BAB III

ANALISIS DAN PERANCANGAN

III.1. Analisa Masalah

Kebutuhan manusia akan perangkat informasi dan komunikasi seakan menjadi kebutuhan yang tidak terpisahkan dalam kehidupan. Dengan banyaknya aplikasi saat ini sangat membantu mengurangi aktifitas yang dilakukan banyak orang. Saat ini perkembangan teknologi informasi dan komunikasi dari waktu ke waktu kian meningkat. Didalam dunia teknologi informasi dan komunikasi sangat diperlukan suatu tempat penyimpanan data yang berfungsi menampung data yang penting khususnya pada perangkat *Android Mobile Phone.* Dewasa ini sudah semakin marak pembobolan data baik secara langsung maupun tidak langsung. Untuk itu pentingnya dilakukan pengamanan agar data penting dapat terjamin keamanannya. Perangkat *Android Mobile Phone* merupakan perangkat yang sangat handal karena memiliki kemampuan yang dapat digunakan hampir pada seluruh perangkat lain seperti jam tangan, kulkas, tv, ac, lampu, bahkan pada mobil.

Dalam dunia komputer pengamanan dikenal dengan kriptografi yang berasal dari bahasa Yunani yaitu *cryptos* yang artinya *"secret"* (yang tersembunyi) dan *graphein* yang artinya "*writing"* (tulisan). Jadi kriptografi berarti *"secret writing"* (tulisan rahasia). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pada data sehingga menjamin keamanannya. Salah satu metode yang dipergunakan untuk mengamankan data adalah dengan Algoritma ElGamal.

Pada desain *menu* di aplikasi untuk keamanan data pesan singat ini dapat dijelaskan sebagai berikut :

1. *Splash*, yang berfungsi permulaan untuk mengload aplikasi.
2. *Menu* Utama, merupakan tampilan yang digunakan untuk menapilkan menu tulis pesan, pesan masuk, pesan terkirim,dan about.
3. Tulis pesan, berfungsi untuk mengirimkan pesan yang akan di *enkrips*i ke no tujuan.
4. Pesan masuk, berfungsi untuk melihat pesan yang di terima, memproses *dekripsi* isi pesan dan membalas pesan.
5. Pesan terkirim, berfungsi untuk melihat laporan pesan yang dikirim.
6. *About*, merupakan tampilan dari tentang aplikasi.

III.2. Algoritma ElGamal

Algoritma ElGamal merupakan algoritma berjenis *Asimetric key* yang artinya bahwa kunci yang digunakan dalam proses enkripsi dan dekripsi berbeda.

A. Studi Kasus

Pada suatu hari, Irdham akan berkomunikasi tentang lokasi transaksi jual beli barang dagangannya kepada Andi yang hanya mengetahui lokasi tersebut. Akan tetapi, pesan itu harus rahasia dan dienkripsi. Pesan itu berbunyi “kampus”.

Prosesnya adalah sebagai berikut,

1. Pembentukan kunci

   Irdham harus membuat kunci publik, misalkan dipilih bilangan prima aman, p = 2579 dan elemen primitive α = 2. Selanjutnya dipilih a = 765 dan dihitung,

   $\beta = 2^{765} \ mod \ 2579 = 949$

   Diperoleh kunci publik (p, α, ß)=(2579,2,949) dan kunci rahasia a = 765. Irdham memberikan kunci publik ini kepada Andi. Sementara kunci rahasia tetap dipegang oleh Irdham.

2. Andi memperoleh kunci publik (p, a, ß) = (2579,2,949). Dan Andi kemudian akan mengenkripsi pesan rahasia yang akan dikirimkannya. Sebelumnya, pesan itu diterjemahkan dalam kode ASCII, seperti pada tabel III.1 di bawah ini.

Tabel III.1. Konversi Pesan ke dalam Kode ASCII

i	Karakter	Plainteks m_i	ASCII
1	k	m_1	107
2	a	m_2	97
3	m	m_3	109
4	p	m_4	112
5	u	m_5	117
6	s	m_6	115

3. Proses selanjutnya, adalah menentukan bilangan acak rahasia $k_i \in \{0,1,\ldots,2577\}$, i = 1, 2, …, 30. Kemudian dihitung, $\gamma = 2^{k_i} \ mod\ 2579$ dan $\delta = 949^{ki}\ , m_i \ mod\ 2579$. Hasil enkripsi seperti tabel III.2 dibawah ini

Tabel III.2. Proses Enkripsi

i	m_i	k_i	$\gamma = 2^{k_i} \ mod\ 2579$	$\delta = 949^{ki}\ , m_i \ mod\ 2579$
1	107	766	1898	342
2	97	2298	520	1516
3	109	146	22	359
4	112	2483	1742	830
5	117	702	1052	1302
6	115	988	21253	2087

4. Kemudian cipherteks itu dikirimkan oleh Andi kepada Irdham. Saat diterima, Irdham harus mendekripsikan cipherteks tersebut agar dapat dibaca. Irdham mempunyai kunci

publik p = 2579 dan kunci rahasia a = 765 untuk mendekripsikan cipherteks tersebut sesuai dengan algoritma dekripsi.

Tabel III.3. Proses Dekripsi

I	$y_i,\ \delta_i$	$y_i^{1813} \ mod\ 2579$	$m_{i=\delta i}.\ y_i^{1813} \ mod\ 2579$	Huruf
1	(1898,342)	219	107	k
2	(520,1516)	1771	97	a
3	(22,359)	1825	109	m
4	(1742,830)	286	112	p
5	(1052,1302)	422	117	u
6	(2153,2087)	655	115	s

Jadi, pesan rahasia yang dikirimkan Andi berbunyi " kampus ".

III.2.1 Proses Enkripsi Algoritma ElGamal

Enkripsi data merupakan bagian awal dari proses pengamanan data. Proses enkripsi menggunakan kunci publik (p,g,y) dan sebuah bilangan integer acak k ($k \in \{0,1,..., p - 1\}$) yang dijaga kerahasiaannya oleh penerima pesan. Untuk setiap karakter dalam pesan dienkripsi dengan menggunakan bilangan k yang berbeda beda. Satu karakter yang direpresentasikan dengan menggunakan bilangan bulat ASCII akan menghasilkan kode dalam bentuk blok yang terdiri atas dua nilai (a,b).

a) Ambil sebuah karakter dalam pesan yang akan dienkripsi dan transformasi karakter tersebut ke dalam kode ASCII sehingga diperoleh bilangan bulat m. Plainteks tersebut disusun menjadi blok-blok m1, m2, ……, sedemikian hingga setiap blok merepresentasikan nilai di dalam rentang 0 (nol) sampai p-1.

b) Memilih bilangan acak k, yang dalam hal ini $0 < k < p-1$, sedemikian hingga k relative prima dengan p-1.

c) Hitung nilai a dan b dengan persamaan berikut :

$a = g^k \pmod p$

$b = y^k m \pmod p$

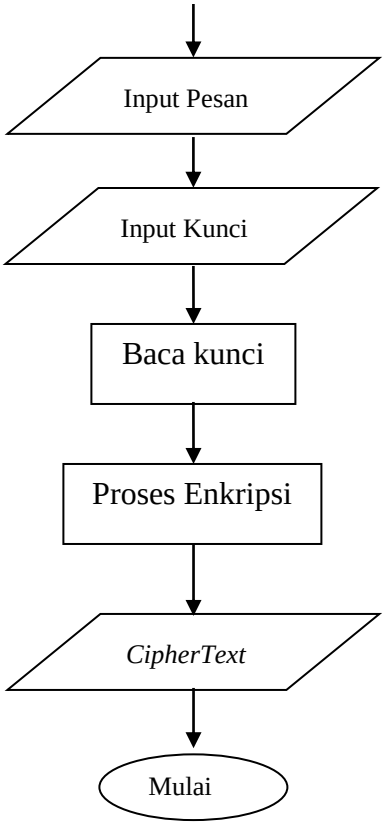
d) Diperoleh cipherteks untuk karakter m tersebut dalam blok (a,b)

e) Melakukan proses di atas untuk seluruh karakter dalam pesan termasuk karakter spasi.

III.2.2. Enkripsi

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang lain. Dengan ekkripsi, data kita disandikan (*Encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (men-*decrypt*) data tersebut, digunakan kunci yang berbeda yaitu dengan kunci rahasia (*private key*).

Keamanan dari enkripsi tergantung beberapa faktor salah satunya yaitu menjaga kerahasiaan kuncinya bukan algoritmanya. Proses enkripsi dapat diterangkan dengan gambar III.1 berikut ini.



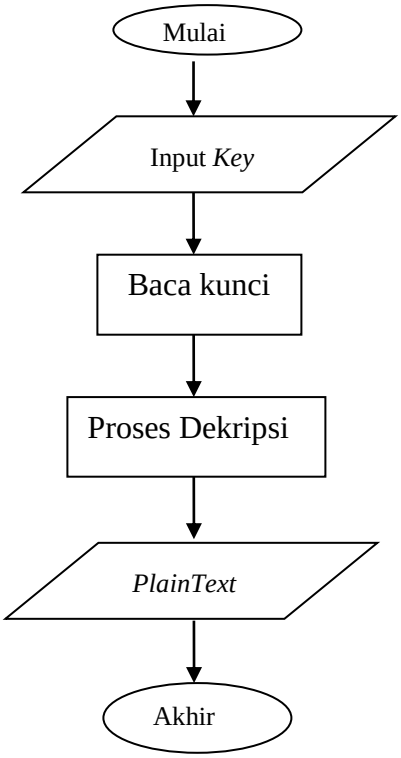
Gambar III.1. *Flowchart* Proses Enkripsi

Keterangan :

1. Input pesan
2. Input kunci
3. Baca kunci untuk melakukan enkripsi pesan
4. Lakukan perhitungan untuk melakukan enkripsi dengan menggunakan rumus $a = g^k \pmod p$ dan $b = y^k m \pmod p$
5. Outputnya adalah *ciphertext* a dan b
6. Selesai

III.2.3. Dekripsi

Dekripsi digunakan untuk mengembalikan data-data atau informasi yang sudah dienkripsi sehingga dapat dibaca kembali. Dengan dekripsi, data dikembalikan kebentuk awal sehingga dapat dibaca dengan baik. Adapun *Flowchart* dekripsi dapat dilihat pada gambar III.2 berikut.



Gambar III.2. *Flowchart* Proses Dekripsi

Keterangan :

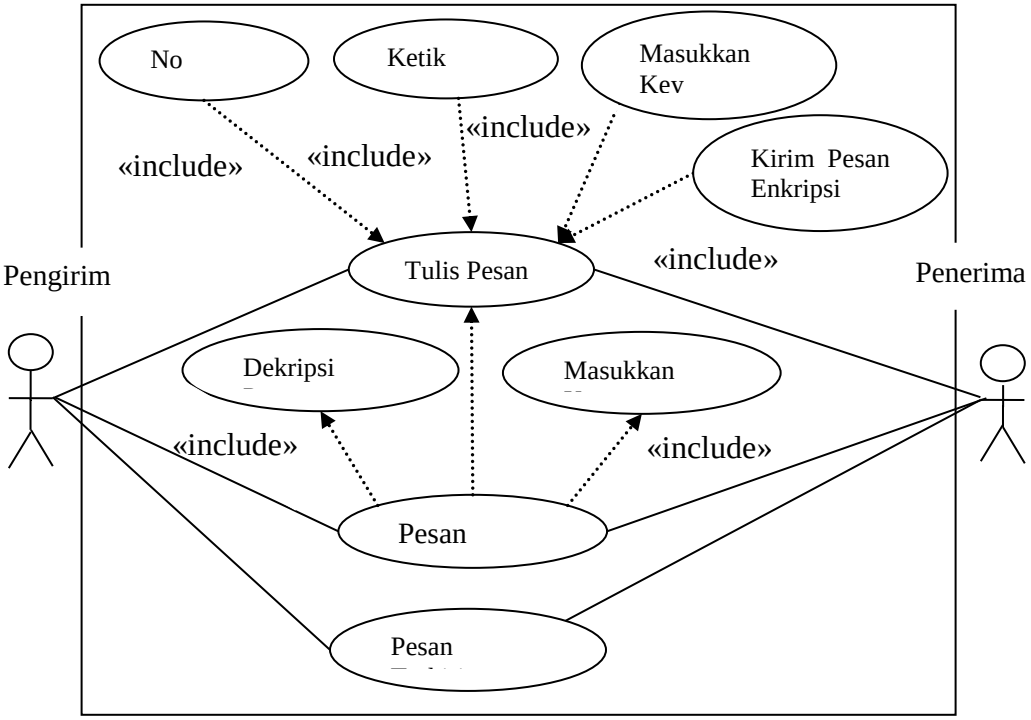
1. Input kunci untuk didekripsi
2. Baca kunci
3. Lakukan perhitungan untuk dekripsi dengan menggunakan rumus $m = b/a^x \pmod p$ dengan $(a^x)^{-1} = a^{p-1-r} \bmod p$
4. Outputnya adalah *plaintext*
5. Selesai

III.3. *Unified Modeling Language* (UML)

Penggambaran UML menggunakan diagram *use-case* yang selanjutnya setiap proses bisnis yang terjadi akan diperjelas dengan diagram *activity* lalu diilustrasikan secara detail menggunakan diagram *sequence*. Aktor dan pelaku yang terlibat dalam sistem adalah sebagai berikut :

III.3.1. *Use Case* Diagram

Adapun *use-case* diagram dapat dilihat pada gambar III.3 berikut.



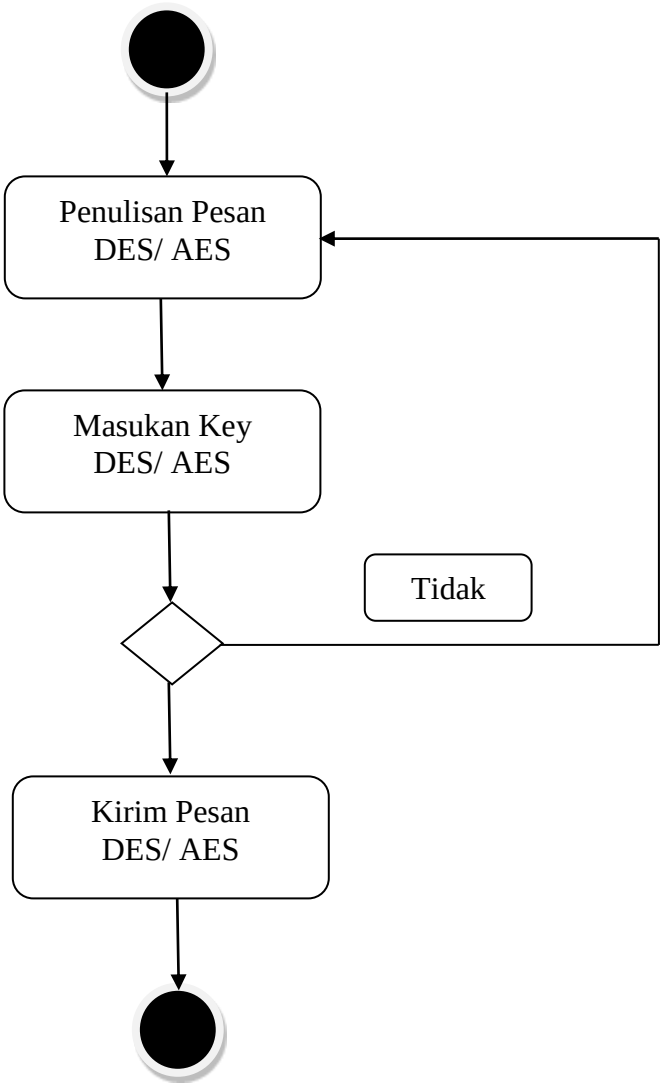
Gambar III.3. *Use Case* Diagram

III.3.2. *Activity* Diagram

Activity diagram adalah teknik untuk menggambarkan logika prosedural, proses bisnis, dan jalur kerja. Berikut ini akan dijelaskan *activity* diagram pada setiap proses enkripsi dan dekripsi yang terjadi pada aplikasi yang dibangun.

1. Activity Diagram Penulisan Pesan

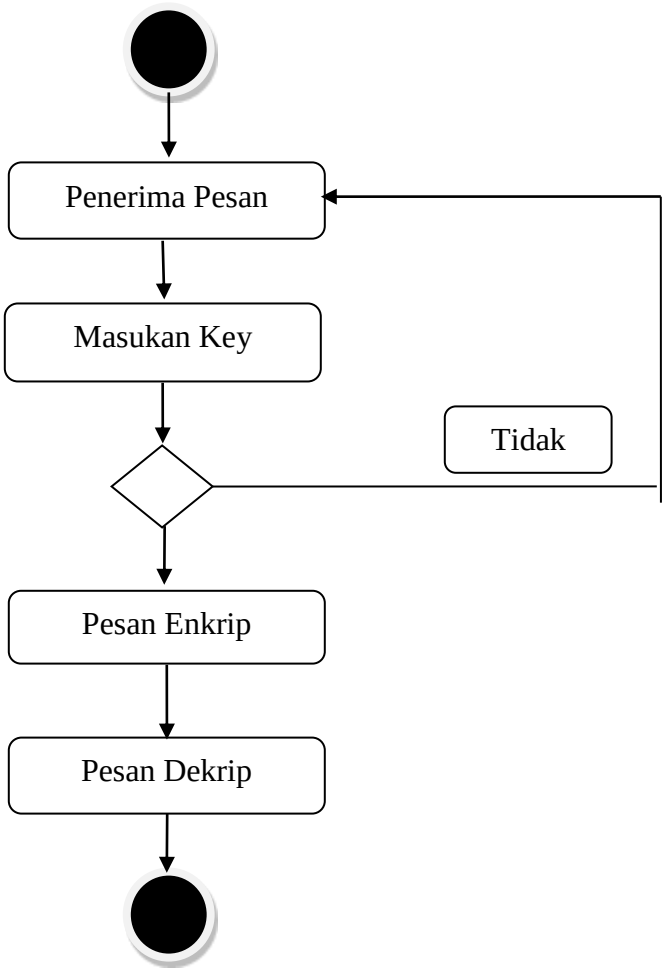
Activity diagram Penulisan Pesan, dapat dilihat pada gambar dibawah ini :



Gambar III.4. *Activity Diagram* Penulisan Pesan

2. Activity Diagram Penerima Pesan

Activity diagram Penerima Pesan, dapat dilihat pada gambar dibawah ini :



Gambar III.5. *Activity Diagram* Penerima Pesan

Pada proses enkripsi, menunjukkan bahwa hal pertama dilakukan adalah menulis pesan lalu memasukkan kunci pesan. Setelah pesan di inputkan maka isi pesan akan diambil lalu akan dilakukan proses enkripsi dengan menggunakan algoritma ElGamal. Kemudian pesan yang sudah dienkripsi akan di kirim. Begitu juga halnya pada proses dekripsi setelah pesan masuk masukkan kunci jika benar pesan akan di dekripsi.

III.4. Spesifikasi Perangkat

Dalam perancangan aplikasi untuk perangkat *Android Mobile Phone* ini penulis menggunakan beberapa perangkat agar aplikasi ini dapat berjalan lancar dan sesuai dengan yang diharapkan, yaitu sebagai berikut ini :

1. Perangkat Keras (*Hardware*)
   a. Komputer yang setara *Core i3*
   b. *Smartphone Android* dengan OS 4.2.1 atau diatasnya
   c. *Mouse, Keyboard* dan Monitor
2. Perangkat Lunak (*Software)*
   a. *Operating System,* OS yang dipergunakan dalam perancangan adalah *Windows* 7 dan untuk pengujian adalah OS *Android* pada perangkat *mobile.*
   b. *Eclipse ADT (Android Development Tools),* sebagai editor *source code Java.*
   c. JDK *Java 7.0,* sebagai bahasa program.

III.5. Desain Sistem

Dalam proses perancangan ini akan dijelaskan beberapa rancangan aplikasi yang akan dibangun yaitu sebagai berikut :

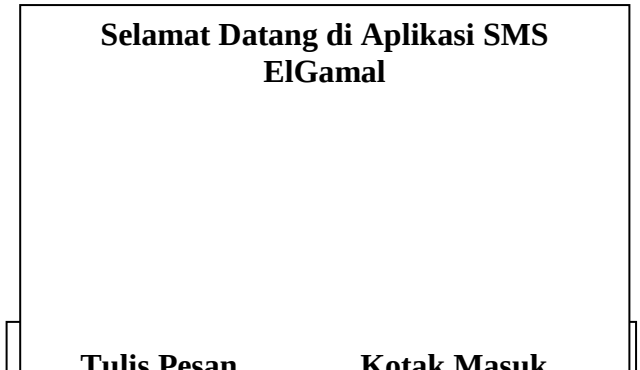
III.5.1. Rancangan Awal Pembukaan Program

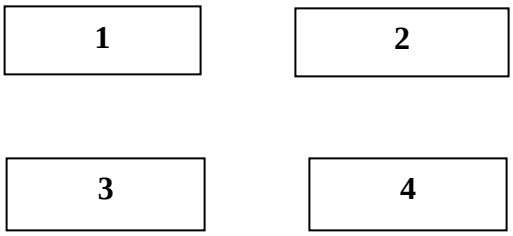
Gambar III.6 ini dibuat untuk menampilkan rancangan awal ketika program pertama kali dibuka.

Gambar III.6. Halaman Pembuka Program

III.5.2. Rancangan Menu Utama

Berikut ini adalah rancangan form menu utama yang dapat lihat pada gambar III.7 di bawah ini.





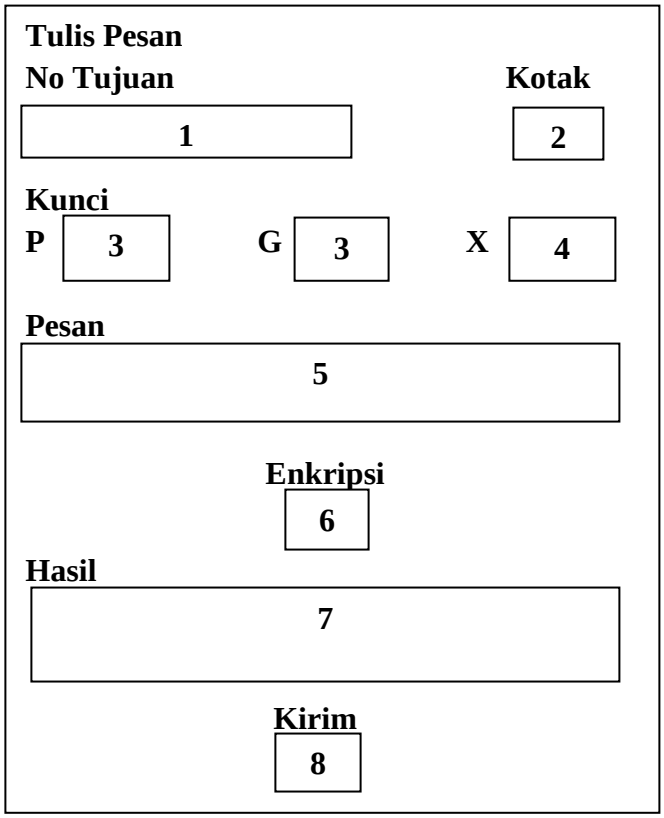
Gambar III.7. *Form* Utama

Pada desain menu utama di aplikasi untuk keamanan data pesan singat ini dapat dijelaskan sebagai berikut :

1. Tulis pesan, berfungsi untuk mengirimkan pesan yang akan di *enkrips*i ke no tujuan.
2. Pesan masuk, berfungsi untuk melihat pesan yang di terima, memproses *dekripsi* isi pesan dan membalas pesan.
3. Pesan terkirim, berfungsi untuk melihat laporan pesan yang dikirim.
4. *About*, merupakan tampilan dari tentang aplikasi.

III.5.3. Rancangan *Form* Hasil Enkripsi

Berikut ini adalah rancangan *form* hasil enkripsi yang dapat lihat pada gambar III.8 di bawah ini.



Gambar III.8. *Form* Hasil Enkripsi

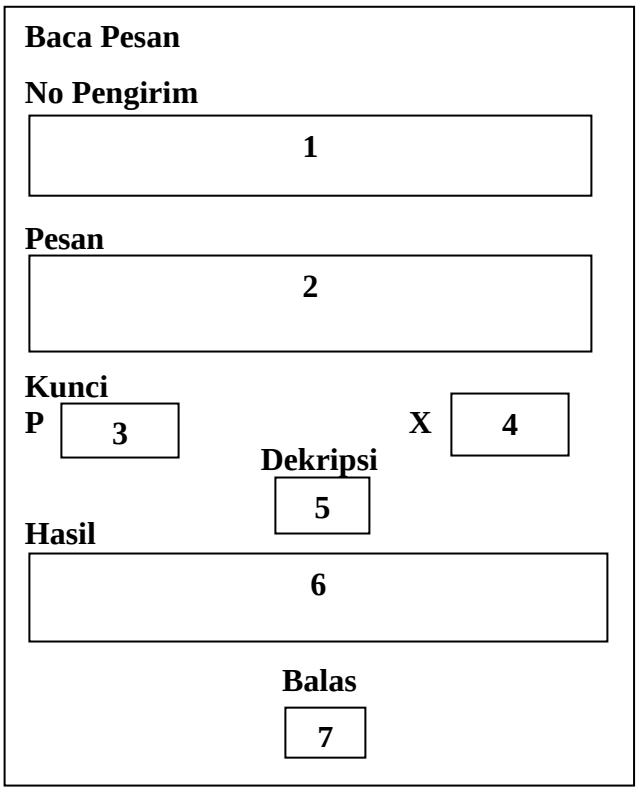
Pada desain *menu* tulis pesan di aplikasi untuk keamanan data pesan singat ini dapat dijelaskan sebagai berikut :

1. No tujuan, berfungsi untuk memasukkan no.
2. Kontak, berfungsi untuk mengambil no tujuan dari penyimpanan no.
3. Kunci p, g, berfungsi untuk menginputkan kunci publik untuk melakukkan enkripsi pesan.
4. Kunci x, berfungsi untuk menginput kunci privat sebelum melakukan enkripsi pesan.
5. Pesan, berfungsi untuk memasukkan pesan yang akan di enkripsi.
6. Tombol enkripsi, berfungsi untuk memproses enkripsi pesan.
7. Hasil, berfungsi untuk menampilkan hasil proses dari enkripsi pesan.

8. Tombol kirim, berfungsi untuk mengirimkan pesan.

III.5.4. Rancangan *Form* Hasil Denkripsi

Berikut ini adalah rancangan *form* hasil dekripsi yang dapat lihat pada gambar III.9 di bawah ini.



Gambar III.9. *Form* Hasil Dekripsi

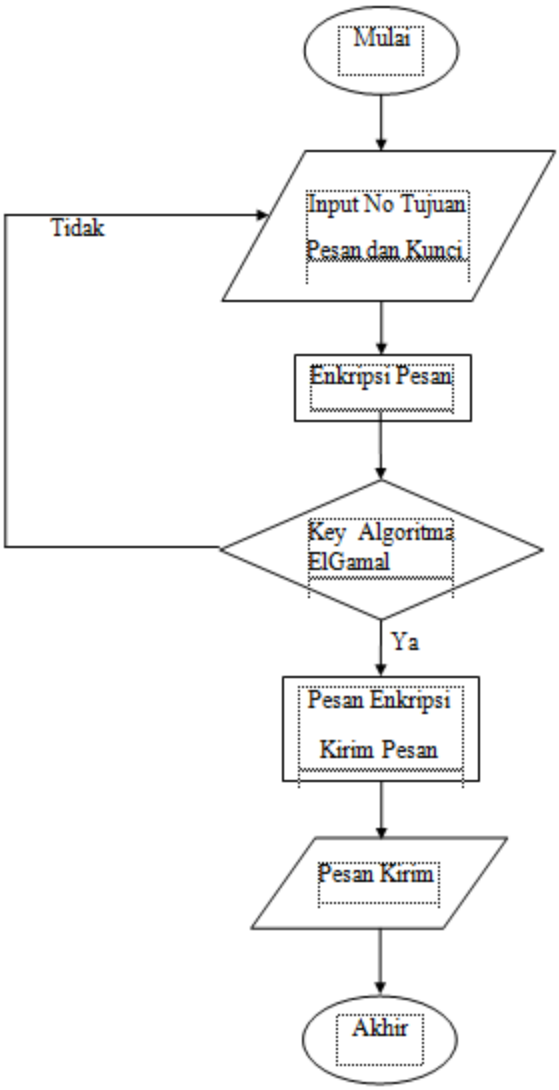
Pada desain *menu* kotak masuk di aplikasi untuk keamanan data pesan singat ini dapat dijelaskan sebagai berikut :

1. No pengirim, berfungsi untuk informasi no pengirim pesan.
2. Pesan, berfungsi untuk menampilkan pesan enkripsi.
3. Kunci p, berfungsi menginputkan kunci publik untuk melakukkan dekripsi pesan.

4. Kunci x, berfungsi menginputkan kunci privat untuk melakukan dekripsi pesan.
5. Tombol dekripsi, berfungsi untuk memproses dekripsi pesan.
6. Hasil, berfungsi untuk menampilkan hasil proses dari dekripsi pesan.
7. Tombol balas, berfungsi untuk membalas pesan.

III.6. *Flowchart* Enkripsi

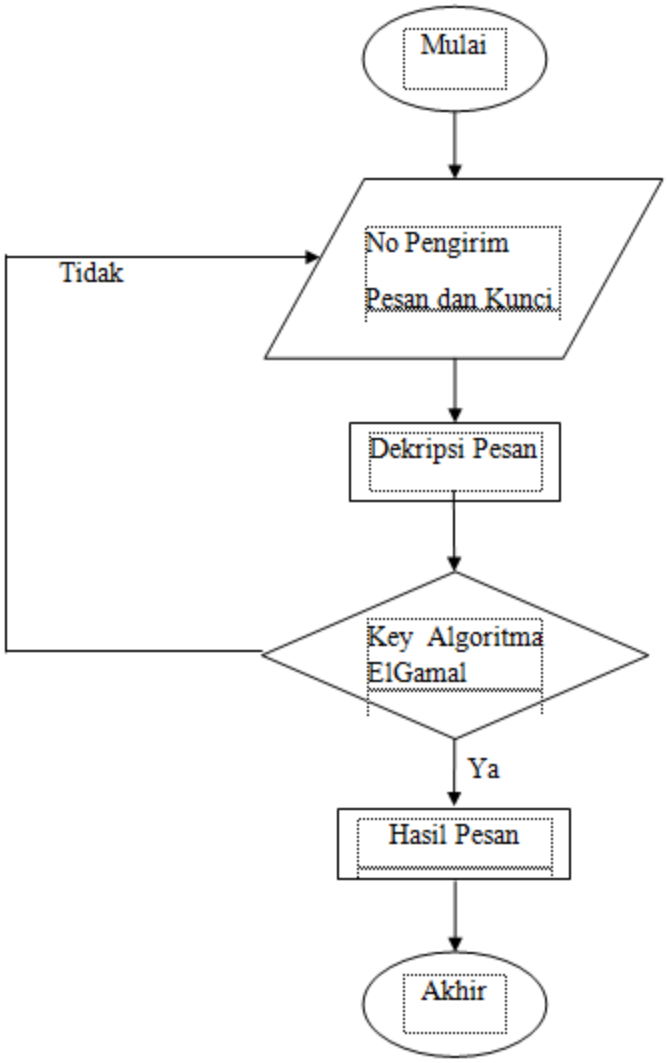
Flowchart ini dibuat untuk menjelaskan proses jalannya enkripsi pada program, seperti pada gambar III.10 di bawah ini.



Gambar III.10. *Flowchart* Enkripsi

III.7. *Flowchart* Dekripsi

Flowchart ini dibuat untuk menjelaskan proses jalannya dekripsi pada program, seperti pada gambar III.11 di bawah ini.



Gambar III.11. *Flowchart* Dekripsi