

BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisis Masalah

Rentannya keamanan data pada perusahaan merupakan salah satu aspek penting dari sebuah sistem informasi. Sangat pentingnya nilai dari sebuah informasi menyebabkan banyaknya pihak lain yang ingin mencuri informasi tersebut. Jika informasi tersebut jatuh ke pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Dalam hal ini, penulis mengambil contoh dalam sebuah data konsumen pada perusahaan PT. Coca Cola dimana masalah pengolahan data konsumen merupakan sesuatu yang sangat penting sehingga dibutuhkan suatu sistem informasi pengolahan data konsumen yang dapat meningkatkan keamanan dalam sebuah perusahaan.

III.2. Pemecahan Masalah

Untuk mengatasi masalah dalam hal pengaman data konsumen dalam suatu perusahaan ataupun instansi terkait, penulis mengambil satu langkah metode dalam melakukan pengamanan data yaitu metode algoritma *elgmal*. Metode *Elgamal* merupakan metode dalam kriptografi yang menggunakan algoritma asimetris dan memiliki 2 kunci utama, yakni kunci *public* dan kunci *private*. Kunci yang didistribusikan dikenal dengan istilah kunci publik, jika kunci *public* ini diketahui

oleh orang lain yang tidak berhak berkepentingan, maka data yang dikirim akan tetap aman. Untuk kunci *private* adalah kunci yang tetap disimpan oleh pihak-pihak yang berhak. Pada algoritma *Elgamal* digunakan kunci *private* dan kunci *public* dalam melakukan proses kriptografinya, metode ini juga memiliki pengamanan ganda sehingga susah untuk ditembus.

III.3. Penerapan Elgamal

Langkah-langkah metode elgamal untuk enkrip dapat dilihat sebagai berikut :

1. Algoritma Pembentukan Kunci Kriptografi

Input :

- a. Sembarang bilangan prima, p .
- b. Sembarang bilangan acak g .
- c. Sembarang bilangan acak x .

Proses :

Hitung nilai y , dengan persamaan :

=

Output :

- a. Keluaran berupa bilangan y .
- b. Kunci publik (y, g, p) .
- c. Kunci *private* (x, p) .

2. Algoritma Enkripsi

Input :

- a. Susun *plaintext* menjadi blok-blok m_1, m_2 , dst.
- b. Tentukan bilangan acak k sepanjang jumlah *plaintext*.

Proses :

Setiap blok m di enkripsi dengan persamaan :

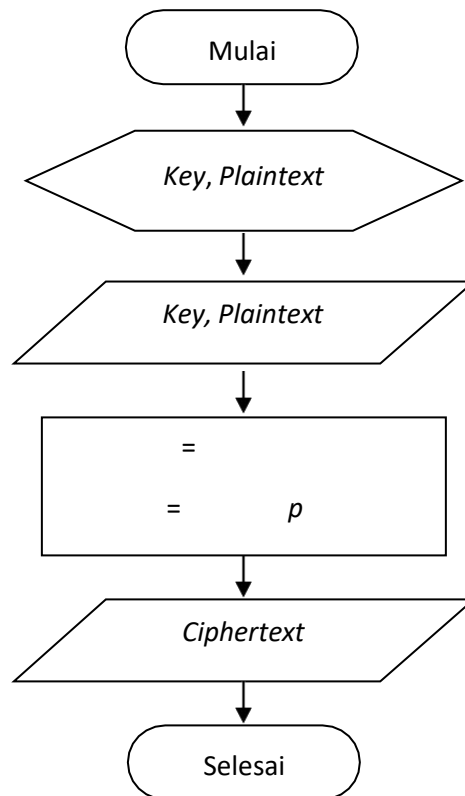
=

= p

Output :

- a. Pasangan a dan b adalah *ciphertext* untuk blok pesan m .
- b. Penyajian *ciphertext* seperti berikut : $a_1 b_1 a_2 b_2$ dst.

Flowchart enkripsi metode Elgamal dapat dilihat sebagai berikut :



Gambar III.5. Flowchart Enkripsi Metode Elgamal

Keterangan :

1. Mulai

Merupakan simbol untuk memulai sebuah *flowchart*.

2. Key, Plaintext

Merupakan simbol deklarasi atau pengenalan input data.

3. Key

Merupakan input data berupa kunci untuk metode elgamal.

4. Plaintext

Merupakan pesan asli dan pada penelitian ini pesan asli berupa teks di dalam *database*.

5. =

$$= p$$

Merupakan rumus untuk enkripsi pada algoritma elgamal yang diletakkan pada simbol proses *flowchart*. Hasil enkripsi memiliki 2 karakter pada setiap proses yaitu karakter dari rumus a (alpha) dan b (beta) kemudian hasil enkripsi a dan b disusun dan digabung secara berdampingan sehingga membentuk kalimat.

6. Ciphertext

Merupakan hasil enkripsi algoritma elgamal yang diletakkan pada simbol *output flowchart*.

7. Selesai

Merupakan simbol akhir sebuah proses pada *flowchart*.

Contoh :

a. Plaintext

Plaintext yang akan dienkripsi adalah admin.

b. Ubah Plaintext Menjadi Kode ASCII Dan Susun Menjadi Blok-Blok Nilai m.

$a = 97$

$d = 100$

$m = 109$

$i = 105$

$n = 110$

c. Menghasilkan Nilai m.

$m1 = 97$

$m2 = 100$

$m3 = 109$

$m4 = 105$

$m5 = 110$

d. Tentukan Bilangan Acak k Sepanjang Jumlah Plaintext.

$k1 = 11$

$k2 = 13$

$k3 = 17$

$k4 = 19$

$k5 = 23$

e. Menghasilkan Bilangan Acak k.

Bilangan acak k yang telah dihasilkan akan digunakan sebagai pemangkat pesan.

f. Enkripsikan Setiap Blok m.

a. Enkripsi Nilai Gamma :

$$\gamma = g^k \bmod p \dots\dots\dots (1)$$

$$\gamma_1 = 13^{11} \bmod 127 = 82 = R$$

$$\gamma_2 = 13^{13} \bmod 127 = 15 =$$

$$\gamma_3 = 13^{17} \bmod 127 = 44 = b$$

$$\gamma_4 = 13^{19} \bmod 127 = 70 =$$

$$\gamma_5 = 13^{23} \bmod 127 = 36 = \$$$

b. Enkripsi Nilai Delta :

$$\delta = y^k \cdot m \bmod p \dots\dots\dots (2)$$

$$\delta_1 = 44^{11} \cdot 97 \bmod 127 = 90 = Z$$

$$\delta_2 = 44^{13} \cdot 100 \bmod 127 = 98 =$$

$$\delta_3 = 44^{17} \cdot 109 \bmod 127 = 5 = ,$$

$$\delta_4 = 44^{19} \cdot 105 \bmod 127 = 28 = F$$

$$\delta_5 = 44^{23} \cdot 110 \bmod 127 = 126 = \sim$$

g. Menghasilkan *Ciphertext*.

Satukan nilai gamma dan nilai delta sehingga menjadi *ciphertext*.

Ciphertext : RZb, F \$~

3. Algoritma Dekripsi

Input :

Kunci *private* (x, p).

Proses :

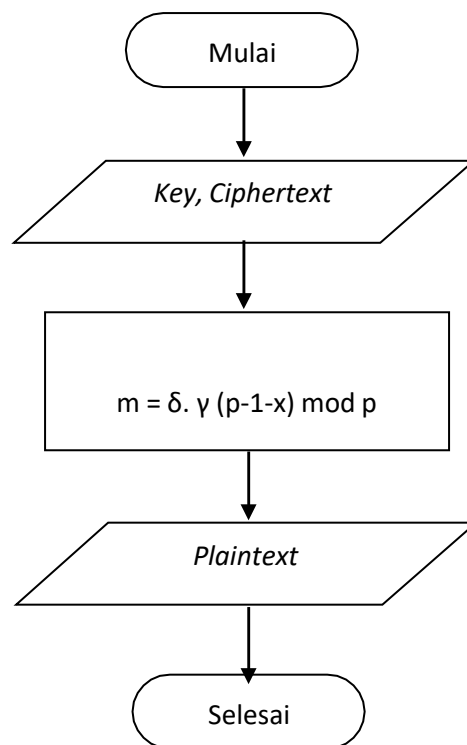
Konversi *ciphertext* ke dalam *plaintext*, dengan persamaan :

Output :

- a. *Plaintext* yang dihasilkan berupa m dalam desimal ASCII.
- b. Lakukan penyusunan pesan m yang dihasilkan dan lakukan konversi karakter.

(Purwanto, 2018 : 2).

Flowchart dekripsi metode Elgamal dapat dilihat sebagai berikut :



Gambar III.6. Flowchart Dekripsi Metode Elgamal

Keterangan :

1. Mulai

Merupakan simbol untuk memulai sebuah *flowchart*.

2. Key, Plaintext

Merupakan simbol deklarasi atau pengenalan input data.

3. Key

Merupakan input data berupa kunci untuk metode elgamal.

4. Ciphertext

Merupakan pesan rahasia dan pada penelitian ini pesan rahasia berupa teks di dalam *database*.

5. $m = \delta \cdot \gamma (p-1-x) \bmod p$

Merupakan rumus untuk dekripsi pada algoritma elgamal yang diletakkan pada simbol proses *flowchart*. Nilai δ (delta) didapatkan dari karakter posisi ganjil dan nilai γ (gamma) didapatkan dari karakter posisi genap, kemudian dipisahkan untuk mendapatkan hasil pesan asli.

6. Plaintext

Merupakan hasil dekripsi algoritma elgamal yang diletakkan pada simbol *output flowchart*.

7. Selesai

Merupakan simbol akhir sebuah proses pada *flowchart*.

Contoh :

a. Ciphertext

Ambil *ciphertext* yang akan didekripsi menggunakan algoritma elgamal yaitu RZb,F\$~.

b. Pisahkan Nilai Gamma dan Delta Pada Pesan Rahasia (*Ciphertext*).

Lakukan pemisahan urutan teks ganjil dan teks genap. Teks ganjil merupakan nilai gamma dan teks genap merupakan nilai delta.

1. nilai gamma

$$\gamma_1 = R = 82$$

$$\gamma_2 = = 15$$

$$\gamma_3 = , = 44$$

$$\gamma_4 = F = 70$$

$$\gamma_5 = \$ = 36$$

2. nilai delta

$$\delta_1 = Z = 90$$

$$\delta_2 = b = 98$$

$$\delta_3 = = 5$$

$$\delta_4 = = 28$$

$$\delta_5 = \sim = 126$$

c. Menghasilkan Nilai Gamma dan Delta

Nilai gamma dan delta didapatkan setelah melakukan pemisahan dan disatukan dengan kelompok ganjil dan genap.

d. Konversi Nilai Gamma dan Delta Menjadi *Plaintext*

Konversi nilai gamma dan delta menjadi *plaintext*, dengan persamaan :

$$m = \delta \cdot \gamma (p-1-x) \bmod p \dots\dots\dots(3)$$

Sehingga menghasilkan *plaintext* yang dihasilkan berupa m dalam desimal ASCII.

$$m1 = 82.90(127 \cdot 1-17) \bmod 127$$

$$= 7390 \cdot 109 \bmod 127$$

$$= 805510 \bmod 127$$

$$= 97 = a$$

$$m2 = 15.98(127 \cdot 1-17) \bmod 127$$

$$= 1470 \cdot 109 \bmod 127$$

$$= 160230 \bmod 127$$

$$= 100 = d$$

$$m3 = 44.5(127 \cdot 1-17) \bmod 12$$

$$= 220 \cdot 109 \bmod 127$$

$$= 23980 \bmod 127$$

$$= 109 = m$$

$$m4 = 70.28(127 \cdot 1-17) \bmod 127$$

$$= 1960 \cdot 109 \bmod 127$$

$$= 213640 \bmod 127$$

$$= 105 = i$$

$$m5 = 36.126(127 \cdot 1-17) \bmod 127$$

$$= 4536 \cdot 109 \bmod 127$$

$$= 494424 \bmod 127$$

$$= 110 = n$$

e. Menghasilkan *Plaintext*

Lakukan penyusunan pesan *m* yang dihasilkan dan lakukan konversi karakter sehingga menjadi *plaintext* yaitu admin.

III.4. 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 konsumen dengan menggunakan website. Secara umum gambaran sistemnya adalah aplikasi keamanan ini dibuat untuk di implementasikan pada data konsumen. Aplikasi ini bersifat Kriptografi, tugas utama aplikasi ini adalah enkripsi dan dekripsi file konsumen.

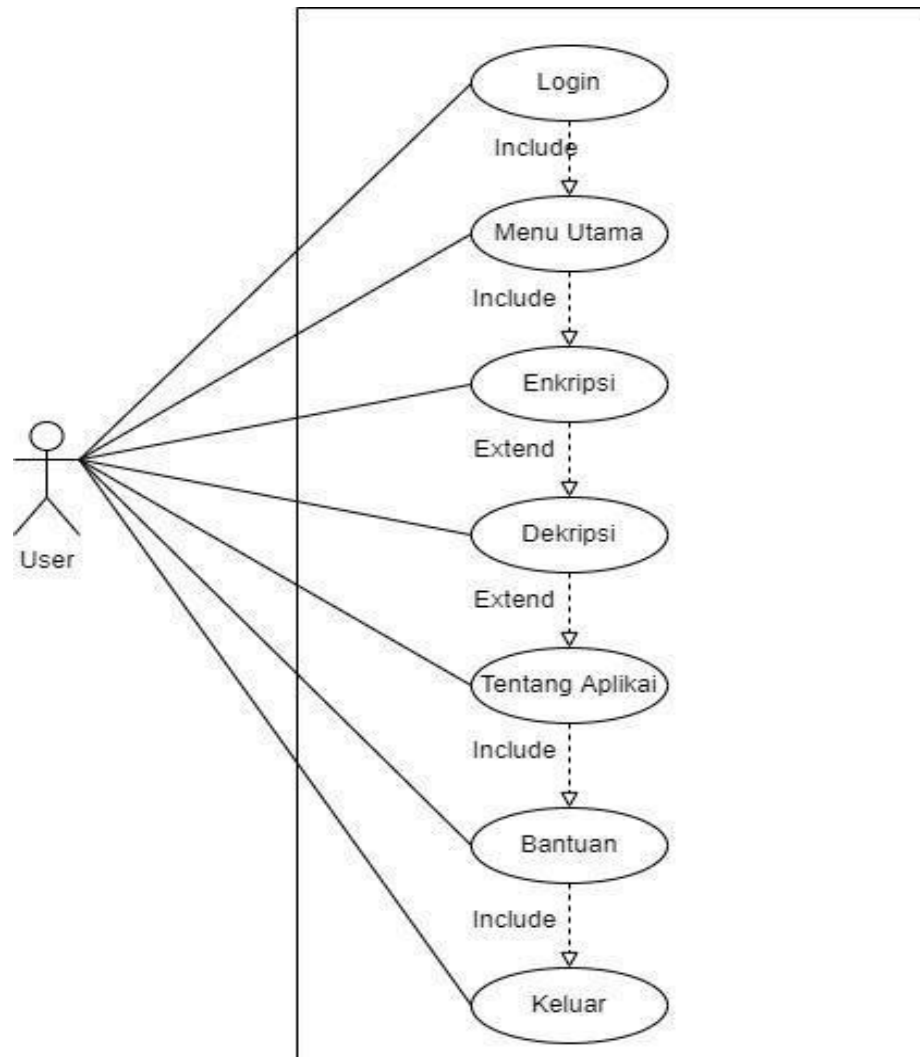
III.5 Desain Sistem

Perancangan ini akan memberikan penjelasan mengenai rancangan aplikasi serta pembentukan dan pembangunan aplikasi kriptografi algoritma *Elgamal* dalam mengamankan data konsumen.

III.5.1. 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 Gambar III.7:



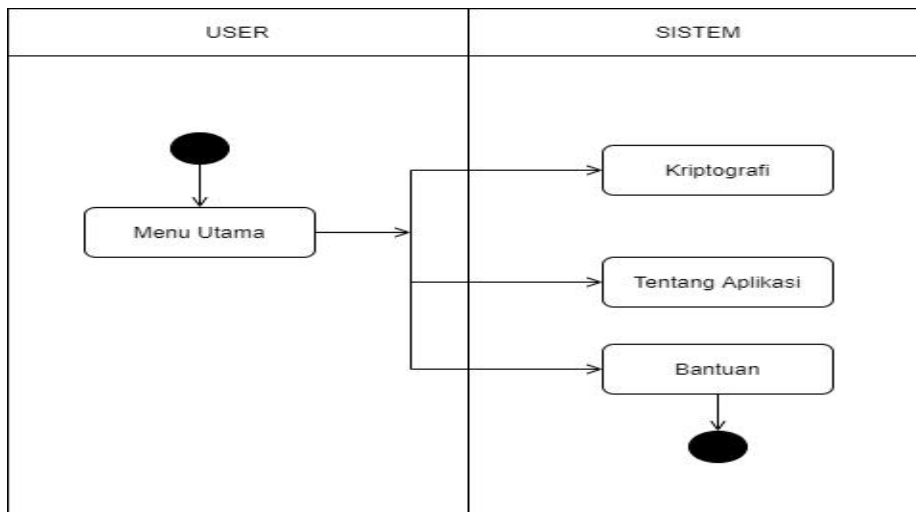
Gambar III.7 Use Case Diagram

III.5.2 Activity Diagram

Activity diagram diagram yang menggambarkan worlflow (aliran kerja) atau aktivitas dari suatu sistem atau proses bisnis. Pada dasarnya activity diagram sering digunakan oleh flowchart, activity diagram berfokus pada aktivitas-aktivitas yang terjadi yang terkait dalam suatu tunggal. Jadi dengan kata lain, diagram ini menunjukkan bagaimana aktivitas-aktivitas tersebut bergantung satu sama lain. Berikut adalah gambaran activity diagram dari sistem yang di rancang yaitu:

1. Activity Diagram Menu Utama

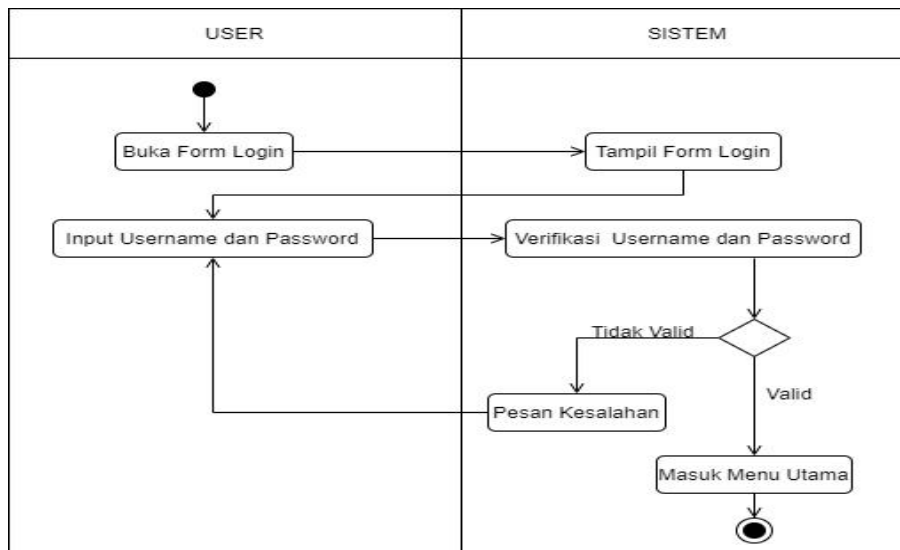
Adapun Activity Diagram Menu Utama dapat dilihat pada gambar III.8:



Gambar III.8. Activity Diagram Menu Utama

2. Activity Diagram Login

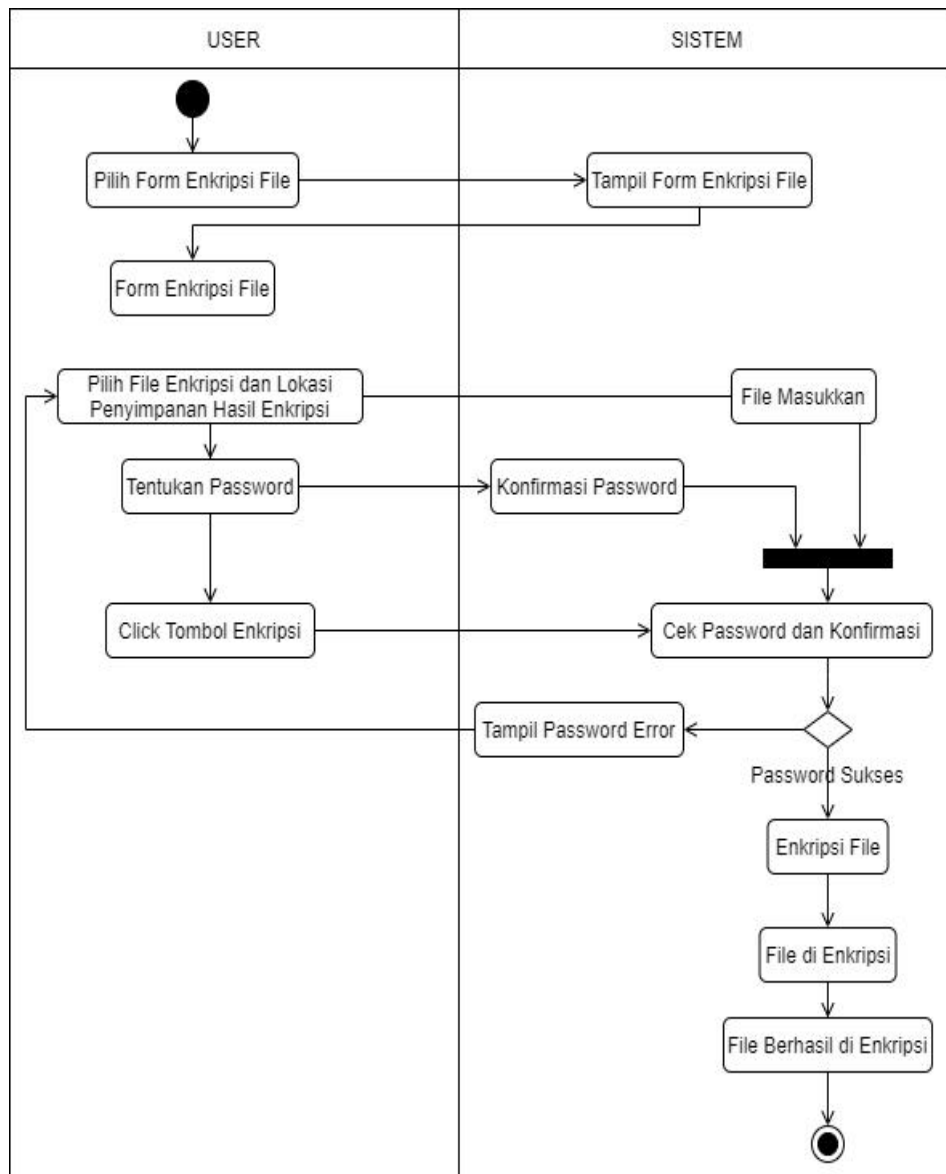
Adapun Activity Diagram login dapat dilihat pada gambar III.9:



Gambar III.9. Activity Diagram Login

3. Activity Diagram Enkripsi File

Adapun Activity Diagram Enkripsi File dapat dilihat pada gambar III.10:

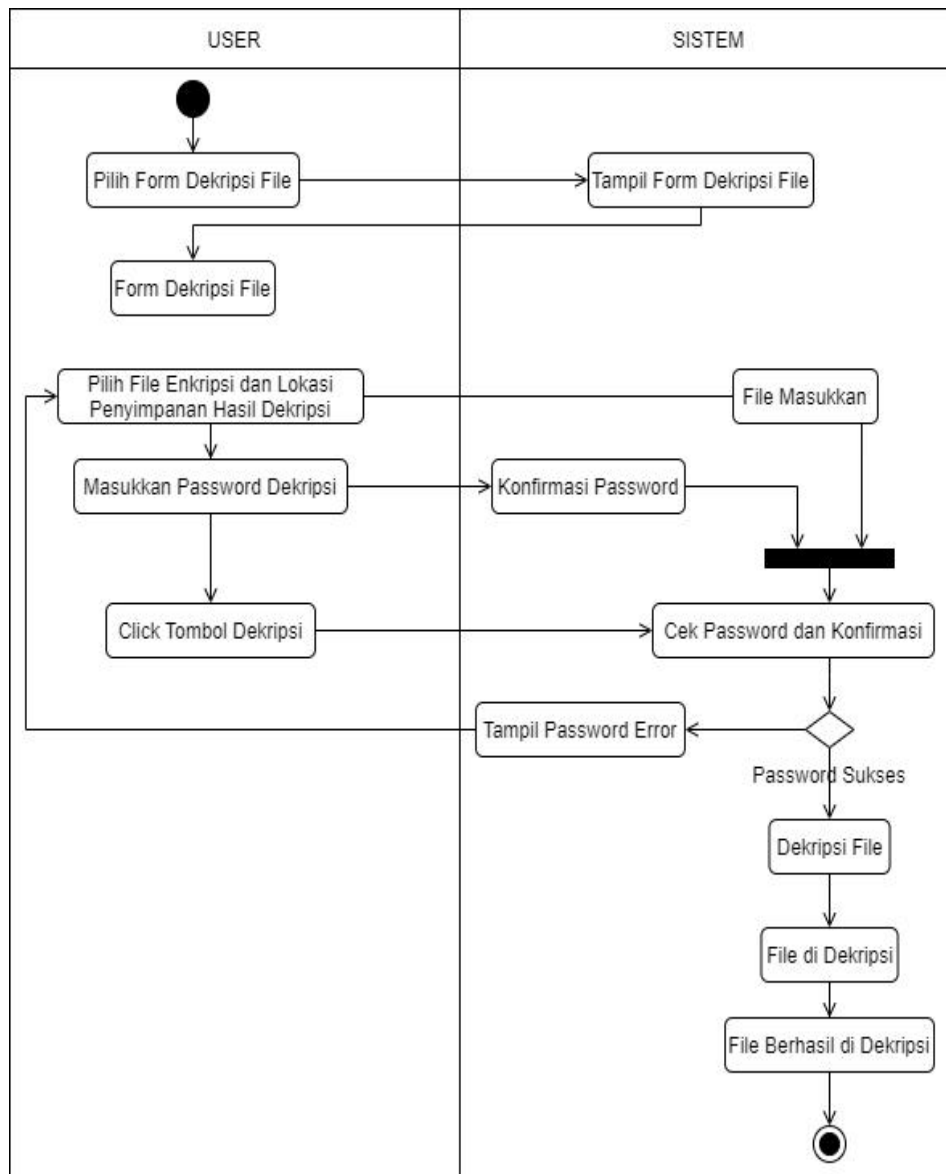


Gambar III.10. Activity Diagram Enkripsi File

4.

Activity Diagram Dekripsi File

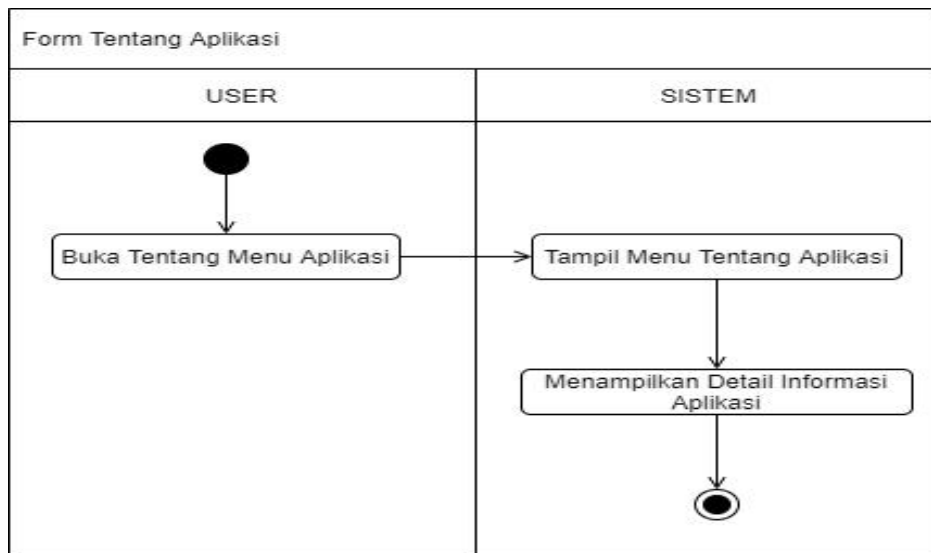
Adapun Activity Diagram Dekripsi File dapat dilihat pada gambar III.11:



Gambar III.11. Activity Diagram Dekripsi File

5. Activity Diagram Tentang Aplikasi

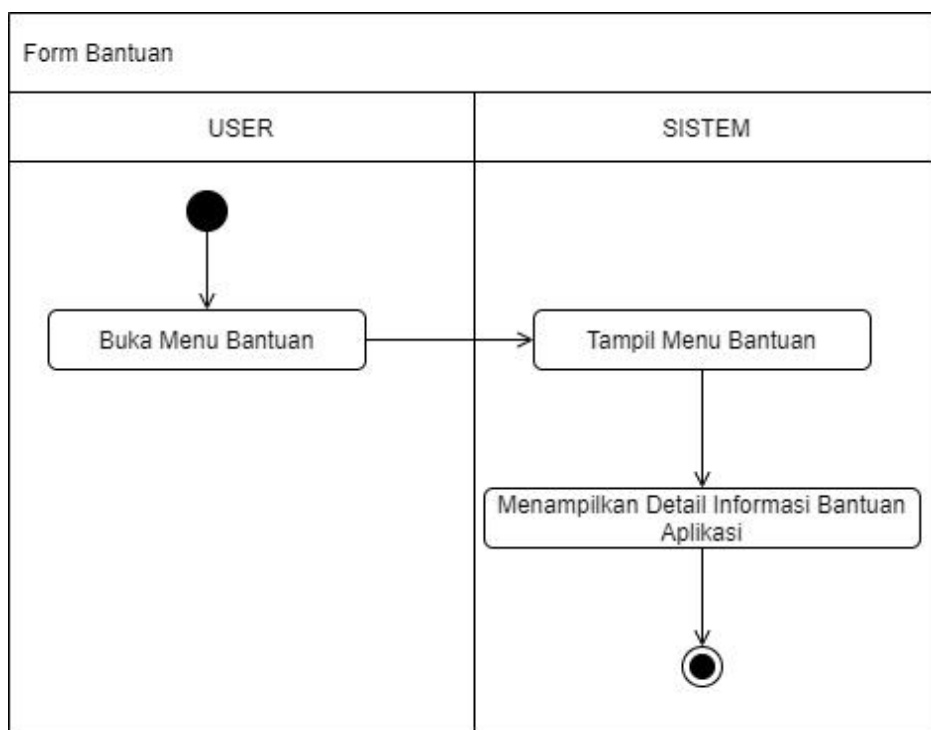
Adapun Activity Diagram Tentang Aplikasi dapat dilihat pada gambar III.12:



Gambar III.12. Activity Diagram Tentang Aplikasi

6. Activity Diagram Bantuan

Adapun Activity Diagram Bantuan dapat dilihat pada gambar III.13:



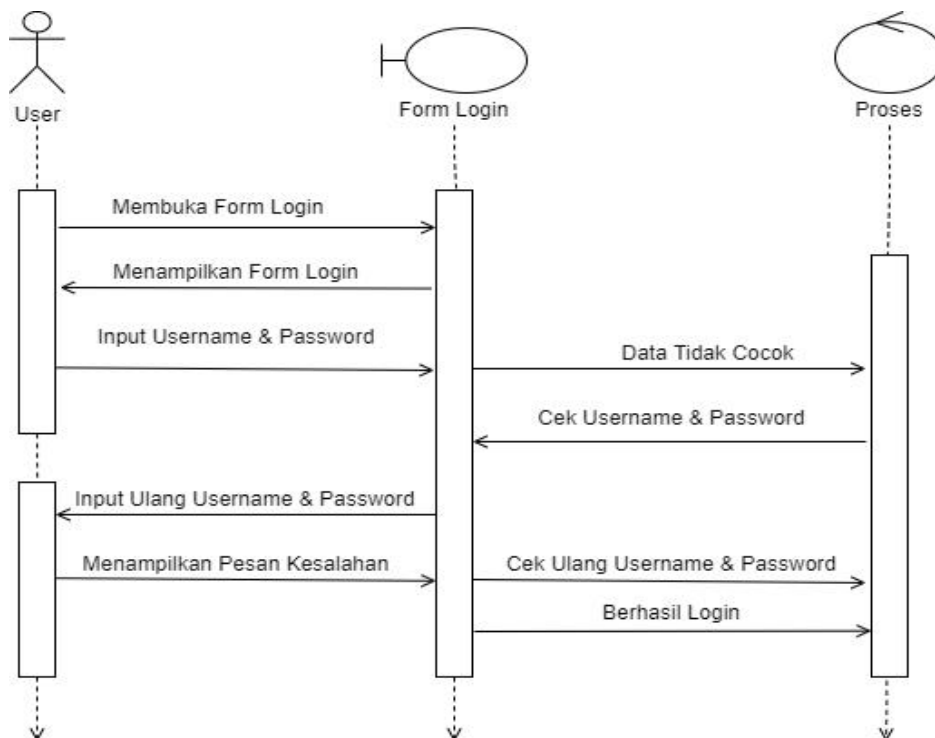
Gambar III.13. Activity Diagram Bantuan

III.5.3. Sequence Diagram

Sequence diagram merupakan salah satu diagram interaction yang menjelaskan bagaimana suatu operasi itu dilakukan message (pesan) apa yang dikirim dan kapan pelaksanaan nya. Diagram ini diatur berdasarkan waktu. Obyek-obyek yang berkaitan dengan proses berjalannya operasi diurutkan dari kiri ke kanan berdasarkan waktu terjadinya dalam pesan yang terurut. Adapun gambar sequence diagram dapat dilihat pada gambar dibawa ini.

1. Sequence Diagram Login

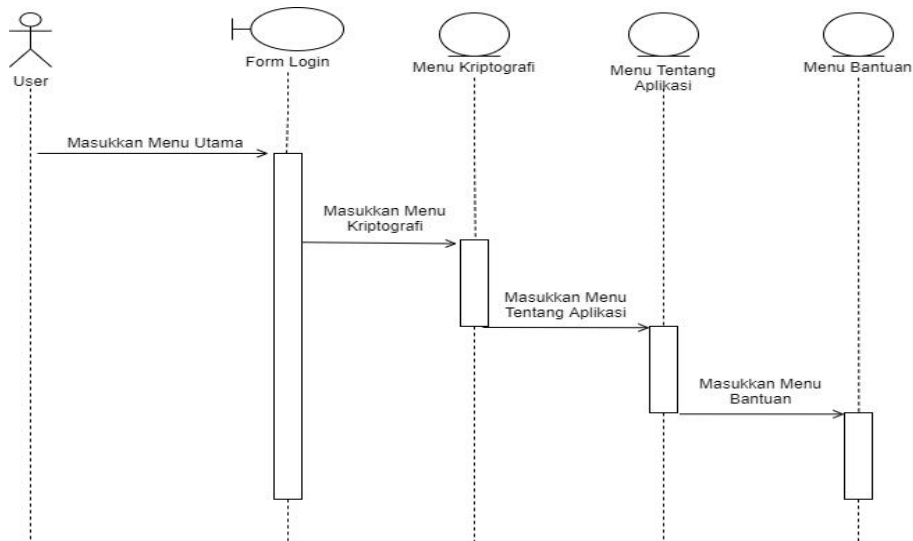
Adapun Sequence Diagram Login dapat dilihat pada gambar III.14:



Gambar III.14. Sequence Diagram pada form Login

2. Sequence Diagram Menu Utama

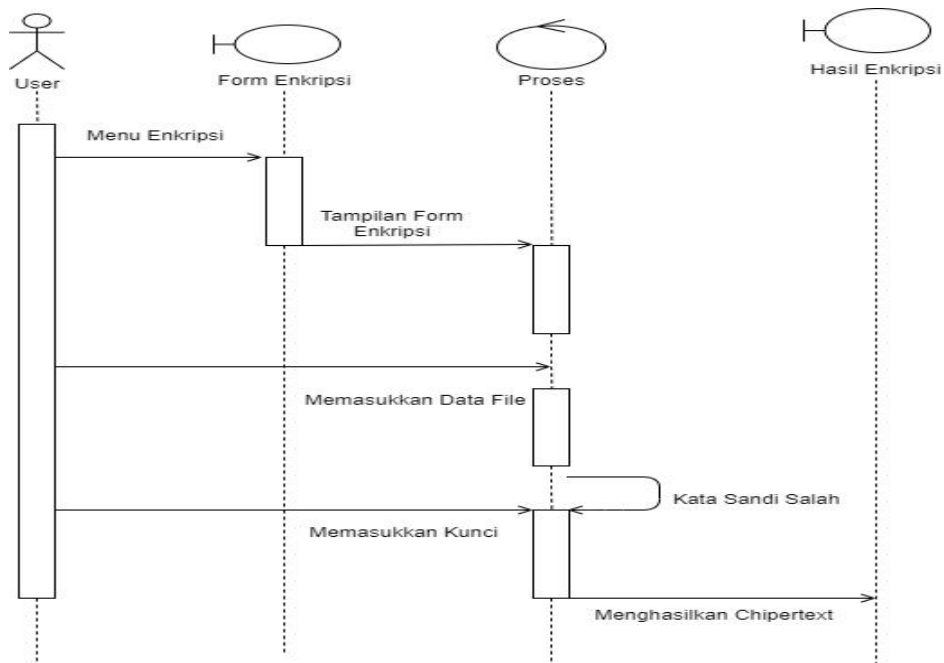
Adapun Sequence Diagram Menu Utama dapat dilihat pada gambar III.15:



Gambar III.15. Sequence Diagram Menu Utama

3. Sequence Diagram Enkripsi

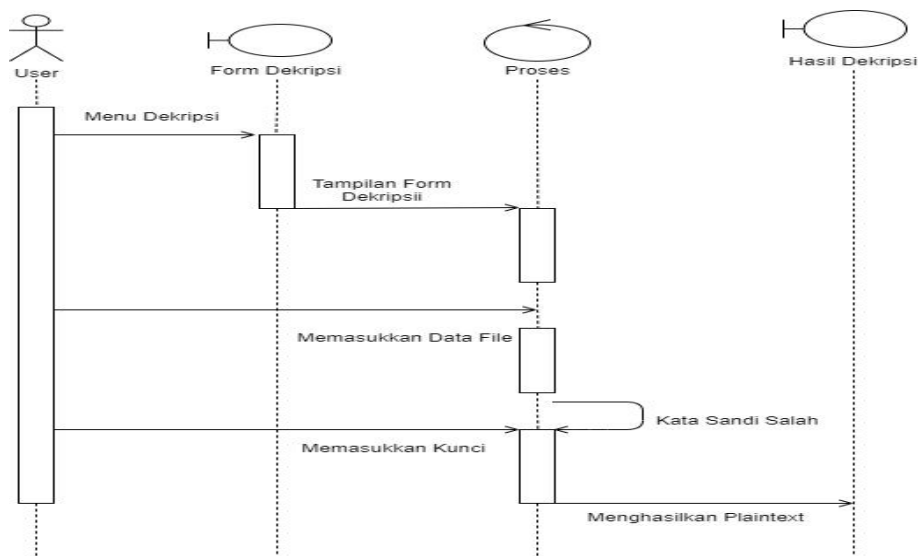
Adapun Sequence Diagram Enkripsi dapat dilihat pada gambar III.16:



Gambar III.16. Sequence Diagram Enkripsi

4. Sequence Diagram Dekripsi

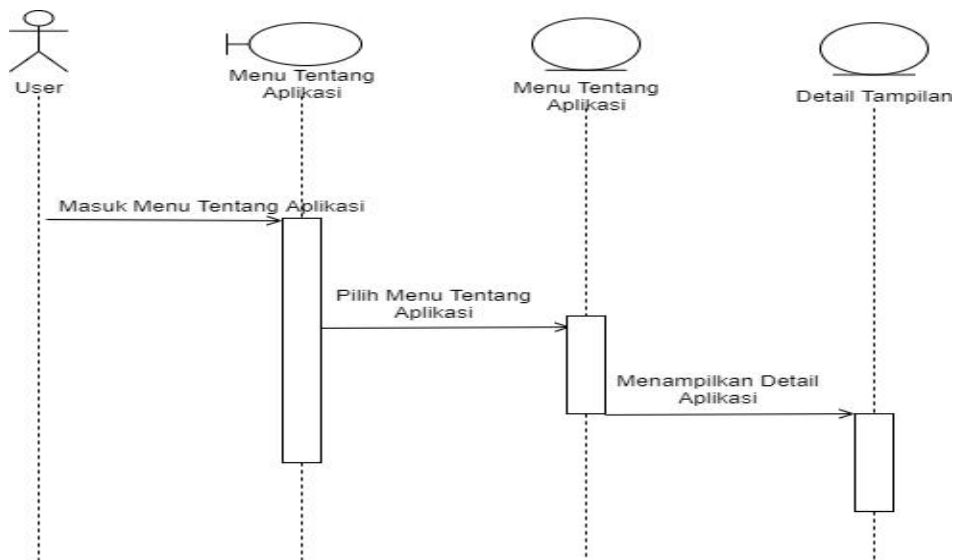
Adapun Sequence Diagram Dekripsi dapat dilihat pada gambar III.17:



Gambar III.17. Sequence Diagram Dekripsi

5. Sequence Diagram Tentang Aplikasi

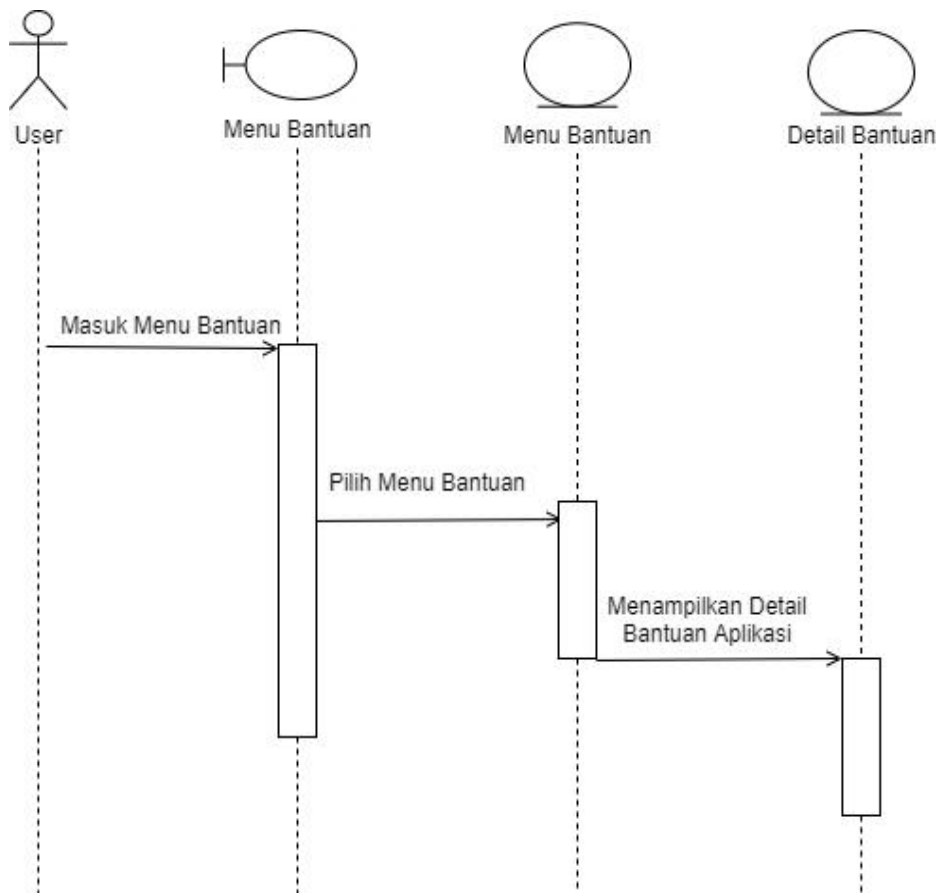
Adapun Sequence Diagram Tentang Aplikasi dapat dilihat pada gambar III.18:



Gambar III.18. Sequence Diagram Menu Utama

6. Sequence Diagram Bantuan

Adapun Sequence Diagram Bantuan dapat dilihat pada gambar III.19:



Gambar III.19. Sequence Diagram Bantuan

III.5.4 Desain User Interface

Perancangan User Interface merupakan masukan yang penulis rancang guna lebih memudahkan dalam entry data. Entry data yang dirancang akan lebih mudah dan cepat dan meminimalisir kesalahan penulisan dan memudahkan perubahan. Perancangan User Interface tampilan yang dirancang adalah sebagai berikut :

1. Rancangan Form Login

Form Login berfungsi untuk menampilkan tampilan utama dari user interface.

Adapun rancangan form login dapat dilihat pada gambar III.20:

The image shows a login form within a rectangular frame. At the top, a header bar contains the text 'Aplikasi Keamanan Data Pelanggan'. Below this, the text 'Silahkan Login :' is centered. The form includes two input fields: 'User Name' and 'Password', each followed by a text box. Below the password field is a 'Submit' button.

Gambar III.20. Desain Form Login

2. Rancangan menu utama setelah login

Rancangan menu utama adalah untuk menampilkan menu pilihan yang ada didalam website, berikut ini tampilan halaman utama dapat dilihat pada gambar III.21 :

The image shows a main menu layout. At the top, there is a header bar. On the left side of the header, there is a box containing the text 'LOGO COCA COLA'. To the right of this box, there are five menu items: 'Enkrip', 'Dekrip', 'Tentang', 'Bantuan', and 'Keluar'. Below the header bar, the main content area displays the text 'Selamat Datang'.

Gambar III.21. Desain Menu Utama

3. Rancangan Form Enkripsi

Pada bagan ini berfungsi untuk melakukan pengamanan file, Adapun rancangan Enkripsi dapat dilihat pada gambar III.22:

Data Pelanggan											
KUNCI	CABANG	PERIODE	REG.MPA	PEMOHON	ALAMAT	CBG LOKASI	TGL BAYAR	GOLONGAN	JLH BAYAR	KETERANGAN	AKSI
G											cari simpan
X											
P											
Y											

Gambar III.22. Desain Enkripsi

4. Rancangan Form Dekripsi

Pada bagan ini berfungsi untuk melakukan proses Dekripsi file yang sudah di enkripsi sebelumnya, Adapun rancangan Dekripsi dapat dilihat pada gambar III.23:

LOGO COCA COLA		Enkrip	Dekrip	Tentang	Bantuan	Keluar
Data Pelanggan						
CABANG		SIMPAN				
PERIODE						
REG.NPA						
PEMOHON						
ALAMAT						
CBG LOKASI						
TGL BAYAR						
GOLONGAN						
JLH BAYAR						
KETERANGAN						
KUNCI	X:					
	P:					
	CARI					

Gambar III.23. Desain Dekripsi

5. Rancangan Form Tentang Aplikasi

Pada bagian ini berfungsi untuk mengetahui tentang aplikasi dimana konsumen akan di jelaskan oleh desain. Adapun rancangan form tentang aplikasi dapat dilihat pada gambar III.24:

PT . Coca Cola	Enkrip	Dekrip	Tentang	Bantuan	Keluar
TENTANG APLIKASI					

Gambar III.24. Desain Form Tentang Aplikasi

6. Rancangan Form Bantuan

Pada bagian ini berfungsi untuk memberitahu tentang aplikasi yang akan digunakan untuk membantu konsumen dalam menggunakan aplikasi. Adapun rancangan form tentang aplikasi dapat dilihat pada gambar III.25:

PT . Coca Cola	Enkrip	Dekrip	Tentang	Bantuan	Keluar
BANTUAN APLIKASI					

Gambar III.25. Desain Form Bantua