BAB III
ANALISIS DAN DESAIN SISTEM

III.1. Analisis Masalah

Analisa masalah sistem pada rancang bangun aplikasi *kriptografi email gmail* ini memerlukan antarmuka untuk mengamankan dan mengendalikan email sebagai pelindung email yang masuk, menggunakan bahasa pemprograman *Java Script*. Dalam pengembangan aplikasi ini menerapkan metode enkripsi dan dekripsi dengan menggunakan algoritma RC4. Algoritma RC4 merupakan jenis algoritma kriptografi yang sifatnya simetri dan chipper block. Dengan demikian algoritma ini menggunakan kunci yang sama pada saat enkripsi dan dekripsi serta input dan outputnya berupa blok dengan jumlah bit tertentu. Algoritma RC4 mendukung berbagai variasi ukuran kunci yang akan digunakan.

III.2. Evaluasi Sistem yang Berjalan

Sistem yang sedang berjalan memiliki beberapa sebuah algoritma kriptogrfi ditambah semua kemungkinan plaintext, ciphertext dan kunci. Dalam sistem ini, seperangkat parameter yang menentukan transformasi cipher tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses enkripsi dan dekripsi tidak perlu identik, tergantung pada sistem yang digunakan.

III.3. Penerapan Algoritma RC4

Berikut adalah implementasi algoritma RC4 dengan mode 4 byte (untuk lebih menyederhanakan). Inisialisasi S-Box dengan panjang 4 byte, dengan S[0]=0, S[1]=1, S[2]=2 dan S[3]=3 sehingga array S menjadi: 0 1 2 3

Inisialisasi 4 byte kunci array, Ki. Misalkan kunci terdiri dari 2 byte yaitu byte 1 dan byte 7. Ulang kunci sampai memenuhi seluruh array K sehingga array K menjadi: 1 7 1 7

Berikutnya mencampur operasi dimana kita akan menggunakan variabel i dan j ke index array S[i] dan K[i]. Pertama diinisialisasi i dan j dengan 0. Operasi Pencampuran adalah pengulangan rumusan (j + S[i]+ K[i]) mod 4 yang diikuti dengan penukaran S[i] dengan S[j]. Untuk contoh ini, karena kita menggunakan array dengan panjang 4 byte maka algoritma menjadi:

for i = 0 to 4

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

swap S[i] dan S[j]

Dengan algoritma seperti di atas maka dengan nilai awal i = 0 sampai i = 3 akan menghasilkan array S seperti di bawah ini:

iterasi pertama:

i = 0, maka

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

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

= (0 + 0 + 1) mod 4

= 1

Swap S[0] dan S[1] sehingga menghasilkan array S: 1 0 2 3

iterasi kedua:

i = 1, maka

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

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

= (1 + 0 + 7) mod 4

= 0

Swap S[1] dan S[0] sehingga menghasilkan array S: 0 1 2 3

iterasi ketiga:

i = 2, maka

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

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

= (0 + 2 + 1) mod 4

= 3

Swap S[2] dan S[3] sehingga menghasilkan array S: 0 1 3 2

iterasi keempat:

i = 3, maka

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

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

= (3 + 2 + 7) mod 4

= 0

Swap S[3] dan S[0] sehingga menghasilkan array S : 2 1 3 0

Berikutnya adalah proses enkripsi yaitu meng-XOR kan pseudo random byte dengan plainteks, misalnya plaintetks “HI”. Plainteks terdiri dari dua karakter maka terjadi dua iterasi. Berikut iterasi 1:

Inisialisasi i dan j dengan i = 0; j = 0.

i = 0; j = 0

i = (i + 1) mod 4

= (0 + 1) mod 4

= 1

dan

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

= (0 + 2) mod 4

= 2

Swap S[i] dan S[j] yaitu S[1] dan S[2] sehingga array S menjadi 2 3 1 0

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

= (3 + 1) mod 4

= 0

K = S[t] = S[0] = 2

Byte K di-XOR-kan dengan plainteks “H”. Kemudian

iterasi 2:

i = 1; j = 2

i = (i + 1) mod 4

= (1 + 1) mod 4

= 2

dan

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

= (2 + 2) mod 4 = 0

Swap S[i] dan S[j] yaitu S[2] dan S[0] sehingga array S menjadi: 1 3 2 0

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

= (2 + 1) mod 4

= 3

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

Byte K di-XOR-kan dengan plainteks “I”.

Plainteks pada enkripsi HI

Plainteks	01001000	01001001
Pseudo random byte	00000010	00000010
Chipherteks	01001010	01001011
Hasil	J	K

Cipherteks pada dekripsi JK

Chipherteks	01001010	01001011
Pseudo random byte	00000010	00000010
Plainteks	01001000	01001001
Hasil	H	I

III.4. Desain Sistem

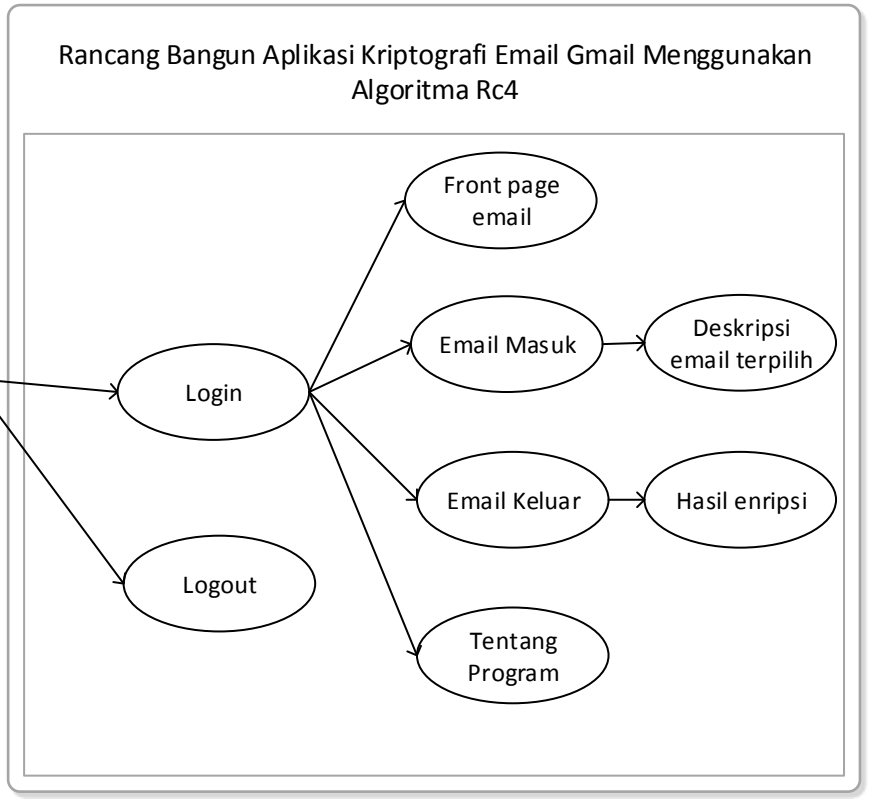
Desain sistem pada penelitian ini dibagi menjadi dua desain, yaitu desain sistem secara global untuk penggambaran model sistem secara garis besar dan desain sistem secara detail untuk membantu dalam pembuatan sistem.

III.4.1. Desain Sistem Secara Global

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

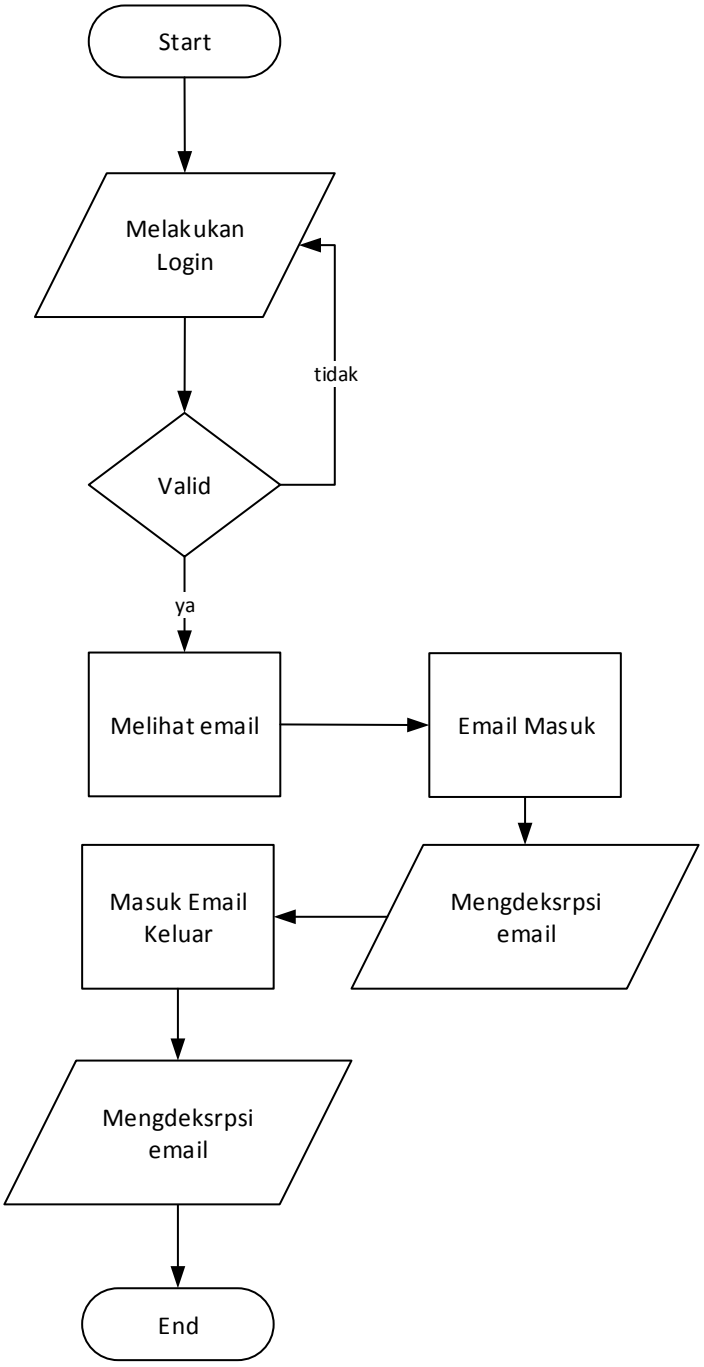
III.4.1.1. *Usecase* Diagram

Rancangan ini disusun dengan tujuan mendesain dan merepresentasikan program. Fungsinya adalah untuk memudahkan email masuk dan keluar yang akan dibuat pada gambar III.1 berikut.



Gambar.III.1. *Use Case Diagram*

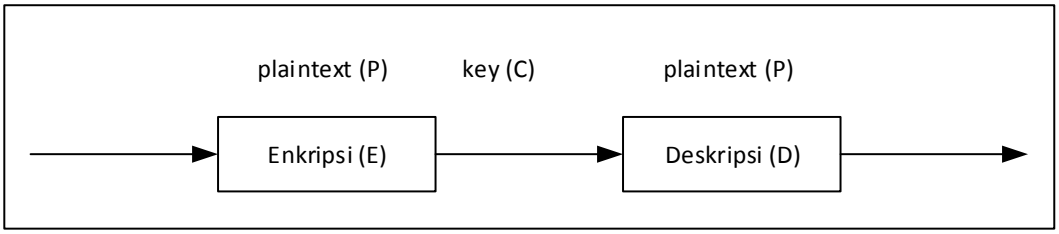
III.4.1.2. *Flow Chart*



Gambar.III.2. ***Flow Chart***

III.4.1.3. Blok Diagram Enkripsi Dan Deskrpsi

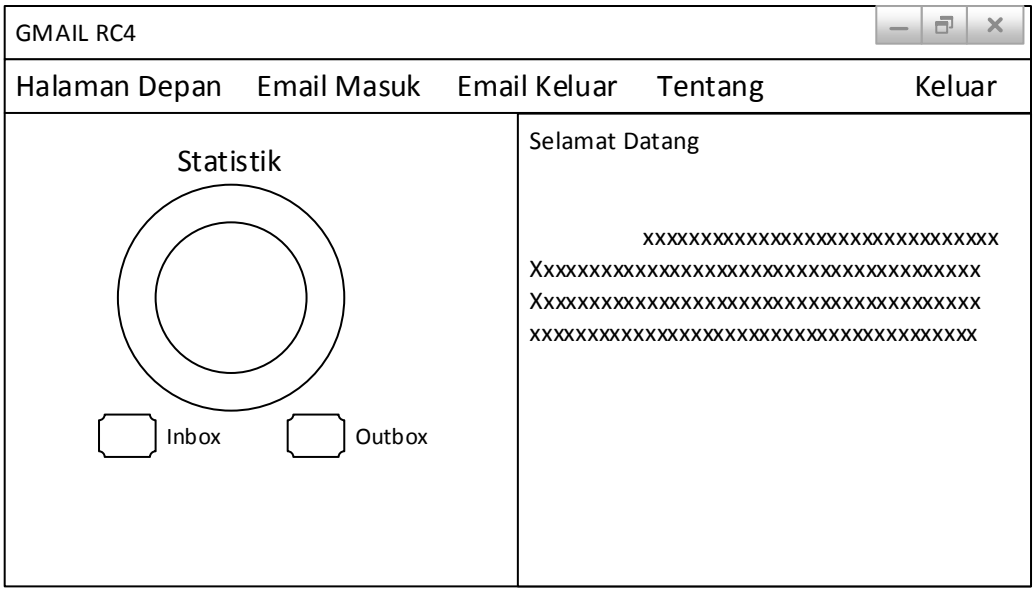
Pesan yang akan dienkripsi yang dimisalkan plaintext (P), proses enkripsi dimisalkan enkripsi (E), proses dekripsi dimisalkan dekripsi (D), dan pesan yang sudah dienkripsi disebut ciphertext yang dimisalkan ciphertext (C) maka dapat digambarkan pada gambar berikut ini :



Gambar III.3. Proses *enkripsi* dan *deskripsi*

III.5. Desain User Interface

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



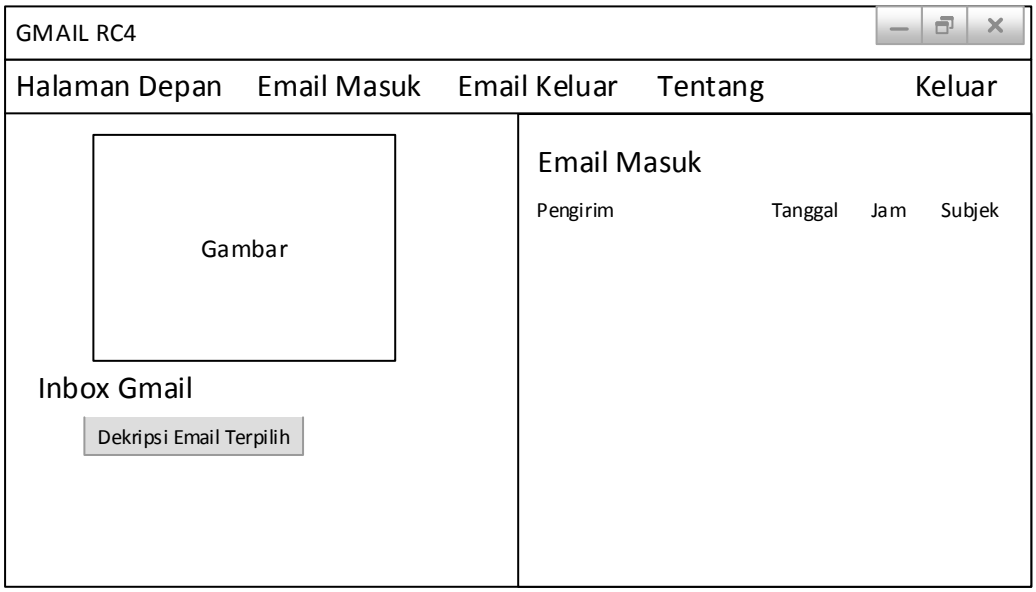
Gambar.III.4. Desain Tampilan Depan

Keterangan :

Dari desain tampilan depan terdapat halaman dashboard untuk melihat gerafik email masuk dan keluar.

1. Desain Tampilan Email Masuk

Desain yang dirancang untuk melihat tampilan email masuk untuk pesan siapa saja yang masuk terlihat seperti pada gambar III.5 berikut :



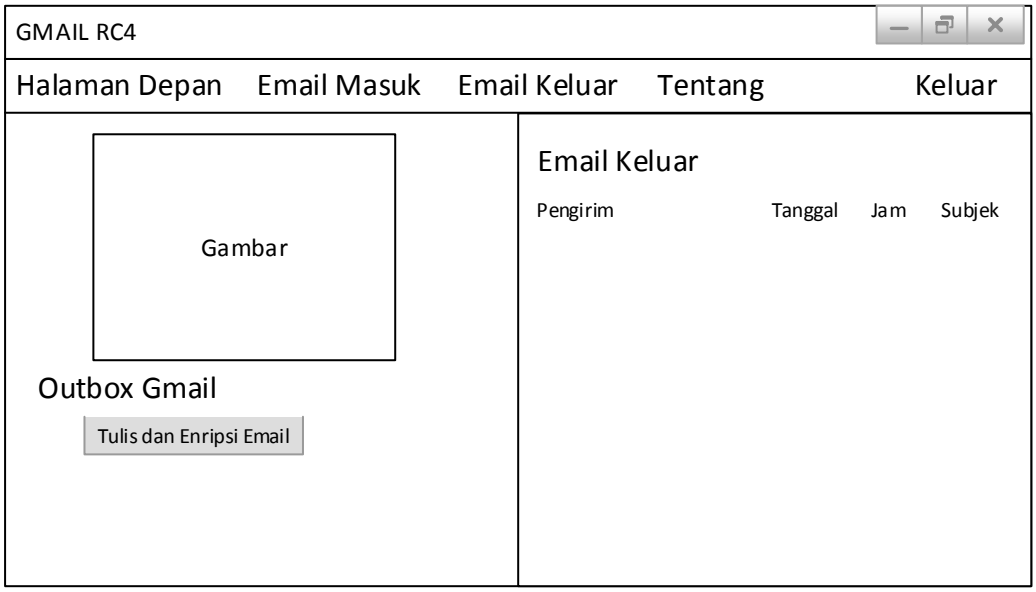
Gambar.III.5. Desain Email Masuk

Keterangan :

Dari desain email masuk terdapat table nama email masuk, admin siap melakukan tulis email menekan tombol-tombol yang telah disediakan.

2. Desain Tampilan Enkripsi Email Keluar

Desain tampilan enkripsi email keluar yang dirancang untuk mengunci pesan yang keluar terlihat seperti pada gambar III.6 berikut :



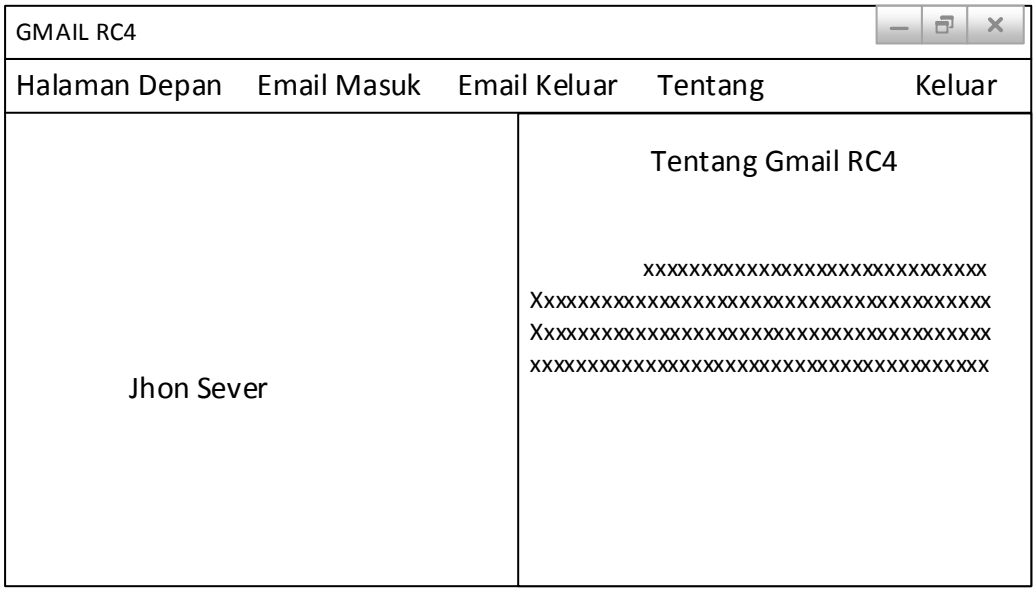
Gambar.III.6. Desain Tampilan Enkripsi Email Keluar

Keterangan :

Dari desain mengenkripsi pesan yang keluar untuk mengirim pesan yang ada, dan admin bisa melakukan enkripsi pesan.

3. Desain Tampilan Tentang

Desain tampilan tentang untuk mengetahui aplikasi terlihat seperti pada gambar III.7 berikut :



Gambar.III.7. Desain Tampilan Tentang

Keterangan :

Dari desain tampilan tentang untuk mengetahui versi program yang telah dibuat.