BAB III

ANALISIS DAN RANCANGAN

Sebelum merancang sebuah sistem, perlu dilakukan analisis terlebih dahulu. Analisis sistem adalah proses menentukan kebutuhan sistem, apa yang harus dilakukan sistem untuk memenuhi kebutuhan klien (*user*). Dengan adanya analisis sistem, sistem yang dirancang akan lebih baik dan memudahkan pengembang sistem dalam perbaikan apabila pada kemudian hari ditemukan kesalahan atau kekurangan.

III.1. Analisa Masalah

Penggunaan Email sudah menjadi kebutuhan tersendiri dan banyaknya penyedia layanan email memudahkan pengguna untuk memilih email yang digunakan, email biasanya digunakan untuk saling berkomunikasi antara 1 atau lebih pihak penerima email dan salah satu kelemahan yang penulis analisa dari penggunaan email adalah tidak tersedianya fungsi enkrripsi dan dekripsi terhadap email sehingga siapapun yang mempunyai akses ke email penerima email bisa membaca email tersebut, untuk mengatasi permasalahan tersebut penulis mengajukan sebuah proses pengiriman email terenkripsi dengan menerapkan algoritma One Time Pad sebagai proses enkripsi dan dekripsi pesan email.

III.1.1 Input

Input data pada aplikasi pengiriman email dengan menggunakan algoritma *One Time Pad* adalah berupa pesan email, alamat pengirim, email penerima dan juga kunci dari algoritma.

III.1.2 Proses

Berdasarkan sistem yang sedang berjalan, tahapan-tahapan proses enkripsi pesan di dalam aplikasi pengiriman email menggunakan algoritma *One Time Pad* adalah sebagai berikut :

1. *User* melakukan koneksi ke *server* mail dengan memasukkan *username* dan *password email*
2. *User* memasukkan alamat penerima email, nama, subjek, pesan email dan juga file lampiran jika ada
3. *User* melakukan proses pembangkitan kunci secara random sesuai dengan panjang pesan email
4. Kemudian pesan email di enkripsi dan dilanjutkan dengan melakukan pengiriman email kepada pengguna.

III.1.3 Output

Hasil *output* pada aplikasi pengiriman email terenkripsi ini adakah pesan email yang dikirim kepada penerima email dalam bentuk *ciphertext* sehingga diperlukan proses dekripsi dengan memasukkan kunci yang sudah dimiliki oleh penerima email sebelumnya.

III.2. Analisis Algoritma One Time Pad

Algoritma *One Time Pad* merupakan jenis algoritma *substitutional alphabetic* yang menukar huruf dari suatu kalimat menjadi huruf lain, pada penelitian ini algoritma *One Time Pad* digunakan untuk mengamankan pesan email yang akan dikirimkan, berikut adalah penerapannya dengan melakukan

enkripsi terhadap pesan “POTENSI” dengan kunci yang digunakan sesuai panjang pesan sebanyak panjang pesan n=7, kunci yang digunakan adalah “UZUMAKI”, berikut adalah prosesnya

PESAN = POTENSI
KUNCI = UZUMAKI

Langkah pertama yang harus dibuat adalah membuat tabel, seperti dibawah ini :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

Dari tabel diatas dilakukanlah proses enkripsi dengan menerapkan algoritma *One Time Pad*, berikut adalah hasil prosesnya

1. Ubah menjadi kode ASCII dan biner untuk kata POTENSI dan UZUMAKI, sehingga didapat hasil sebagai berikut:

Karakter	ASCII	BINER
P	80	0101 0000
O	79	0100 1111
T	84	0101 0100
E	69	0100 0101
N	78	0100 1110
S	83	0101 0011
I	73	0101 0011
Hal yang sama dilakukan pada kunci		
U	85	0101 0101
Z	90	0101 1010
U	85	0101 0101
M	77	0100 1101
A	65	0100 0001
K	75	0100 1011
I	73	0100 1001

2. Pesan di-XORkan dengan kunci maka akan diperoleh

   10100010 10100000 00100001 00000001 11100011 00000000 00000000

3. Kode Biner tersebut diterjemahkan lagi menjadi karakter Diperoleh : ¢ !ã

4. Untuk memperoleh plainteks kembali, penerima pesan cukup mengubah lagi plainteks menjadi ASCII dan meng-XORkan kembali dengan kunci

   Proses dekripsinya dapat dilihat sebagai berikut:

1. Hasil *ciphertext* ¢ !ã terlebih dahulu di konversi menjadi biner hingga hasilnya sebagai berikut:

   10100010 10100000 00100001 00000001 11100011 00000000 00000000

2. Hasil binary *ciphertext* di XOR kembali dengan kunci UZUMAKI, seperti dibawah ini

U	85	0101 0101
Z	90	0101 1010
U	85	0101 0101
M	77	0100 1101
A	65	0100 0001
K	75	0100 1011
I	73	0100 1001

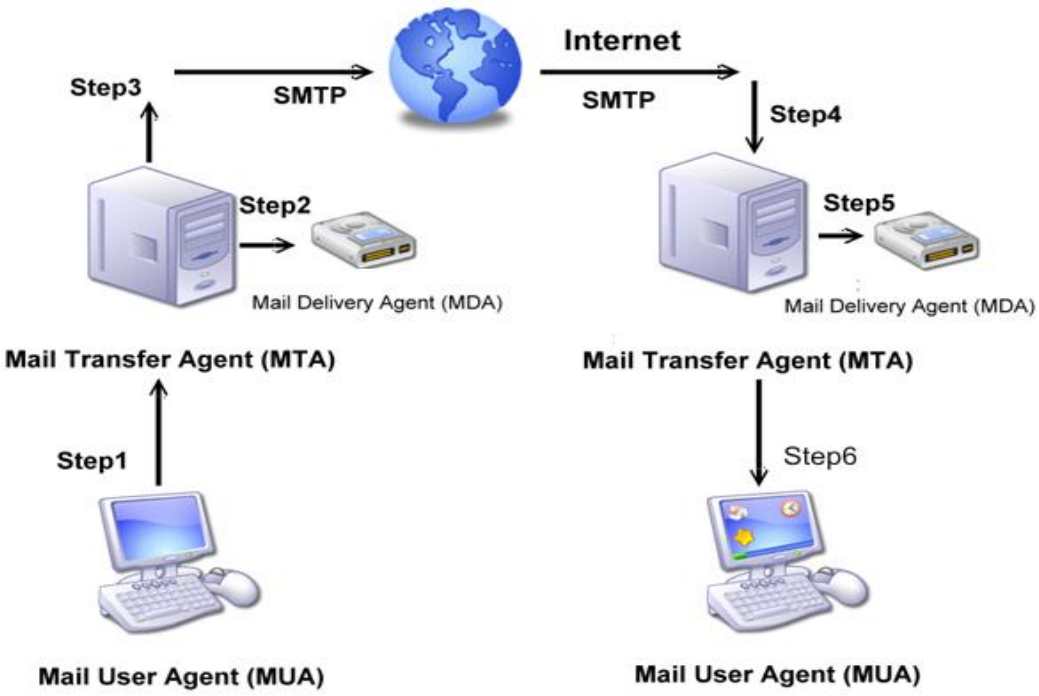
3. Setelah melalui proses XOR Hasilnya sebagai berikut:

   01010000 01001111 01010100 01000101 01001110 01010011 01001001

4. Hasil prorses XOR di konversi menjadi ASCII hasilnya adalah POTENSI.

III.3. Service Mail Transfer Protocol

Service mail tranfer protocol merupakan sebuah layanan yang ada pada setiap sistem operasi, untuk sistem operasi windows service SMTP harus diaktifkan secara manual, dan untuk cara kerja dari SMTP tampak seperti pada gambar dibawah ini:



Gambar III.1. SMTP Service

Adapun keterangan dari proses SMTP diatas adalah sebagai berikut:

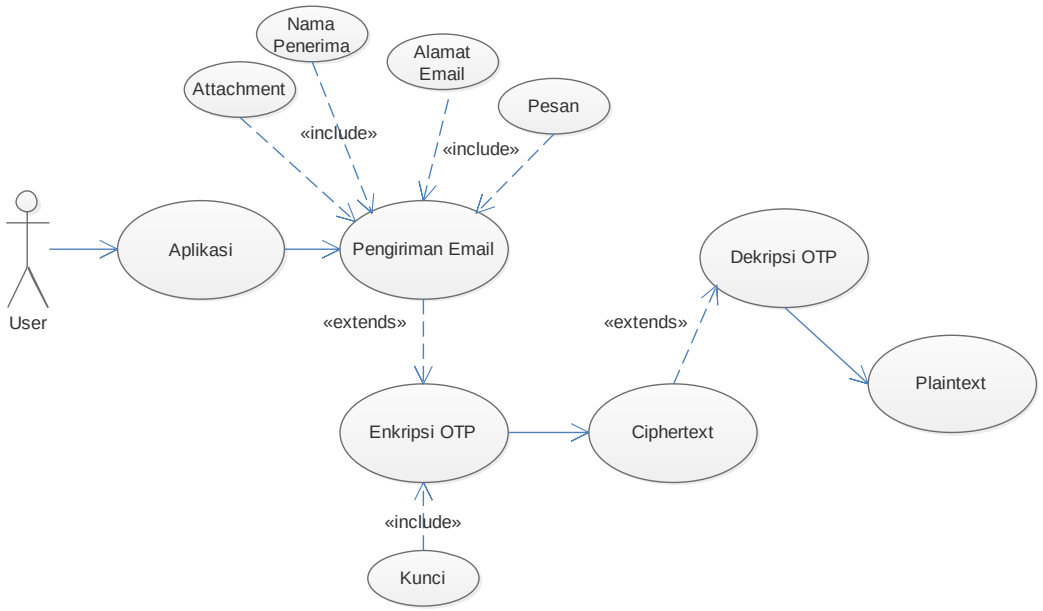
1. SMTP Pengirim melakukan koneksi TCP/IP dengan SMTP penerima dan menunggu server untuk mengirim pesan 220 yang menandakan pelayanan terhadap pesan sudah siap atau pesan 421 pelayanan tidak siap.
2. HELO dikirim oleh server dengan menunjukkan nama domain.
3. Pengirim akan memulai memberikan perintah kepada SMTP dimana apabila SMTP mendukung perintah tersebut akan membalas dengan pesan 250 OK.
4. Memberikan informasi kepada SMTP tentang tujuan dari email dengan perintah RCPT TO dilanjutkan dengan alamat email yang dituju.
5. Setelah tujuan diset, dilanjutkan dengan perintah DATA yang menunjukkan bahwa baris berikutnya adalah isi dari email dengan diakhiri dengan CRLF.
6. Client mengisikan data sesuai dengan pesan yang akan dikirimkan hingga

mengisikan CRLF kembali untuk menandakan berakhirnya data.

7. Pengirimkan akan menghentikan kegiatan dengan memberi perintah QUIT.

III.4. Pemodelan Sistem

Pemodelan sistem yang penulis gunakan adalah UML dengan model *Use Case Diagram*, berikut adalah pemodelan *use case diagram* dari sistem yang penulis rancang



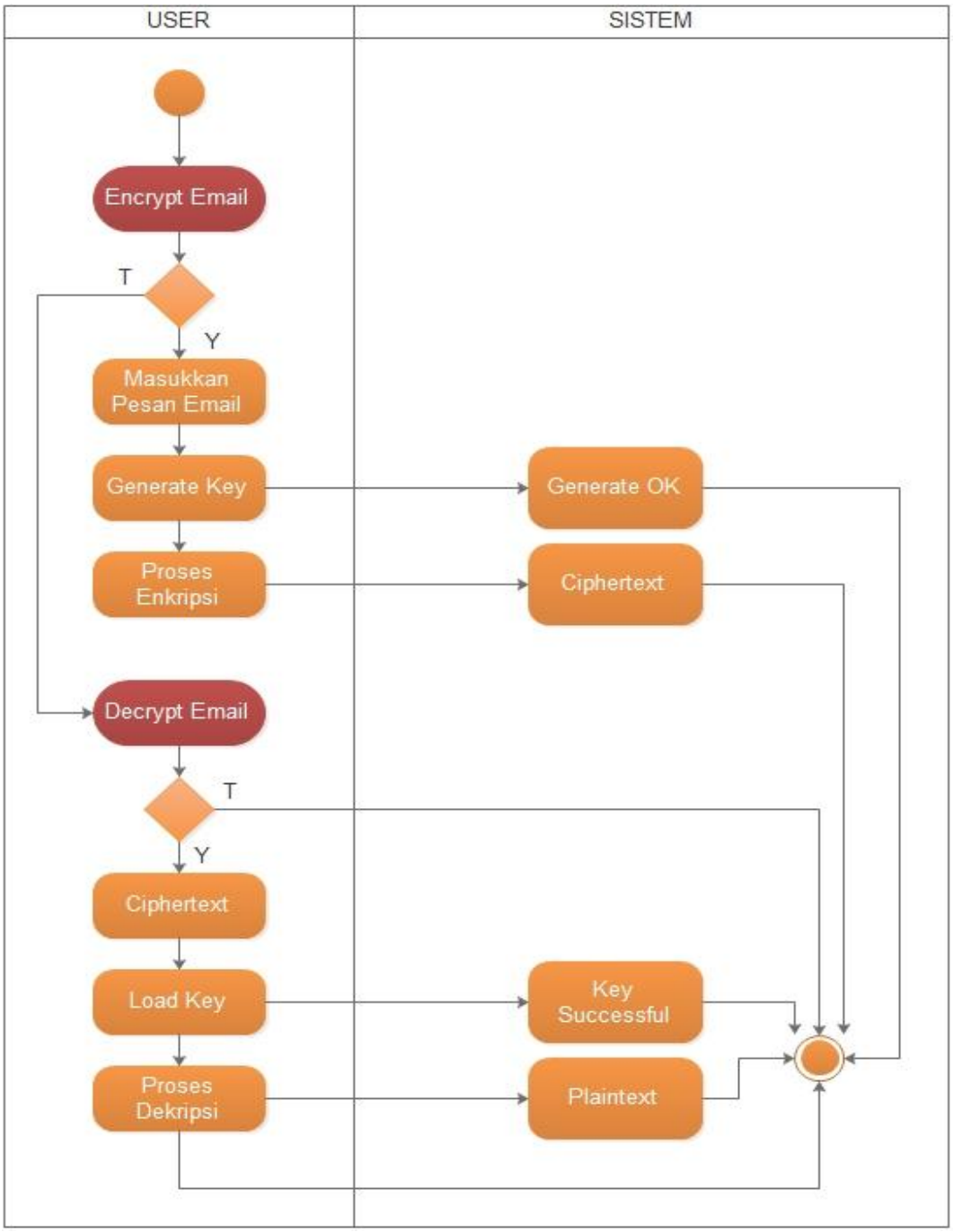
Gambar III.2. Use Case Diagram Sistem

Gambar III.2 merupakan use case diagram dari sistem yang penulis buat, adapun penjelasannya adalah sebagai berikut:

1. Pengguna menjalankan aplikasi OTPEmail
2. Pada aplikasi, pengguna bisa melakukan pengiriman email dengan beberapa informasi seperti pesan, alamat email, nama penerima dan file attachment
3. Proses pengiriman email bisa di enkripsi dengan menggunakan algoritma OTP dengan kunci yang panjangnya sama dengan panjang pesan.
4. Hasil enkripsi menghasilkan *ciphertext* yang akan dikirimkan via email.

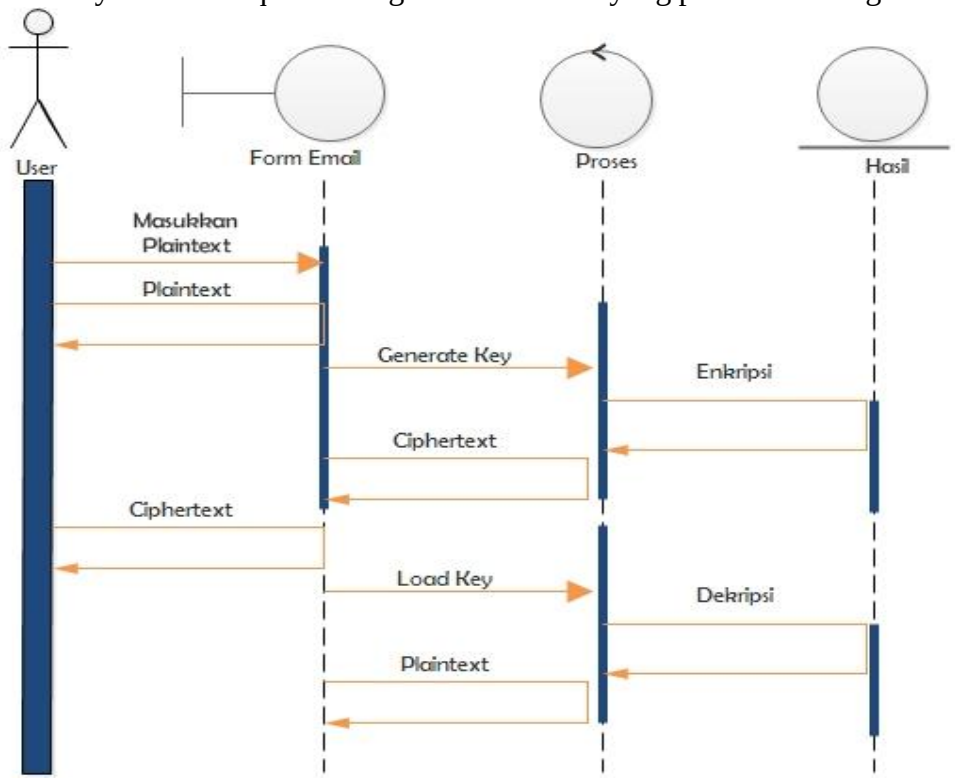
5. Hasil *ciphertext* bisa di dekripsi dengan menggunakan kunci yang sesuai dengan kunci enkripsi sehingga menghasilkan plaintext.

Selain use case diagram penulis juga merancang activity diagram dan sequence diagram dari sistem yang penulis rancang, berikut adalah diagramnya



Gambar III.3 Activity Diagram Sistem

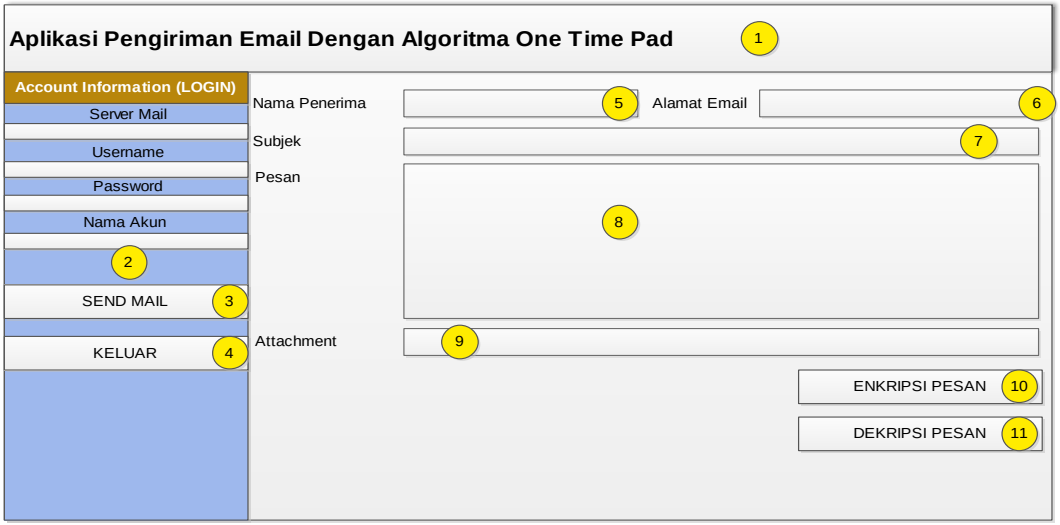
Berikutnya adalah sequence diagram dari sistem yang penulis rancang



Gambar III.4 Sequence Diagram Sistem

III.5. Perancangan Sistem

Perancangan sistem merupakan gambaran dari sistem yang penulis rancang, berikut adalah rancangan dari sistem yang penulis rancang terdiri dari 1 (satu) buah desain.



Gambar III.5. Desain Utama Program

Adapun penjelasannya sebagai berikut:

1. Menampilkan judul dari aplikasi
2. Menampilka pengaturan konfigurasi pengiriman email, pada bagian ini terdiri dari bebeapa informasi sebagai berikut:
   a. Server mail digunakan untuk memilih jenis server yang digunakan, bisa google mail atau yahoo mail
   b. Username digunakan untuk memasukkan username dari email
   c. Password digunakan untuk memasukkan password dari email
   d. Nama akun digunakan untuk memasukkan nama pengirim
3. Tombol yang digunakan untuk mengirim email
4. Tombol yang digunakan untuk menutup aplikasi
5. Textbox yang digunakan untuk memasukkan nama penerima email
6. Textbox yang digunakan untuk memasukkan alamat email
7. Textbox yang digunakan untuk memasukkan subjek email
8. Textbox yang digunakan untuk memasukkan pesan email

9. Textbox yang digunakan untuk memasukkan attachment email
10. Textbox yang digunakan untuk melakukan proses enkripsi sebelum pesan dikirimkan
11. Textbox yang digunakan untuk melakukan proses dekripsi terhadap pesan