BAB III

ANALISIS DAN PERANCANGAN

III.1. Analisis Sistem yang Berjalan

Analisa sistem pada yang berjalan bertujuan untuk mengidentifikasi serta melakukan evaluasi terhadap sistem aplikasi Android pada pemilihan dikarenakan belum adanya aplikasi berbasis Android untuk pengamanan pada *cloud storage dropbox* perangkat smartphone menjadi multiguna yang dapat membantu kinerja pengamanan menjadi lebih efektif dan efesien. Analisis dilakukan agar dapat menemukan masalah-masalah dalam melakukan percakapan yang diperlukan yang diberikan oleh pihak pengguna. Adapun analisis sistem ini meliputi *input,* proses dan *output* yang dijabarkan sebagai berikut :

III.1.1. Analisis *Input*

Analisis *input* yang ada pada sistem yang lama adalah data pengamanan *cloud storage dropbox*, yang akan disampaikan pada penggunaan sistem perangkat smartphone yang telah ada.

III.1.2. Analisis *Process*

Proses yang terjadi pada sistem yang dijelaskan dengan FOD (*Flow Of Document*) Penjelasan FOD (*Flow Of Document*) sebagai berikut :

1. Tampilkan pengamanan *cloud storage dropbox* dengan kunci menggunakan algoritma Elgamal.

2. Kemudian mulai pengamanan *cloud storage dropbox*.
3. *Log cloud storage dropbox* dikelolah oleh developer di dalam aplikasi.

III.1.3. Analisis *Output*

Output yang dihasilkan dari aplikasi pengamanan *cloud storage dropbox* adalah untuk pengamanan email *cloud storage dropbox* oleh Elgamal.

III.2. Evaluasi Sistem yang Berjalan

Sistem yang sedang berjalan memiliki beberapa kelemahan yang dijabarkan sebagai berikut:

1. Perlu dilakukannya rancangan aplikasi pengamanan *cloud storage dropbox* yang akurat sehingga dapat membantu pengguna smartphone.
2. Perlunya diciptakan suatu aplikasi yang dapat memudahkan pihak pengguna dalam melakukan pengamanan *cloud storage dropbox.*
3. Belum adanya aplikasi berbasis Android untuk pengamanan *cloud storage dropbox* pada sistem smartphone.
4. Sistem yang sedang berjalan pada saat ini masih menggunakan sistem biasa dimana setiap *cloud storage dropbox* yang ingin melakukan pengamanan yang cukup akurat.

Sistem yang sedang berjalan memiliki beberapa kelebihan yang dijabarkan sebagai berikut:

1. Sistem dapat memudahkan pengaman *cloud storage dropbox* smartphone.
2. Informasi yang disajikan pada sistem cukup akurat dan efektif.

III.2.1. Penerapan Metode

Studi Kasus:

Misalkan terdapat String “Nugrah Gulo” akan dienkripsi dan didekripsi menggunakan kunci p=277 g=7 dan x=113.

Penyelesaian:
p= 277
g= 7
x= 113
y = g^x % p
y = 7^113 % 277
y = 25
Kunci Public : 277,7,25
Kunci Private : 113

Syarat k adalah $1 \leq k \leq p - 2$

Pesan	ASCII	Random-k
N	78	259
u	117	264
g	103	199
r	114	33
a	97	48
h	104	16
[ ]	32	204
G	71	149
u	117	87
l	108	97
o	111	253

Tahap Enkripsi:
gamma (γ) = g^k % p ……..... (1)
delta (δ) = (y^k)m % p ……..... (2)

k0 = 259 m0 = 78
gamma(γ)-0 = 7^259 % 277 = 249
delta(δ)-0 = 25^259.78 % 277 = 18

k1 = 264 m1 = 117
gamma(γ)-1 = 7^264 % 277 = 27
delta(δ)-1 = 25^264.117 % 277 = 7

k2 = 199 m2 = 103
gamma(γ)-2 = 7^199 % 277 = 268
delta(δ)-2 = 25^199.103 % 277 = 118

k3 = 33 m3 = 114
gamma(γ)-3 = 7^33 % 277 = 261
delta(δ)-3 = 25^33.114 % 277 = 45
k4 = 48 m4 = 97
gamma(γ)-4 = 7^48 % 277 = 84
delta(δ)-4 = 25^48.97 % 277 = 24

k5 = 16 m5 = 104
gamma(γ)-5 = 7^16 % 277 = 171
delta(δ)-5 = 25^16.104 % 277 = 199

k6 = 204 m6 = 32
gamma(γ)-6 = 7^204 % 277 = 256
delta(δ)-6 = 25^204.32 % 277 = 61

k7 = 149 m7 = 71
gamma(γ)-7 = 7^149 % 277 = 192
delta(δ)-7 = 25^149.71 % 277 = 220

k8 = 87 m8 = 117
gamma(γ)-8 = 7^87 % 277 = 208
delta(δ)-8 = 25^87.117 % 277 = 67

k9 = 97 m9 = 108
gamma(γ)-9 = 7^97 % 277 = 86
delta(δ)-9 = 25^97.108 % 277 = 48

k10 = 253 m10 = 111
gamma(γ)-10 = 7^253 % 277 = 117
delta(δ)-10 = 25^253.111 % 277 = 143

Chiper : 249 18 27 7 268 118 261 45 84 24 171 199 256 61 192 220 208 67 86 48 117 143

Tahap Dekripsi:

m = δ. γ^(p-1-x) % p …… (3)

Gamma	Delta	m (ASCII)	Huruf
249	18	m0 = 18.249^(277-1-113) % 277 = 78	N
27	7	m1 = 7.27^(277-1-113) % 277 = 117	u
268	118	m2 = 118.268^(277-1-113) % 277 = 103	g
261	45	m3 = 45.261^(277-1-113) % 277 = 114	r
84	24	m4 = 24.84^(277-1-113) % 277 = 97	a
171	199	m5 = 199.171^(277-1-113) % 277 = 104	h

256	61	m6 = 61.256^(277-1-113) % 277 = 32	[ ]
192	220	m7 = 220.192^(277-1-113) % 277 = 71	G
208	67	m8 = 67.208^(277-1-113) % 277 = 117	u
86	48	m9 = 48.86^(277-1-113) % 277 = 108	l
117	143	m10 = 143.117^(277-1-113) % 277 = 111	o

Pesan : Nugrah Gulo

III.3. Desain Sistem

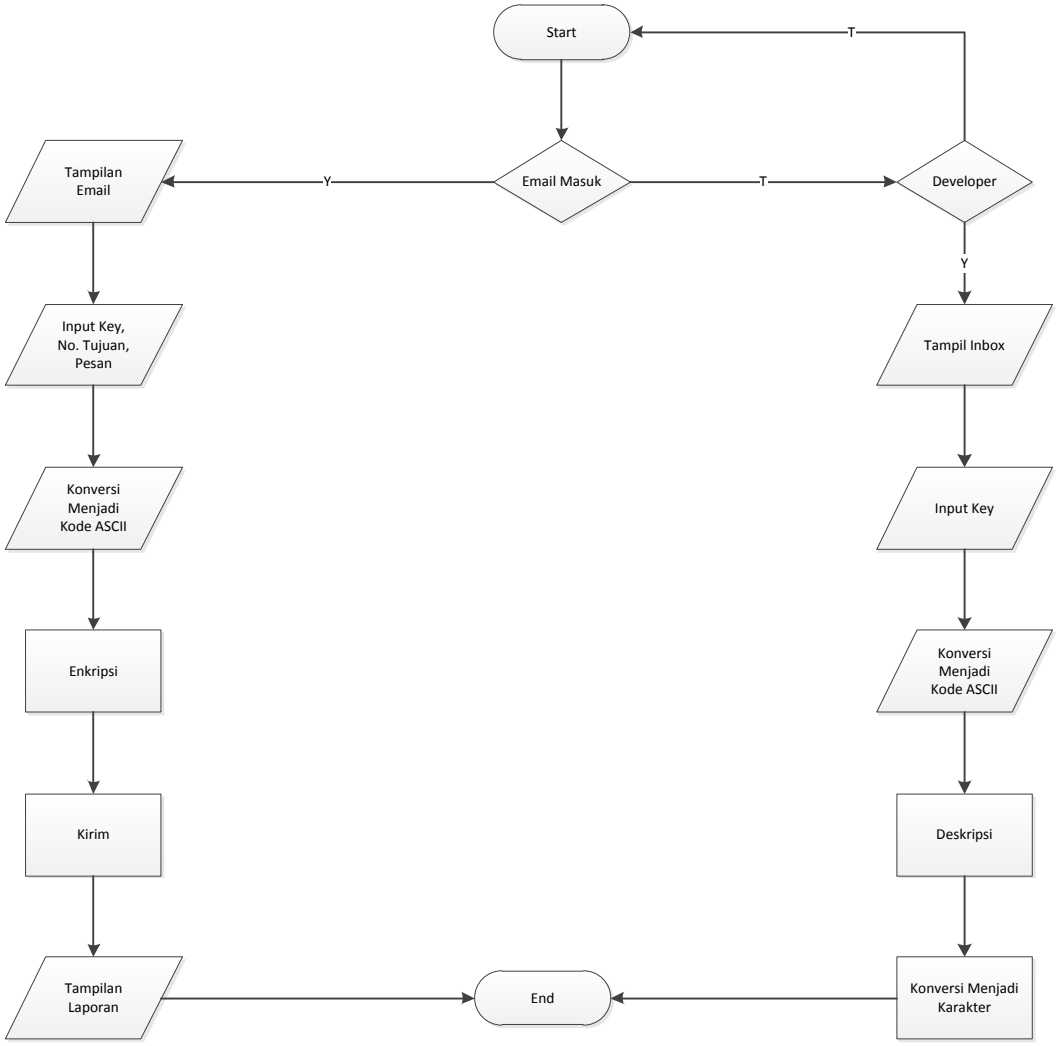
Desain sistem pada penelitian ini dibagi menjadi dua desain, yaitu desain sistem secara global untuk penggambaran model sistem secara garis besar dan desain sistem secara detail untuk membantu dalam pembuatan sistem.

III.3.1. Desain Sistem Secara Global

Desain sistem secara global menggunakan bahasa pemodelan UML yang terdiri dari *flowchart, Usecase Diagram*, *Acitvity Diagram*, dan *Class Diagram*.

III.3.1.1. *Flowchart*

Rancangan ini disusun dengan tujuan mendesain dan merepresentasikan program. Fungsinya adalah untuk memudahkan pengamanan *cloud storage dropbox* yang akan dibuat pada gambar III.1 berikut.

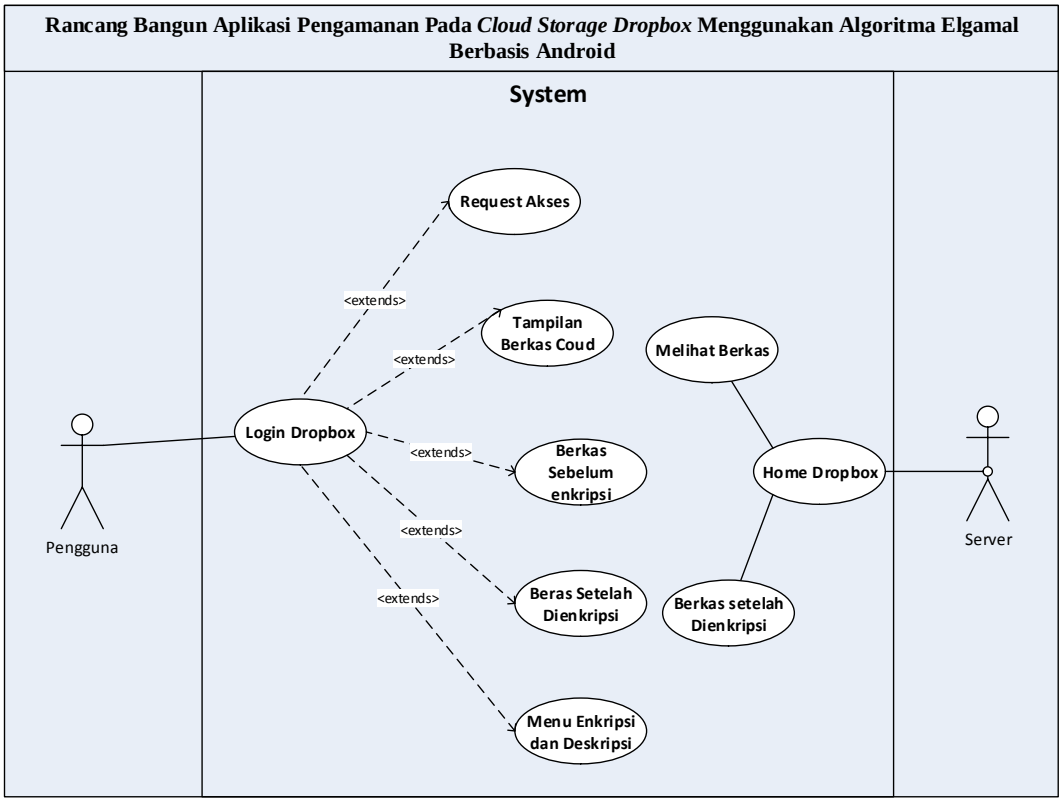


Gambar III.1. *Flowchart*

Tampilan utama aplikasi dari Elgamal untuk mengirim email dan layar untuk menerima email.

III.3.1.2. *Usecase* Diagram

Secara garis besar, bisnis proses sistem yang akan dirancang digambarkan dengan *usecase* diagram yang terdapat pada Gambar III.2 :



Gambar III.2 *Use Case* Diagram Pengaman *Cloud storage dropbox*

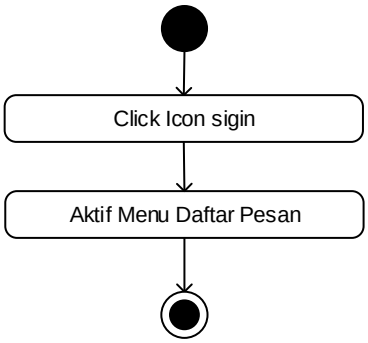
1. Pengguna melakukan login
2. Pengguna merequest akses dropbox untuk menkripsi berkas
3. Setelah memilih berkas pada cloud pengguna akan melakukan enkripsi berkas.
4. Untuk masuk kedalam menu enkripsi dan dekripsi berkas.
5. Server masuk kedalam situs dropbox.
6. Server akan melihat berkas dan berkas akan di enkripsi.

III.3.1.3 *Activity* Diagram

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

1. Activity Diagram Tampilan Berkas cloud

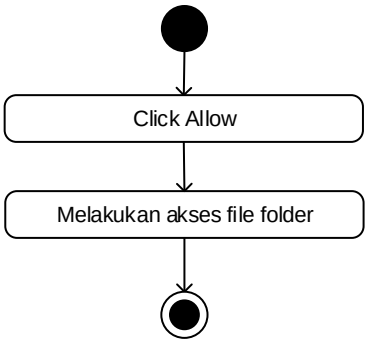
Aktifitas untuk melakukan tampilan berkas cloud untuk dapat masuk kedalam sistem terlihat seperti pada gambar III.3 berikut :



Gambar III.3. *Activity* Diagram Berkas cloud

2. *Activity* Diagram Dlock RC6

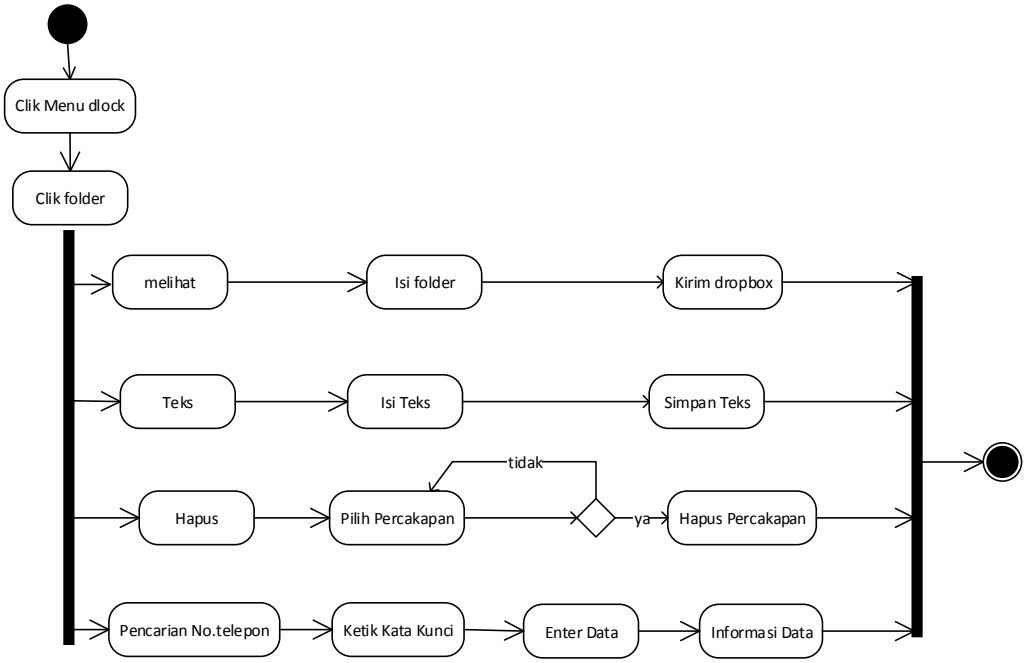
Aktifitas untuk melakukan allow baru terhadap menu menulis email terlihat seperti pada gambar III.4 berikut :



Gambar III.4. *Activity* Diagram Dlock RC6

3. *Activity* Diagram Daftar Dlock

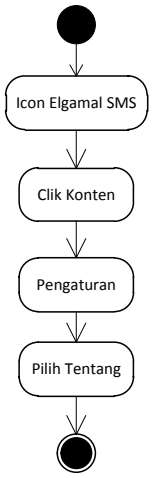
Aktifitas untuk melakukan pengaturan tampilan untuk mengatur tema tampilan terlihat seperti pada gambar III.5 berikut :



Gambar III.5. *Activity* Diagram Daftar Dlock

4. *Activity* Diagram Menu Tentang Pengaturan

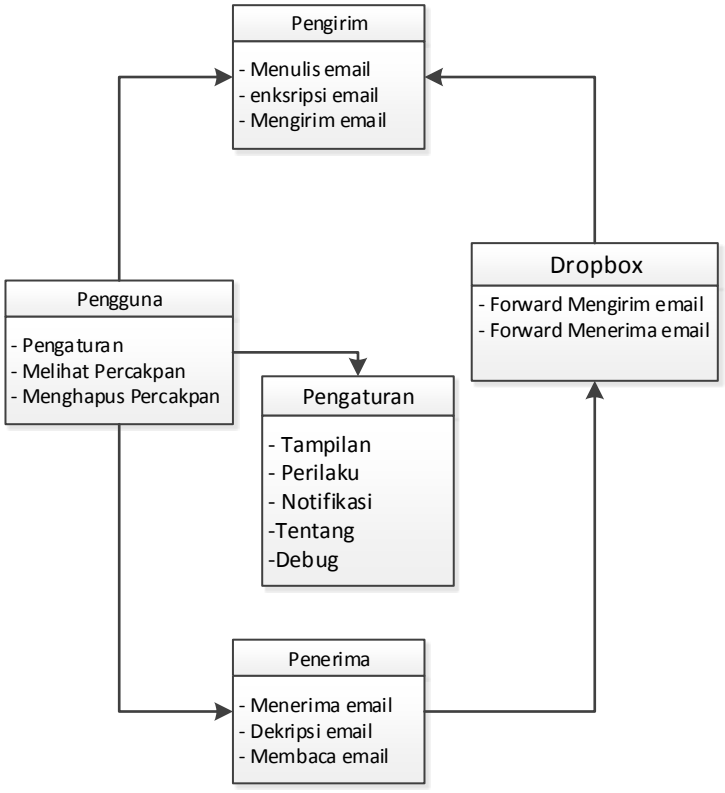
Aktifitas untuk melakukan menu tentang pengaturan terlihat seperti pada gambar III.6 berikut :



Gambar III.6. *Activity* Diagram Menu Tentang Pengaturan

III.3.1.4 *Class* Diagram

Rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat pada gambar III.7 :



Gambar III.7 *Class Diagram* Sistem Pengamanan Cloud Storage Dropbox

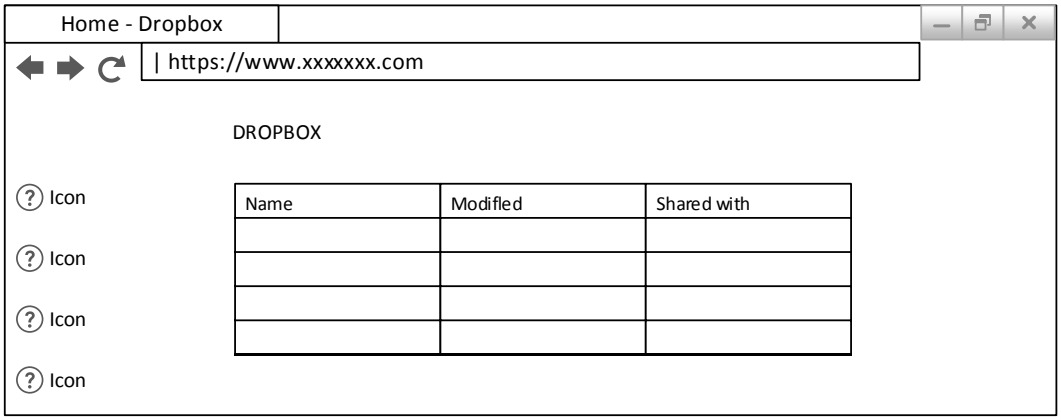
1. Pengirim bisa melakukan menulis email,enksripsi email, dan mengirim email.
2. Operator selular bisa melakukan forward pengiriman email, dan forward penerimaan email.
3. Penerima email bisa melakukan menerima email, deskripsi email, dan membaca email.
4. Pengguna akan melakukan pengaturan email pada Elgamal.

III.3.2. Desain Interface

Berikut ini adalah rancangan atau desain *input* sebagai antarmuka pengguna:

1. Desain Sistem Web Dropbox

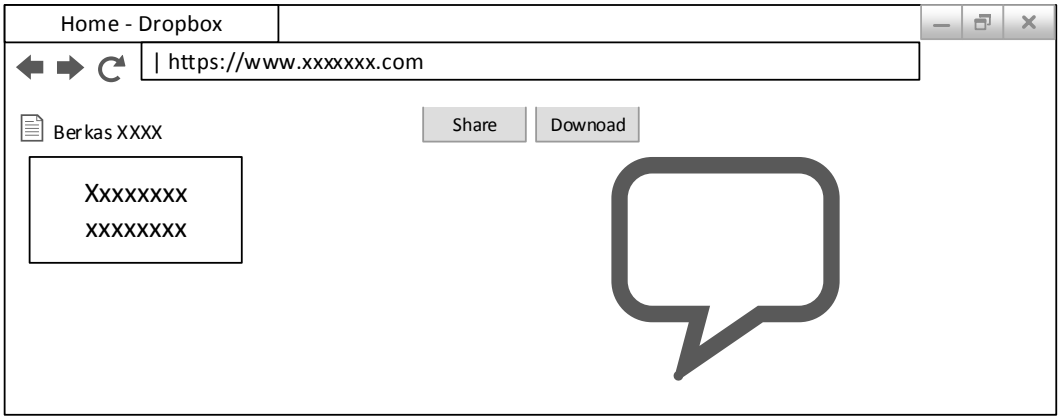
Desian yang dirancang akan menampilkan web situs dropbox untuk memilih berkas yang terenkripsi terlihat pada gambar III.8 Berikut :



Gambar III.8. Desain Tampilan Web Dropbox

2. Desain Sistem Berkas Setelah Dienkripsi

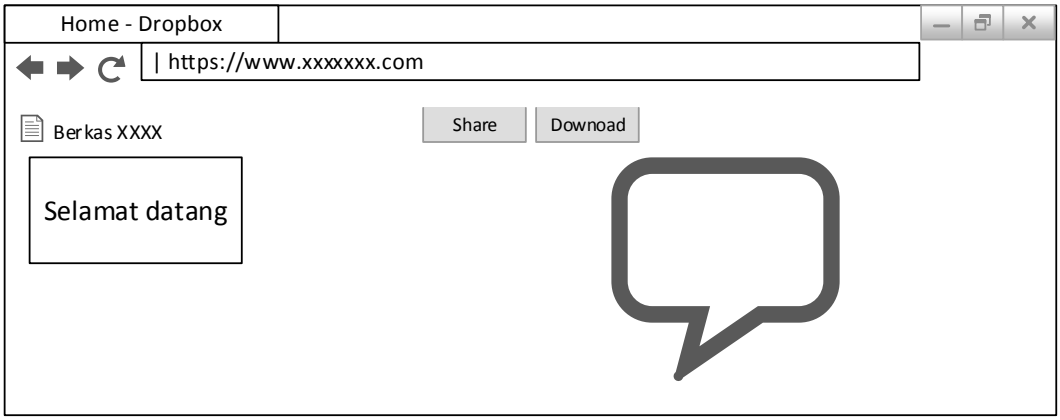
Desian yang dirancang akan menampilkan berkas untuk dienkripsi yang terenkripsi terlihat pada gambar III.9 Berikut :



Gambar III.9. Desain Tampilan Berkas Setelah Dienkripsi

3. Desain Sistem Isi Berkas

Desian yang dirancang akan menampilkan isi berkas yang terenkripsi terlihat pada gambar III.10 Berikut :



Gambar III.10. Desain Tampilan Isi Berkas

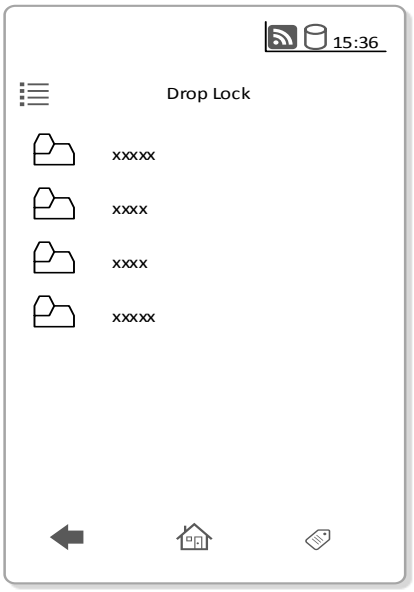
4. Desain Tampilan Login

Desain yang dirancang untuk melakukan login masuk dropbox untuk melakukannya terlebih dahulu masukan username dan password terlihat pada gambar III.11 Berikut :

Gambar III.11. Desain Tampilan Sign In

5. Desain Tampilan Berkas Cloud

Desain yang dirancang untuk melihat berkas *cloud* untuk memulai email terlihat seperti pada gambar III.12 berikut :



Gambar III.12. Desain Tampilan Berkas *Cloud*

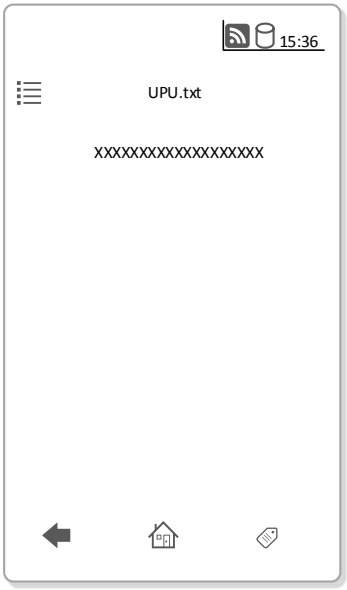
6. Desain Tampilan Berkas Sebelum Enkripsi

Desain tampilan berkas sebelum enkripsi yang dirancang untuk melakukan kirim email dan mengisi no.pengirim terlihat seperti pada gambar III.13 berikut :

Gambar III.13. Desain Tampilan Berkas sebelum enkripsi

7. Desain Tampilan Berkas Setelah Dienkripsi

Desain tampilan berkas setelah dienkripsi yang dirancang untuk melakukan kirim email dan mengisi no.pengirim terlihat seperti pada gambar III.14 berikut :



Gambar III.14. Desain Tampilan Berkas Setelah Dienkripsi

8. Desain Tampilan Menu Tentang Program

Desain tampilan menu tentang program yang dirancang untuk melakukan pengaturan pengiriman terlihat seperti pada gambar III.15 berikut :

Gambar III.15. Desain Tampilan Menu Tentang Program