BAB III
ANALISIS DAN DESAIN SISTEM

III.1. Analisis Masalah

Analisa terhadap suatu permasalahan memerlukan suatu analisa untuk menyelesaikan suatu permasalahan yang ada, keamanan merupakan salah satu hal klasik yang sangat penting dan harus dilakukan agar menjaga informasi atau data yang tidak dapat diketahui oleh pihak lain. Didalam proses perancangan aplikasi ini sebelumnya dilakukan beberapa pengamatan terhadap pentingnya melakukan proses enkripsi terhadap file dokumen word. Hal ini berkaitan dengan banyaknya penyalahgunaan file milik orang lain yang dipergunakan oleh pihak-pihak yang tidak bertanggung jawab demi meraih keuntungan pribadi. Mereka juga sering memodifikasi isi file sehingga pihak yang membutuhkan file tersebut tidak dapat menemukan apa yang dicari dan sering juga terjadinya.

Berdasarkan analisa di atas maka penulis telah melakukan evaluasi dari sistem yang sedang berjalan dan penulis menemukan kelemahan sistem yang ada. Dengan demikian penulis memberikan suatu solusi pemecahan masalah yang diharapkan dapat mengatasi kelemahan sistem yang ada. Adapun solusi yang ditawarkan adalah membangun aplikasi pengamanan file dokumen word menggunakan algoritma massey-omura.

III.2. Penerapan Metode Massey-Omura

Tahap penerapan metode dilakukan untuk mulai dari proses perancangan, evaluasi dan memperbaiki sistem sesuai dengan kebutuhan, agar sistem yang sedang dibuat dapat dimanfaatkan secara optimal. Aplikasi ini menggunakan metode Massey-Omura, metode ini akan digunakan untuk mengamankan file dokumen word yang ada. Strategi yang digunakan pertama harus mempunyai plaintext untuk mengenkripnya agar mendapatkan chipertext. Untuk proses dekripsinya dimana ciphertext yang didapat tadi akan didekrip kembali agar menghasilkan plaintext awal.

III.2.1. Perhitungan Manual Massey-Omura

Dalam perancangan sebuah sistem diperlukan analisis untuk menentukan kebutuhan sistem. Dengan adanya analisis sistem, sistem yang dirancang diharapkan akan lebih baik dan memudahkan dalam pengembangan sistem selanjutnya. Tujuan dari analisis sistem ini sendiri adalah untuk membantu pemodelan rancang bangun sistem yang nantinya akan diimplementasikan dalam bentuk nyata. Sebagai contoh, A ingin mengirimkan pesan “ILKOM” kepada B. A menggunakan eA = 89 dan B menggunakan eB = 67. Dengan begitu, maka proses yang akan terjadi adalah sbb :

Pilih bilangan prima p dengan menggunakan Lehmann *Prime Generator*. Pengecekan bilangan prima yang dibangkitkan adalah dengan menggunakan Lehmann *Prime Generator*. Misalnya: Bangkitkan bilangan prima 101, dan

dilakukan pengecekan apakah bilangan ini merupakan bilangan prima atau bukan dengan carasebagai berikut:

a. Pilih sebuah bilangan a dimana 1< a < 101.

b. Misalkan nilai *random* yang terpilih untuk nilai a adalah 2.

c. Hitung nilai L (*Legendre*), dimana $L \equiv a^{(p-1)/2} \bmod p$, dimana p =101.

$L \equiv a^{(p-1)/2} \bmod p^{(101-1)/2}$

$\equiv 2^{(101-1)/2} \bmod 101$

$\equiv 2^{50} \bmod 101$

$\equiv 1125899906842624 \bmod 101 \equiv -1$

d. Dikarenakan 101 memiliki 3 digit, yaitu1, 0 dan 1, maka pembuktian nilai 101 merupakan prima adalah dicari sebanyak 3kali. Maka pilih kembali nilai a. misal a= 3, maka

$L \equiv a^{(p-1)/2} \bmod p$

$\equiv 3^{(101-1)/2} \bmod 101$

$\equiv 3^{50} \bmod 101$

$\equiv 717897987691852588770249 \bmod 101 \equiv -1$

A = 4, maka

$L \equiv a^{(p-1)/2} \bmod p$

$\equiv 4^{(101-1)/2} \bmod 101$

$\equiv 4^{50} \bmod 101$

$\equiv 1267650600228224014967032053 76 \bmod 101 \equiv 1$

Maka benar bahwa 101 merupakan bilangan prima.

e. Enkripsi pesan dengan menggunakan algoritma Massey-Omura.

Karakter“I”dalam ASCII bernilai 73,

Karakter“L”dalam ASCII bernilai 76,

Karakter “K”dalam ASCII bernilai75,

Karakter “O”dalam ASCII bernilai79,

Karakter “M”dalam ASCII bernilai77,

Kemudian diketahui bahwa untuk mencari cipher teks maka kita menggunakan rumus: $C1=m^{eA} \bmod p$

Dimana eA telah ditentukan sebelumnya bernilai 89 dan p bernilai 101, sehingga:

$C1=m^{eA} \bmod p = 73^{89} \bmod 101 = 59$

$C1=m^{eA} \bmod p = 76^{89} \bmod 101 = 77$

$C1=m^{eA} \bmod p = 75^{89} \bmod 101 = 11$

$C1=m^{eA} \bmod p = 79^{89} \bmod 101 = 19$

$C1=m^{eA} \bmod p = 77^{89} \bmod 101 = 47$

Plainteks“Ilkom”setelah dienkripsi dengan Massey-Omura menjadi “5977111947”. Cipher teks ini kemudian dikirim ke B.

f. Penerapan Three Pass Protocol untukmendapatkan plain teks.

Setelah B meneriman pesan dari A yang merupakan cipherteks, B tidak dapat langsungmendekripsi pesan tersebut untuk mendapatkan plainteksnya. Tetapi, B harus mengenkripsi cipherteks tersebut dengan rumus

$C_2=C_1^{eB} \bmod p$

Dimana eB bernilai 67 dan p bernilai 101,sehingga:

$C_2=C_1^{eB} \bmod p = 59^{67} \bmod 101 = 86$

$C_2=C_1^{eB} \bmod p = 77^{67} \bmod 101 = 96$

$C_2=C_1^{eB} \bmod p = 11^{67} \bmod 101 = 12$

$C_2=C_1^{eB} \bmod p = 19^{67} \bmod 101 = 68$

$C_2=C_1^{eB} \bmod p = 47^{67} \bmod 101 = 23$

Cipherteks“5977111947”setelah dienkripsi lagi oleh B menjadi “8696126823”. Cipherteks ini kemudian dikirim ke A. Kemudian A mendekripsi cipherteks tersebut dengan rumus:

$C_3=C_2^{dA} \bmod p$

Dimana $dA \equiv eA^{-1} \pmod{p-1}$, sehingga:

$C_3=C_2^{dA} \bmod p = 86^{9} \bmod 101 = 46$

$C_3=C_2^{dA} \bmod p = 96^{9} \bmod 101 = 13$

$C_3=C_2^{dA} \bmod p = 12^{9} \bmod 101 = 18$

$C_3=C_2^{dA} \bmod p = 68^{9} \bmod 101 = 92$

$C_3=C_2^{dA} \bmod p = 23^{9} \bmod 101 = 96$

Dimana $dB \equiv eB^{-1} \pmod{p-1}$, sehingga:

$C4=C3^{dE} \bmod p = 46^{3} \bmod 101 = 73$

$C4=C3^{dE} \bmod p = 13^{3} \bmod 101 = 76$

$C4=C3^{dE} \bmod p = 18^{3} \bmod 101 = 75$

$C4=C3^{dE} \bmod p = 92^{3} \bmod 101 = 79$

$C4=C3^{dE} \bmod p = 96^{3} \bmod 101 = 77$

Nilai 73 dalam kode ASCII adalah karakter I

Nilai 76 dalam kode ASCII adalah karakter L

Nilai 75 dalam kode ASCII adalah karakter K

Nilai 79 dalam kode ASCII adalah karakter O

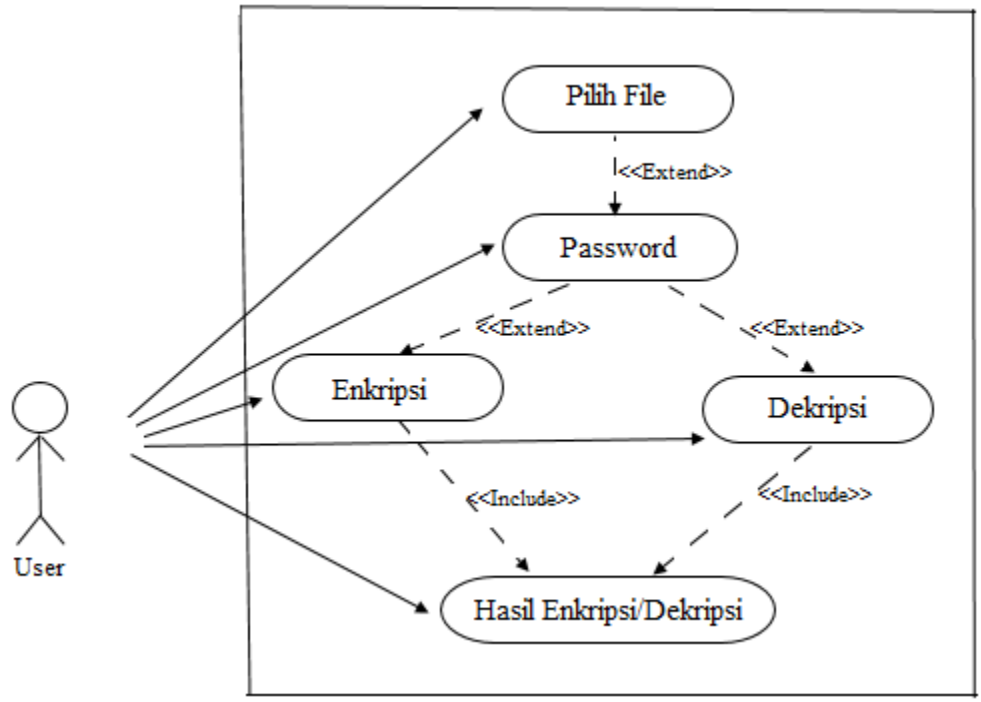
Nilai 77dalam kode ASCII adalah karakter M

Setelah B mendekripsi pesan tersebut, maka diketahuilah bahwa pesan yang dikirim oleh A adalah “ILKOM”.

III.3. Desain Sistem

III.3.1. *Usecase Diagram*

Secara garis besar, proses sistem yang akan dirancang digambarkan dengan *usecase diagram* yang terdapat pada gambar berikut:



Gambar III.1. *Usecase Diagram*

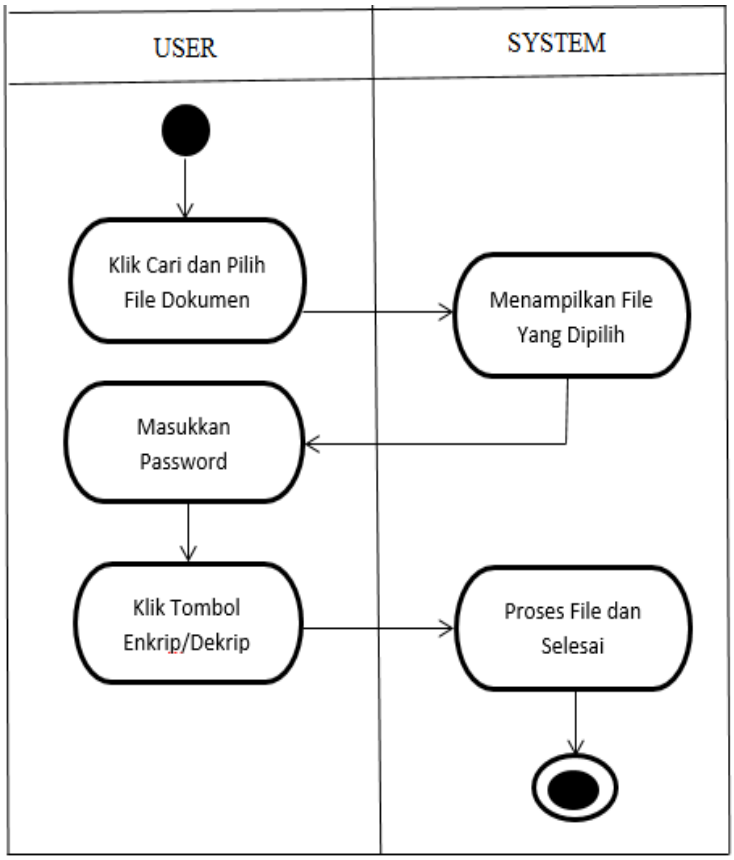
Dari gambar *usecase diagram* diatas menjelaskan bahwa user atau pengguna dapat masuk kedalam aplikasi sederhana ini, dimana user dapat berhubungan dengan system dan hal yang berhubungan dengan user didalam system.

III.3.2. *Activity Diagram*

Diagram aktivitas menggambarkan suatu urutan proses yang terjadi pada sistem dari dimulainya aktivitas hingga aktivitas berhenti. *Activity diagram* hampir mirip dengan diagram *flowchart*. *Activity diagram* merupakan salah satu cara untuk memodelkan event-event yang terjadi dalam suatu *usecase*

III.3.2.1. *Activity Diagram* Pilih File

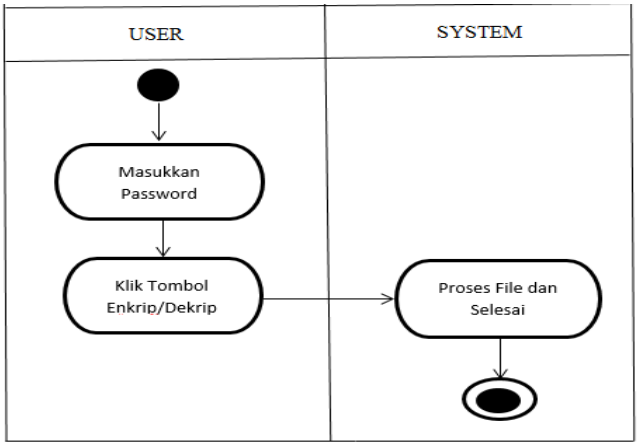
Pada *activity diagram* pilih file menjelaskan informasi atau data pemilihan pada file dokumen word. Adapun *activity diagram* pilih file tersebut dapat dilihat pada gambar berikut:



Gambar III.2. *Activity Diagram* Pilih File Dokumen Word

III.3.2.2. *Activity Diagram* Password

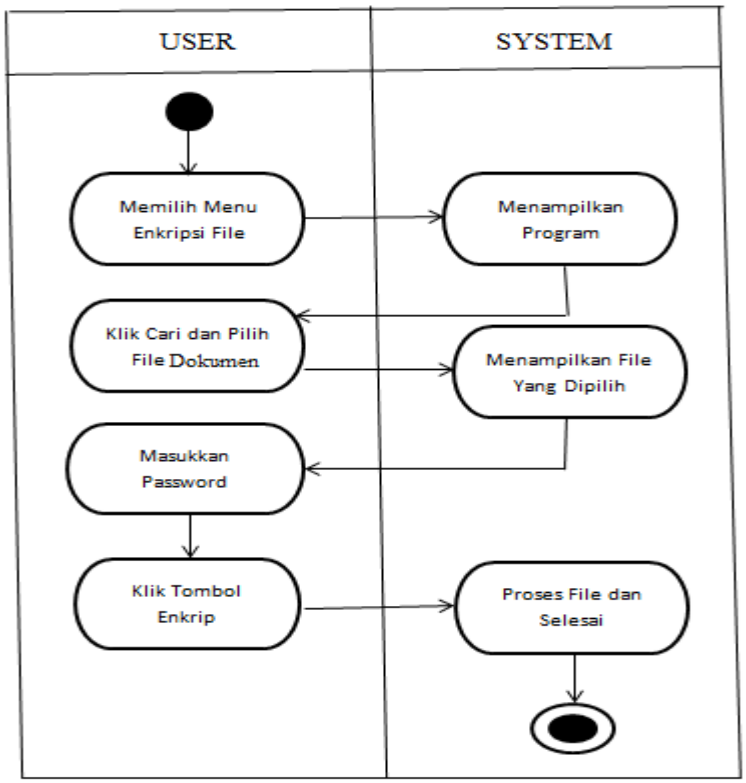
Pada *activity diagram* password menjelaskan bahwa informasi atau cara memasukan password. Adapun *activity diagram* tersebut dapat dilihat pada gambar berikut:



Gambar III.3. *Activity Diagram* Password

III.3.2.3. *Activity Diagram* Enkripsi

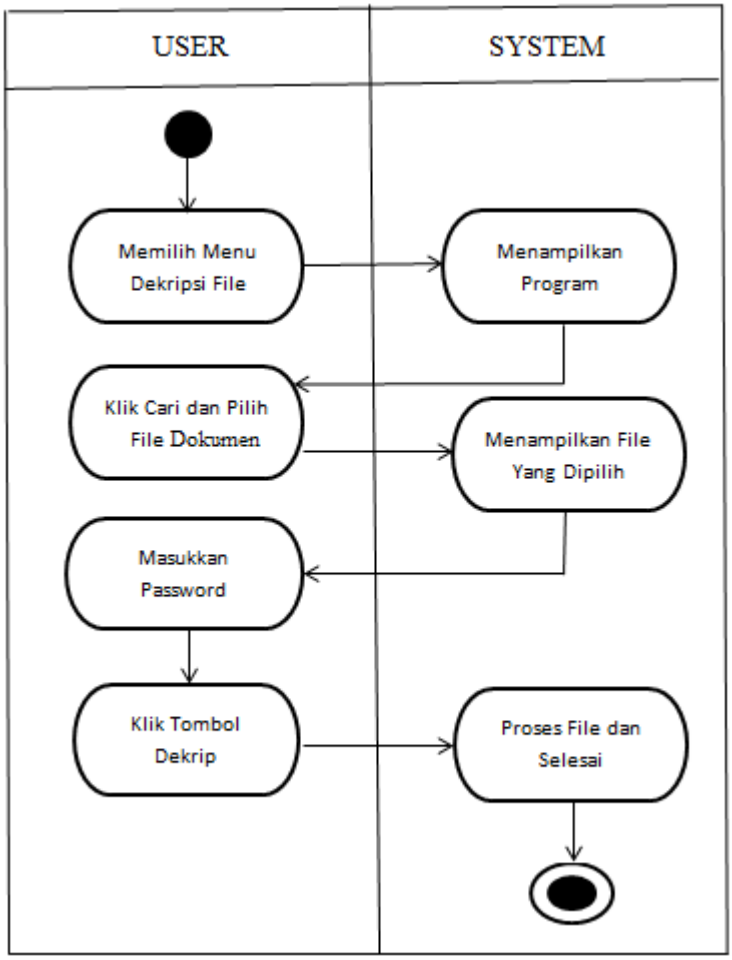
Pada *activity diagram* enkripsi menjelaskan bahwa informasi atau data enkripsi dokumen word. Adapun *activity diagram* dengan enkripsi tersebut dapat dilihat pada gambar berikut:



Gambar III.4. *Activity Diagram* Enkripsi File Dokumen Word

III.3.2.4. *Activity Diagram* Deskripsi File Dokumen Word

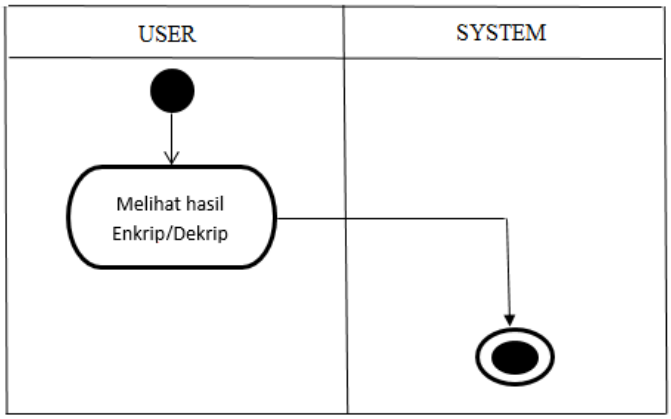
Pada *activity diagram* deskripsi file dokumen word menjelaskan bahwa informasi atau data deskripsi dokumen word. Adapun *activity diagram* deskripsi tersebut dapat dilihat pada gambar berikut:



Gambar III.5. *Activity Diagram* Deskripsi File Dokumen Word

III.3.2.5. *Activity Diagram* Hasil

Pada *activity diagram* hasil menjelaskan bahwa user atau pengguna hanya melihat hasil yang telah di enkrip maupun di dekrip. Adapun *activity diagram* tersebut dapat dilihat pada gambar berikut:

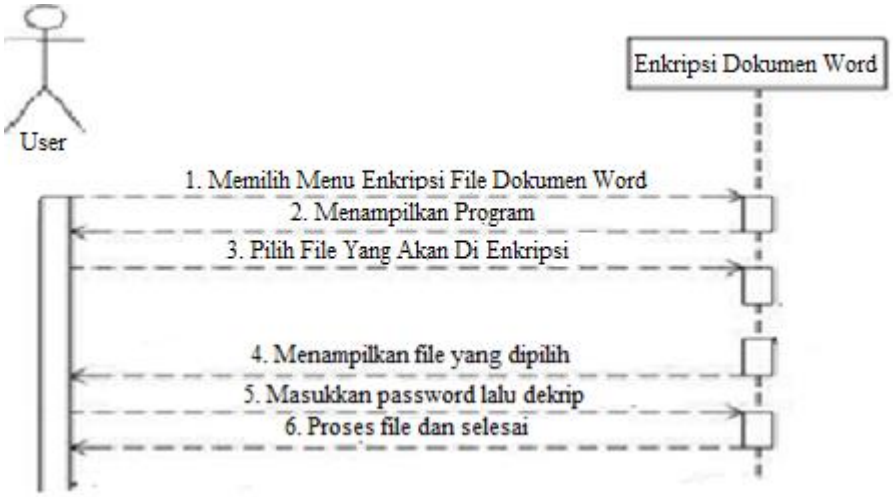


Gambar III.6. *Activity Diagram* Hasil

III.3.3. *Sequence Diagram*

III.3.3.1. *Sequence Diagram* Enkripsi File Dokumen Word

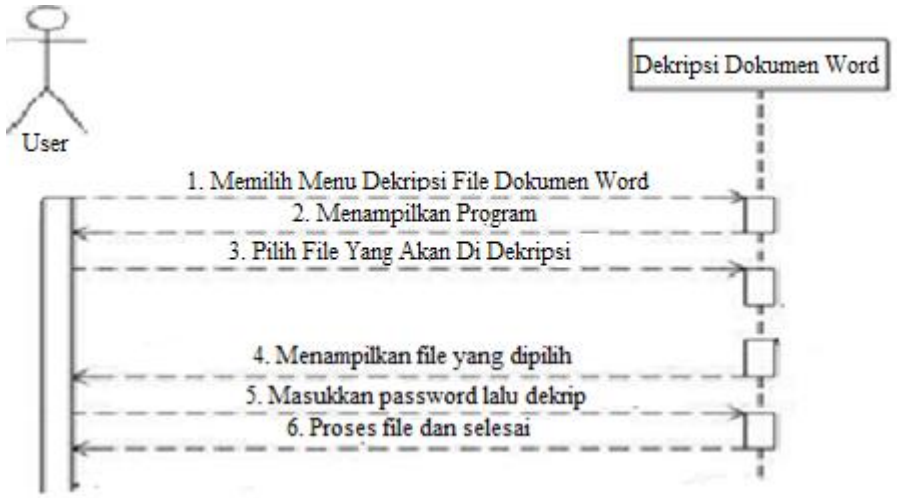
Pada *sequence diagram* enkripsi file dokumen word menjelaskan bahwa informasi atau data enkripsi dokumen word. Adapun *sequence diagram* dengan enkripsi tersebut dapat dilihat pada gambar berikut:



Gambar III.7. *Sequence Diagram* Enkripsi File Dokumen Word

III.3.3.2. *Sequence Diagram* Dekripsi File Dokumen Word

Pada *sequence diagram* dekripsi file dokumen word menjelaskan bahwa informasi atau data dekripsi dokumen word. Adapun *sequence diagram* dengan dekripsi tersebut dapat dilihat pada gambar berikut:

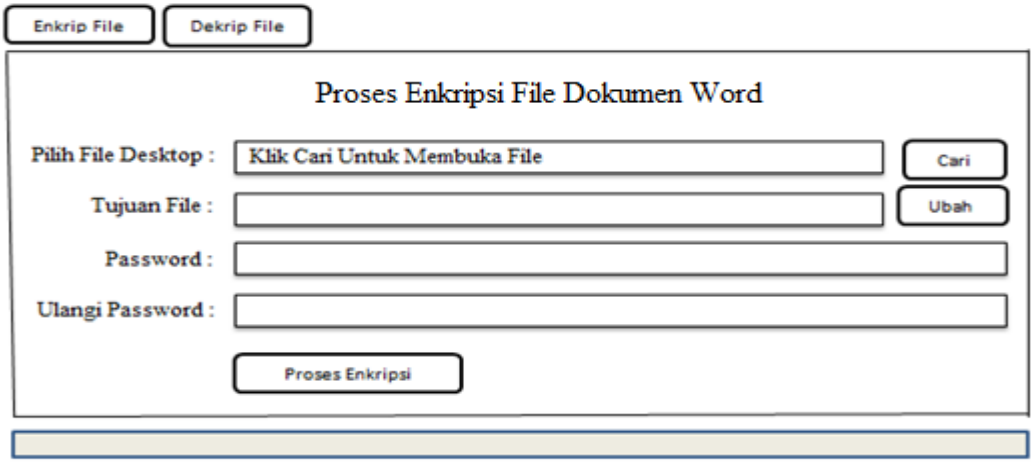


Gambar III.8. *Sequence Diagram* Dekripsi File Dokumen Word

III.4. Desain User Interface

III.4.1. Rancangan Form Enkripsi

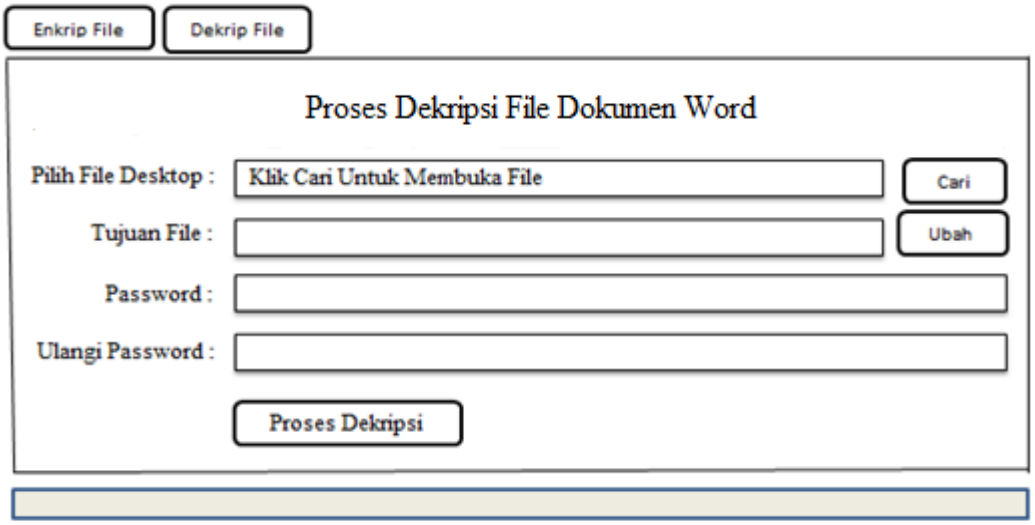
Form enkripsi berfungsi untuk menampilkan form enkripsi aplikasi pengamanan file dokumen word, rancangan ini dapat dilihat dari gambar berikut:



Gambar III.9. Desain Tampilan Form Enkripsi

III.4.2. Rancangan Form Dekripsi

Form dekripsi berfungsi untuk menampilkan form dekripsi aplikasi pengamanan file dokumen word, rancangan ini dapat dilihat pada gambar berikut:



Gambar III.10. Desain Tampilan Form Deskripsi