BAB III

ANALISA DAN PERANCANGAN

III.1. Analisa Masalah

Handphone merupakan salah satu bentuk teknologi yang perkembangannya cukup tinggi dan merupakan suatu media elektronik yang memegang peranan sangat penting dalam perkembangan teknologi saat ini, serta terus menerus mendominasi berbagai proses kerja atau penyampaian dalam proses belajar agar dapat lebih mudah dipahami. Perkembangan teknologi *handphone* juga harus diikuti dengan system keamanan *File*, dengan semakin banyaknya manusia yang menggunakan *File* dihandphone maka *File* akan dapat di baca oleh orang lain tanpa ada persetujuan dari pemilik *File* yang sebenarnnya, maka dari itu diperlukan system keamanan yang lebih dari biasanya

Ada beberapa cara melakukan pengamanan data dalam sebuah *file* adalah kriptografi. Dalam kriptografi, data yang sangat rahasia akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan isitilah *plaintext*, dan setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini akan berubah menjadi *ciphertext*.

III.2. Algoritma Vernam Cipher

Algoritma Vernam Cipher atau *One Time Pad* (OTP) merupakan algoritma berjenis *symetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara stream cipher yang berasal dari hasi *XOR* antara bit plaintext dan bit key. Pada metode ini plain text diubah kedalam kode ASCII dan kemudian dikenakan operasi *XOR* terhadap kunci yang sudah diubah ke dalam kode ASCII.

III.2.1. Proses Enkripsi Vernam Chiper

Enkripsi data merupakan bagian awal dari proses pengamanan data. Dalam proses enkripsi ini data ang asli akan dilakukan proses pengacakan dengan algoritma yang sudah ditentukan, adapun proses enkripsi pada Vernam Chiper dapat dilakukan dengan menggunakan rumus dibawah ini :

C(i) = P(i) XOR K(i).....(1)

Dalam hal ini :

C = Chiper Teks

P = Plain Teks

K = Kunci

I = index karakter

III.2.2. Enkripsi

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi, data kita disandikan (encrypted) dengan mengunakan sebuah kunci (key). Untuk membuka (men-decrypt) data tersebut, juga digunakan kunci yang dapat sama dengan kunci untuk mengenkripsi (privat key) atau dengan kunci yang berbeda (public key)

Keamanan dari enkripsi bergantung pada beberapa factor. Pertama, algoritma enkripsi harus cukup kuat sehingga sulit untuk men-decrypt cipher text dengan dasar cipher text tersebut. Lebih jauh lagi, keamanan dari algoritma enkripsi bergantung pada kerahasiaan dari kuncinya bukan algoritmanya, yaitu dengan asumsi bahwa adalah sangat tidak praktis untuk men-deycrypt informasi dengan dasar chipper text dan pengetahuan tentang algoritma dekripsi atau enkripsi. Atau dengan kata lain, kita tidak perlu menjaga kerahasiaan dari algoritma tetapi cukup dengan kerahasiaan kuncinya. Gambar ini digunakan untuk menerangkan proses enkripsi dalam bentuk Flowchart yang gambarnya seperti gambar III.1

Gambar III.1. Proses Enkripsi One Time Pad

Keterangan :

1. Input Plain Teks, Kunci
2. Ambil Jumlah Karakter Kunci
3. Ubah Kunci Menjadi Ascii

4. Ubah Setiap Karakter Plain Teks Menjadi Ascii
5. Lakukan Perhitungan Untuk mencari Enkripsi dengan menggunakan rumus Enc(i) = = C(i) XOR K(i)
6. Ubah Enc(i) Menjadi Char
7. Selesai

III.2.3. Dekripsi

Dekripsi digunakan untuk mengembalikan data-data atau informasi sehingga dapat dibaca oleh orang yang berhak. Dengan dekripsi, data dikembalikan kedalam bentuk semula sehingga dapat dibaca dengan baik, adapun flowchar enkripsi dapat dilihat seperti gambar III.2

Gambar III.2. Proses Dekripsi One Time Pad

Keterangan :

1. Input Chiper Teks, Kunci
2. Ambil Jumlah Karakter Kunci
3. Ubah Kunci Menjadi Ascii
4. Ubah Setiap Karakter Chiper Teks Menjadi Ascii

5. Lakukan Perhitungan Untuk mencari Dekripsi dengan menggunakan rumus Desc(i) = = C (i) XOR K(i)
6. Ubah Desc(i) Menjadi Char
7. Selesai

Pada penulisan skripsi ini akan dibahas analisa algoritma *Vernam Cipher*. Contonya adalah Pada saat akan mengirimkan file terhadap seseorang tersebut pastinya bersifat rahasia. Pada pembahasan ini *Vernam Cipher* akan mengenkripsi sehingga file tersebut aman. Di bawah ini akan di jelaskan contoh penggunaan algoritma *Vernam Cipher* pada sebuah .

Sebagai contoh : Sebuah **"RUMAH**" akan dienkripsi dengan kunci"**MEDAN"** dengan perhitungan sebagai berikut, maka akan diperoleh hasil sebagai berikut :

Tabel III.1. Ascii Pesan

Plain Teks	Ascii
R	82
U	85
M	77
A	65
H	72

Tabel III.2. Ascii Kunci

Teks Kunci	Ascii
M	77
E	69
D	68
A	65
N	78

Dari tabel diatas dapat disimpulkan sebagai berikut :

Tabel III.3. Contoh Perhitungan Enkripsi

Pesan	**82**	**85**	**77**	**65**	**72**
Kunci	**77**	**69**	**68**	**65**	**78**
Pesan XOR Kunci	**31**	**16**	**9**	**0**	**6**
Karakter	**US**	**DLE**	**TAB**	**NULL**	**ACK**

Maka akan menghasilkan karakter enkripsi : **US – DLE – TAB – NULL - ACK**

Untuk mendeskripsinya, maka dilakukan proses kebalikannya, yaitu.

Tabel III.4. Proses Dekripsi

Plain Teks/Char	Desimal
US	31
DLE	16
TAB	9
NULL	0
ACK	6

Tabel III.5. Ascii Kunci

Teks Kunci	Desimal
M	77
E	69
D	68
A	65
N	78

Tabel III.6. Hasil Perhitungan Dekripsi

Pesan	**31**	**16**	**9**	**0**	**6**
Kunci	**77**	**69**	**68**	**65**	**78**
Pesan XOR Kunci	**82**	**85**	**77**	**65**	**72**
Karakter	**R**	**U**	**M**	**A**	**H**

Dari tabel diatas dapat disimpulkan sebagai berikut :

Pesan Enkripsi **XOR** Kunci : **82 - 85 – 77 – 65 – 72**

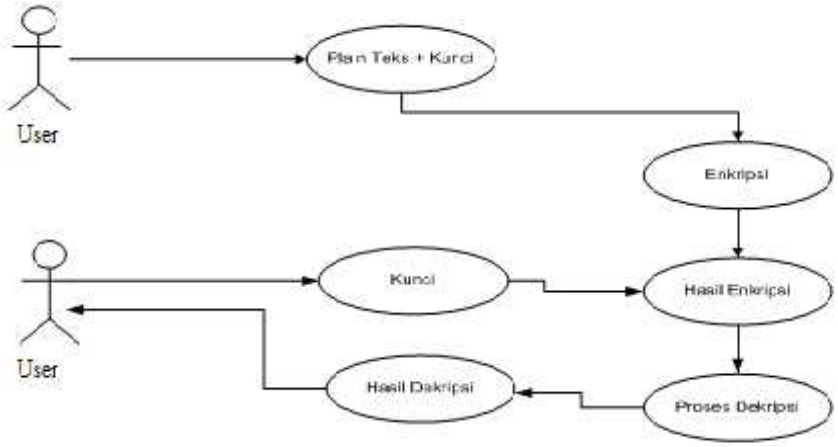
Lalu angka desimal tersebut di konversi kembali ke bentuk char, sehingga hasilnya seperti dibawah ini :

= **R - U - M - A - H**

III.3. UML

Prosedur sistem akan digambarkan dengan menggunakan 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 atau pelaku yang terlibat dalam sistem adalah sebagai berikut :

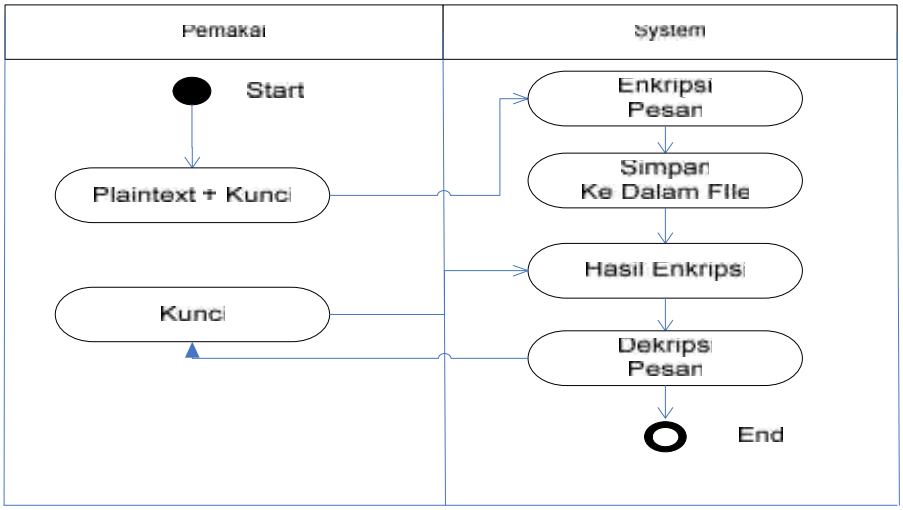
III.3.1. Diagram *Use Case*



Gambar III.3. Diagram *Use Case* Aplikasi

III.3.2. Diagram *Activity*

Activity diagram adalah teknik untuk menggambarkan logika prosedural, proses bisnis, dan jalur kerja. Dalam beberapa hal, diagram ini memainkan peran mirip sebuah diagram alir, tetapi perbedaan prinsip antara diagram ini dan notasi diagram alir adalah diagram ini mendukung behavior paralel.



Gambar III.4. Diagram *Activity*

III.4. Perancangan Program

Rancangan Dialog (user interface) meliputi rancangan input dan output. Rancangan input meliputi rancangan dialog login sistem, menu utama, rancangan memperbaharui data dan rancangan output.

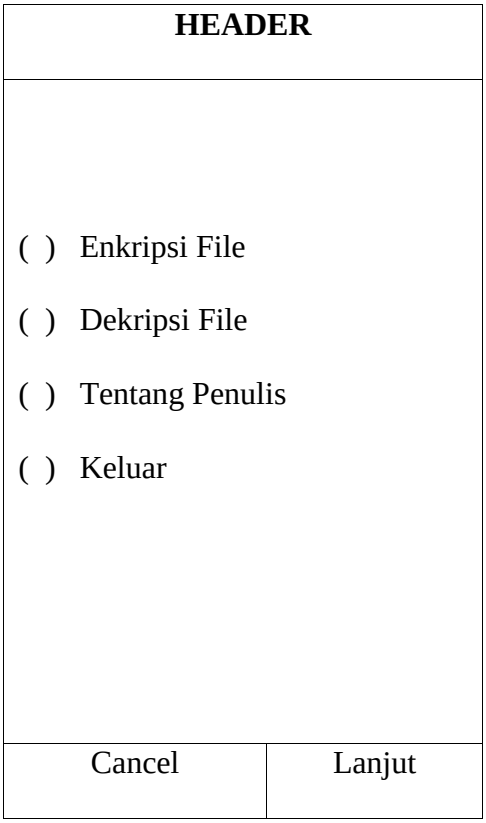
III.4.1. Rancangan Awal Pembukaan Program

Gambar ini dibuat untuk menampilkan rancangan awal ketika program pertama kali dibuka. Yang dapat dilihat seperti gambar III.5

Gambar III.5. Halaman Pembuka

III.4.2. Rancangan Menu Pilihan

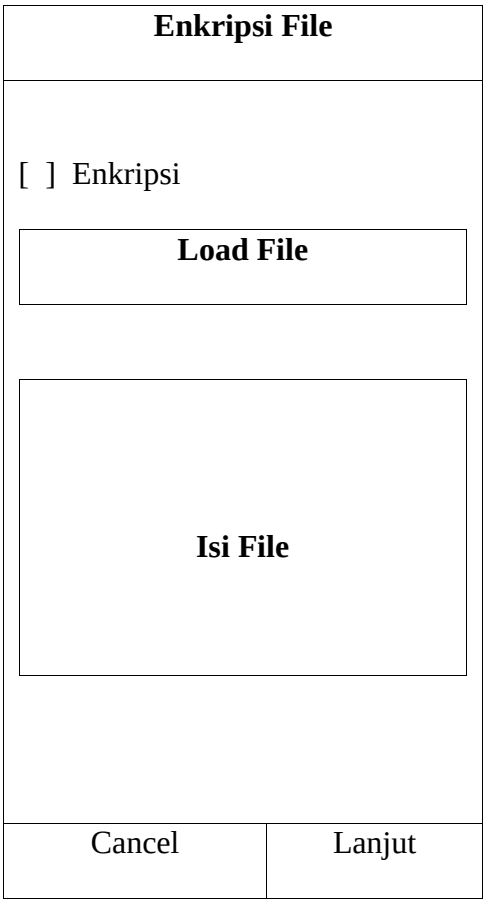
Gambar ini dibuat untuk menampilkan menu pilihan yang disediakan oleh sistem, yang dapat dilihat seperti gambar III.6



Gambar III.6. Halaman Menu Pilihan

III.4.3. Rancangan Enkripsi File

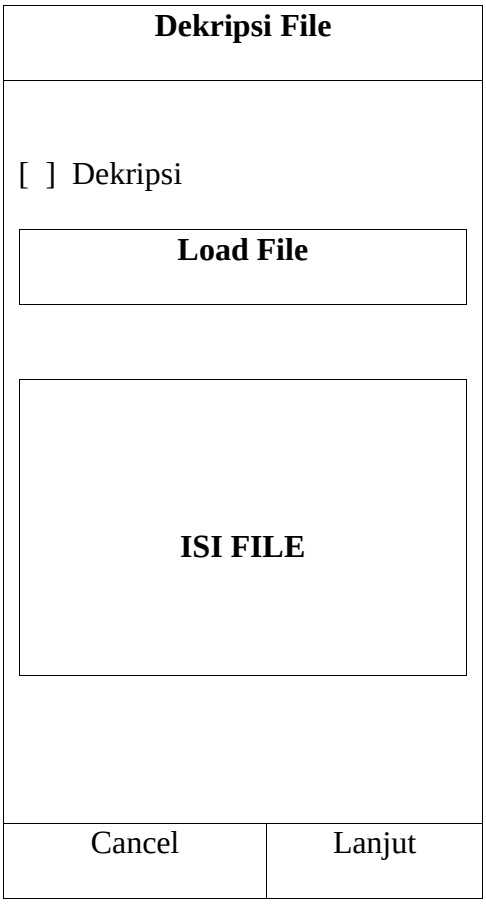
Gambar ini dibuat untuk Enkripsi File, yang dapat dilihat seperti gambar III.7



Gambar III.7. Halaman Enkripsi File

III.4.4. Rancangan Dekripsi File

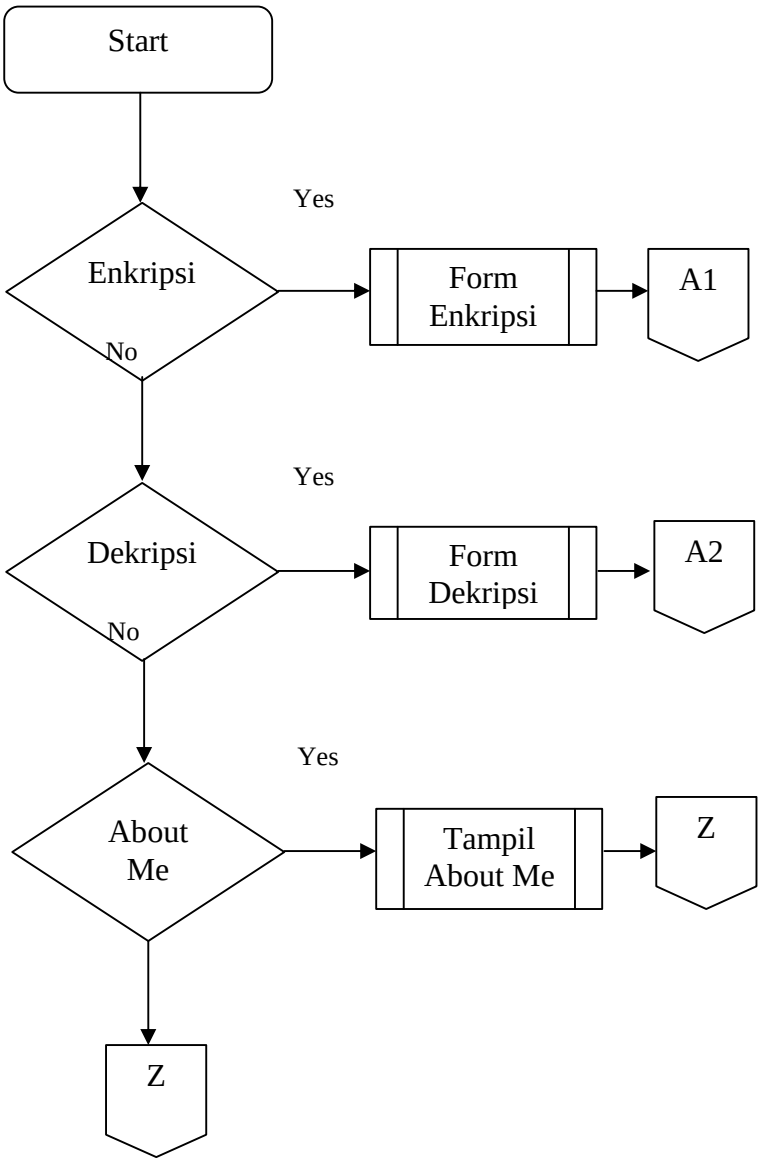
Gambar ini dibuat untuk membaca File yang sudah didekripsi, yang dapat dilihat seperti gambar III.8



Gambar III.8. Halaman Dekripsi File

III.5. Flowchart Menu Pilihan

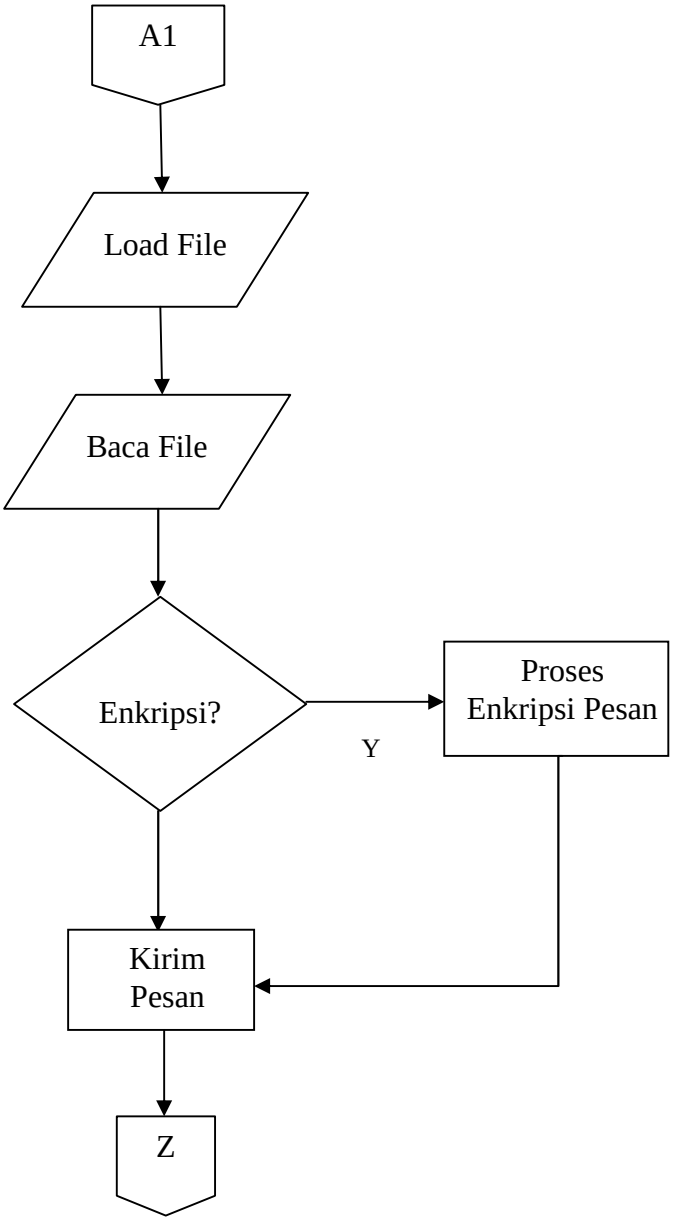
Flowchart ini digunakan untuk menerangkan proses jalannya menu pilihan pada program, seperti gambar III.9



Gambar III.9. *Flowchart Menu* Pilihan

III.6. *Flowchart Enkripsi File*

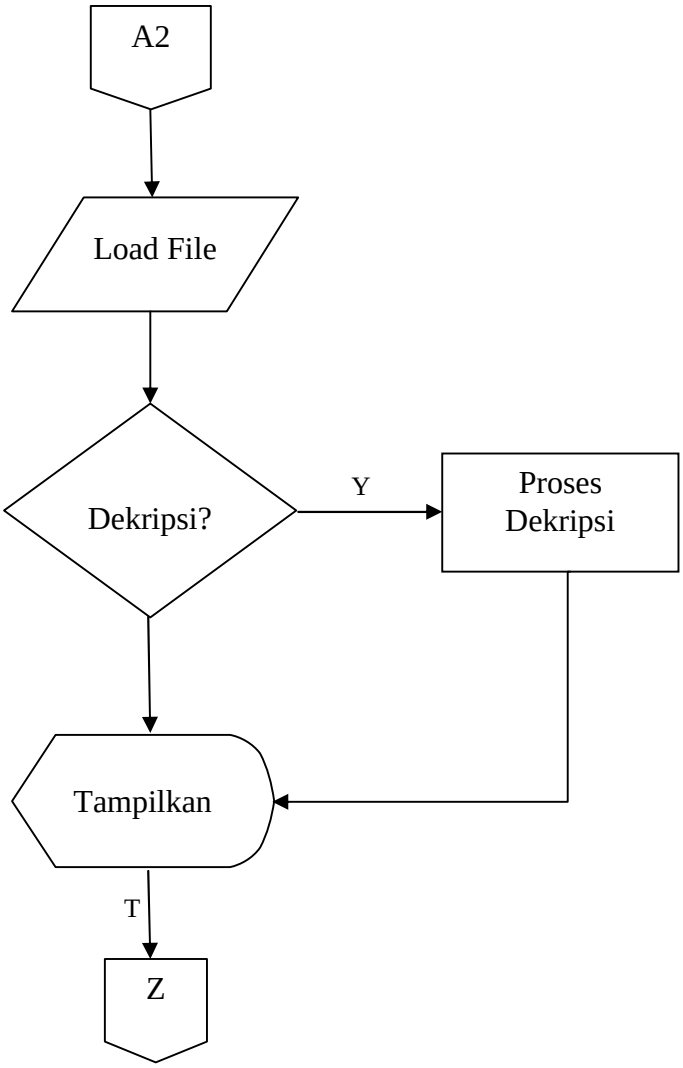
Flowchart ini digunakan untuk menerangkan proses jalannya enkripsi pesan pada program, seperti gambar III.10



Gambar III.10. ***Flowchart Enkripsi File***

III.7. Flowchart Dekripsi File

Flowchart ini digunakan untuk menerangkan proses jalannya pembacaan pesan pada program, seperti gambar III.11



Gambar III.11. ***Flowchart Dekripsi File***