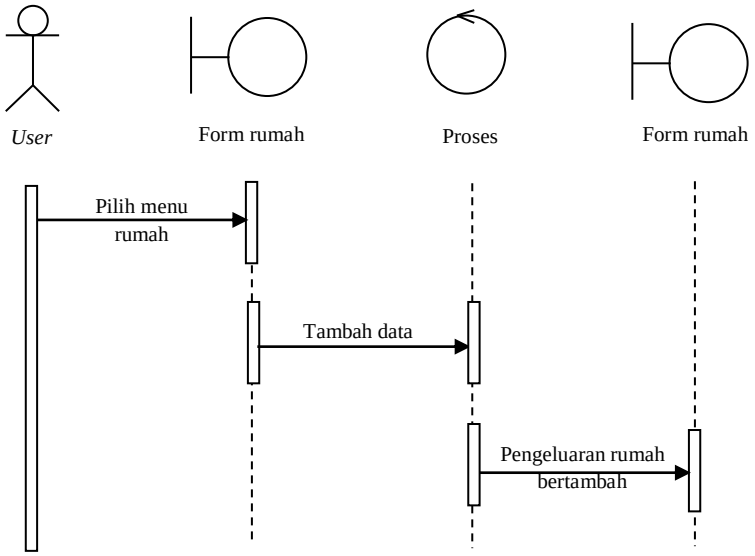
Sequence diagram kas menggambarkan interaksi saat akan menambahkan data uang kas. *Sequence diagram* kas ditunjukkan pada gambar III.11.



Gambar III.6. *Sequence Diagram* Kas

III.5.3.3. *Sequence Diagram* Rumah

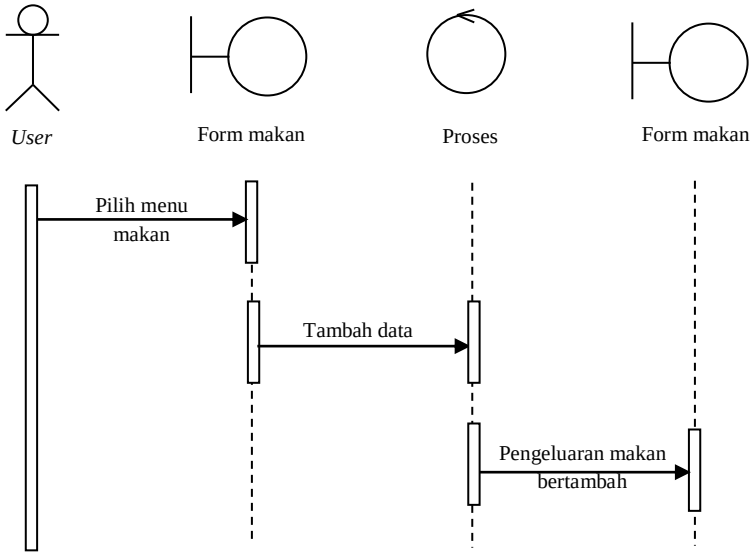
Sequence diagram rumah menggambarkan interaksi yang terjadi pada saat memilih *menu* pengeluaran rumah. *Sequence diagram* rumah ditunjukkan pada gambar III.12.



Gambar III.7. *Sequence Diagram* Rumah

III.5.3.4. *Sequence Diagram* Makan

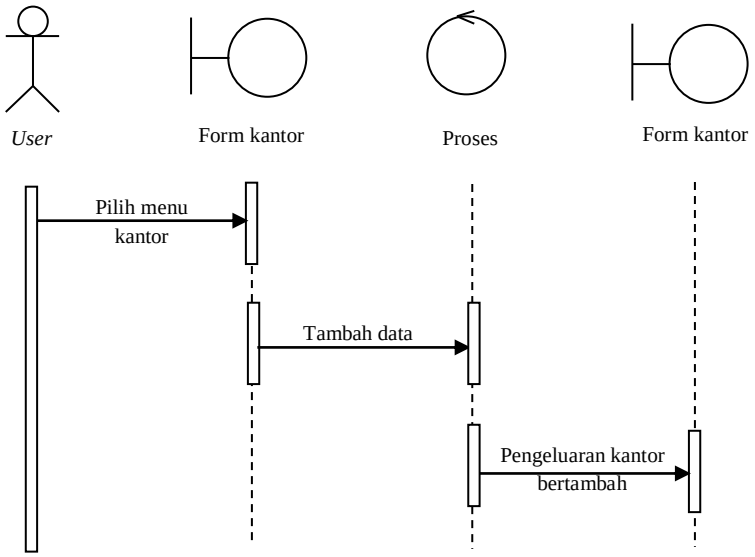
Sequence diagram makan menggambarkan interaksi yang terjadi pada saat memilih *menu* pengeluaran makan. *Sequence diagram* makan ditunjukkan pada gambar III.13.



Gambar III.8. *Sequence Diagram* Makan

III.5.3.5. *Sequence Diagram* Kantor

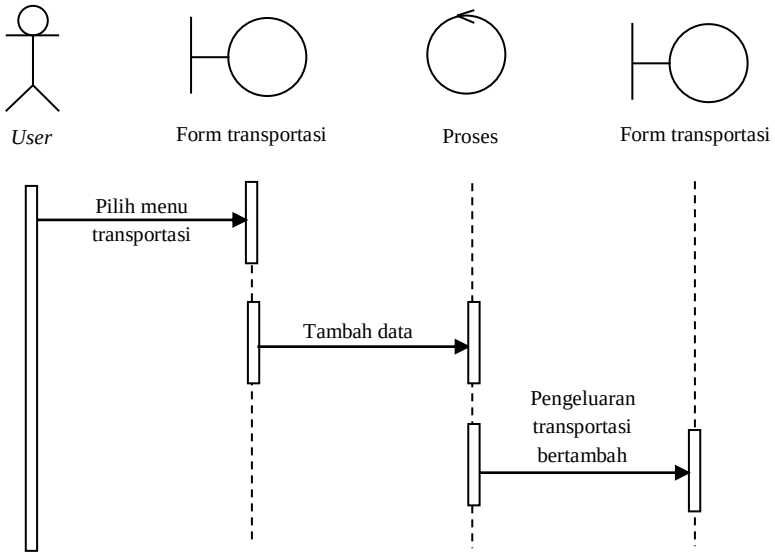
Sequence diagram kantor menggambarkan interaksi yang terjadi pada saat memilih *menu* pengeluaran kantor. *Sequence diagram* kantor ditunjukkan pada gambar III.14.



Gambar III.9. *Sequence Diagram* Kantor

III.5.3.6. *Sequence Diagram* Transportasi

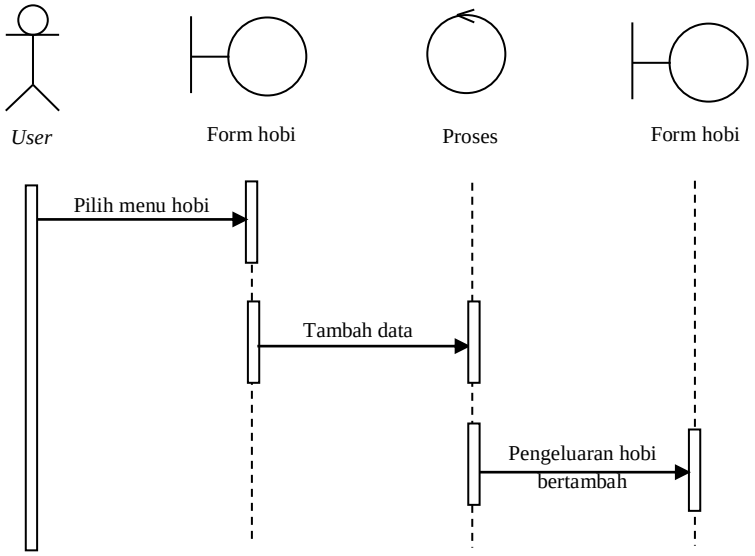
Sequence diagram transportasi menggambarkan interaksi yang terjadi pada saat memilih *menu* pengeluaran transportasi. *Sequence diagram* transportasi ditunjukkan pada gambar III.15.



Gambar III.10. *Sequence Diagram* Transportasi

III.5.3.7 *Sequence Diagram* Hobi

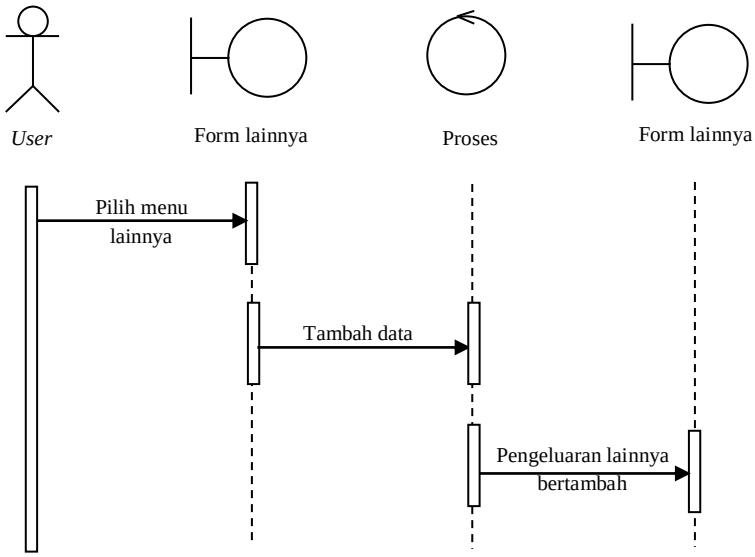
Sequence diagram hobi menggambarkan interaksi yang terjadi pada saat memilih *menu* pengeluaran berdasarkan hobi. *Sequence diagram* hobi ditunjukkan pada gambar III.16.



Gambar III.11. *Sequence Diagram* Hobi

III.5.3.8. *Sequence Diagram* Lainnya

Sequence diagram lain-lain menggambarkan interaksi yang terjadi pada saat memilih *menu* pengeluaran lainnya. *Sequence diagram* lainnya ditunjukkan pada gambar III.17.

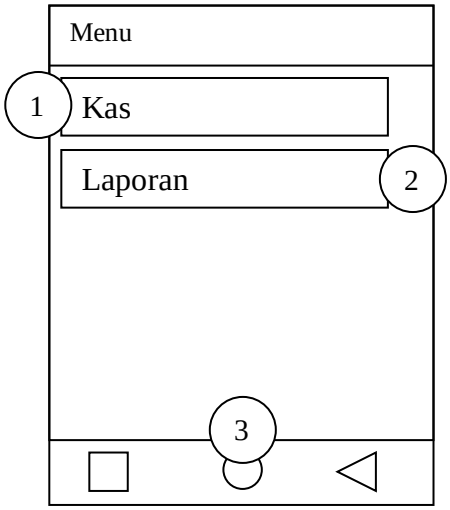


Gambar III.12. *Sequence Diagram* Lainnya

III.6. Desain *User Interface*

Antarmuka peamakai (*user interface*) adalah tampilan program yang dapat dilihat atau dipersepsikan oleh pengguna dan perintah-perintah atau mekanisme yang digunakan pemakai untuk mengendalikan operasi dan memasukkan data. Berikut ini merupakan desain antarmuka rancang bangun aplikasi keamanan data catatan keuangan harian pribadi menggunakan algoritma RC4 berbasis android, yaitu :

1. Desain *Navigation Drawer*

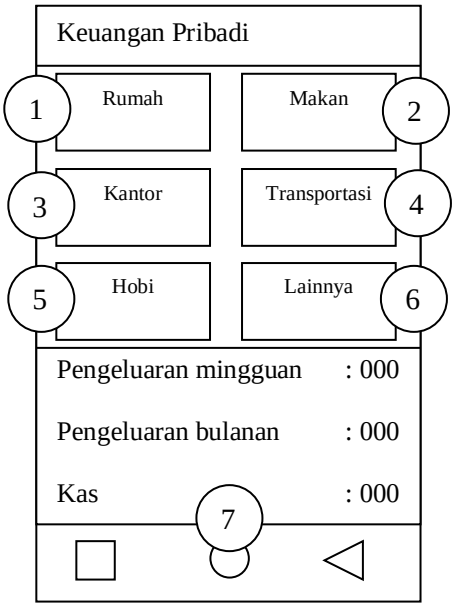


Gambar III.13. Desain *Navigation Drawer*

Pada aplikasi pencatat keuangan harian pribadi terdapat navigation drawer yang menampung menu kas dan laporan. Adapun keterangannya sebagai berikut :

1) Tombol untuk menampilkan *form* kas.
2) Tombol untuk menampilkan laporan catatan keuangan pribadi.
3) Tombol *menu smartphone* android.

2. Desain Halaman Utama

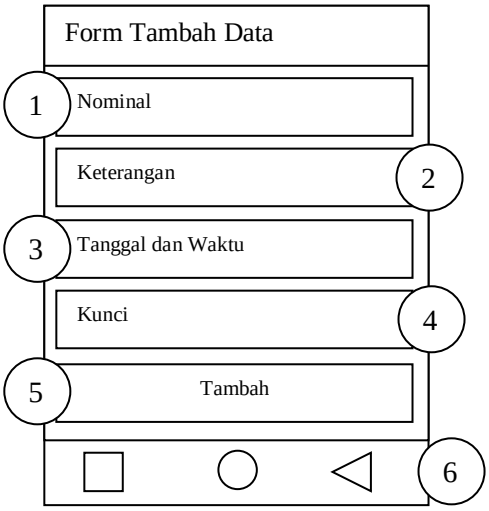


Gambar III.14. Desain Halaman Utama

Merupakan tampilan halaman yang muncul saat pertama aplikasi dijalankan. Adapun keterangannya sebagai berikut :

1) Tombol untuk menampilkan *form* pengeluaran rumah.
2) Tombol untuk menampilkan *form* pengeluaran makan.
3) Tombol untuk menampilkan *form* pengeluaran kantor.
4) Tombol untuk menampilkan *form* pengeluaran transportasi.
5) Tombol untuk menampilkan *form* pengeluaran hobi.
6) Tombol untuk menampilkan *form* pengeluaran lainnya.
7) Tombol *menu smartphone* android.

3. Desain Form Tambah Data

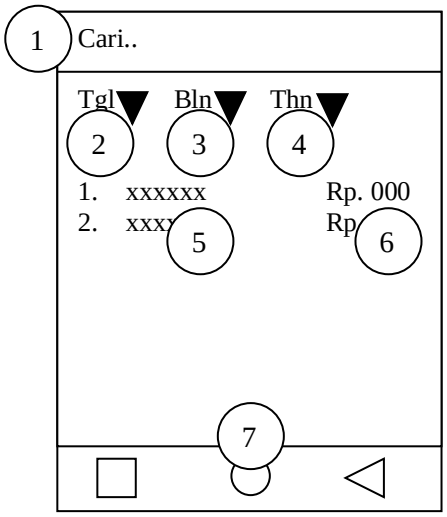


Gambar III.15. Desain *Form* Tambah Data

Form tambah data digunakan untuk menambahkan data uang kas maupun data pengeluaran keuangan pribadi. Adapun keterangannya sebagai berikut :

1) *Edittext* untuk input nominal uang masuk pada saat memilih menu kas dan nominal uang keluar pada saat memilih menu pengeluaran seperti rumah, makan, kantor, transportasi, hobi dan lainnya.
2) *Edittext* untuk *input* keterangan dari uang yang ditambahkan maupun keluar.
3) *Edittext* untuk menampilkan tanggal dan waktu yang secara otomatis tampil berdasarkan tanggal dan waktu pada smartphone yang digunakan.
4) *Edittext* untuk input kunci yang digunakan untuk menyandikan catatan keuangan pribadi.
5) Tombol untuk menambahkan data catatan keuangan pribadi kedalam *database*.
6) Tombol *menu smartphone* android.

4. Desain Halaman Laporan Pengeluaran



Gambar III.16. Desain Halaman Laporan Pengeluaran

Merupakan desain tampilan halaman laporan pengeluaran dari aplikasi catatan keuangan pribadi. Adapun keterangannya sebagai berikut :

1) *Edittext* untuk mencari pengeluaran berdasarkan keterangan.
2) *Dropdown* untuk memilih tanggal pengeluaran.
3) *Dropdown* untuk memilih bulan pengeluaran.
4) *Dropdown* untuk memilih tahun pengeluaran.
5) Daftar keterangan pengeluaran berupa nama pengeluaran dan tanggal.
6) Daftar nominal yang digunakan pada pengeluaran.
7) Tombol *menu smartphone* android.