BAB III

ANALISA DAN DESAIN SISTEM

III.1. Analisa Masalah

Kebutuhan manusia akan perangkat informasi dan komunikasi seakan menjadi kebutuhan yang tidak terpisahkan dalam kehidupan. Pemakaian *file* yang menjadi salah satu kebutuhan yang sering digunakan tetapi masih kurangnya pengamanan data *file* dengan enkripsi. Masih sedikitnya perancangan aplikasi penyandian file menggunakan algoritma *Blowfish*. Hal ini sangat tergantung pada Ilmu pengetahuan yang saat ini mengalami kemajuan sehingga banyak pengguna mengetahui cara membobol suatu *file*.

III.1.1. Analisa Perangkat Perancangan

Pada perancangan ini penerapan perangkat sebagai pendukung perancangan menggunakan beberapa perangkat yang dapat dijelaskan sebagai berikut :

1. Perangkat Lunak (*Software*), perangkat lunak merupakan perangkat yang digunakan untuk mendesain dan melakukan pemrograman, yang terdiri dari.
   a. *Operating System Windows Seven*.
   b. PHP sebagai bahasa pemrograman.
2. Perangkat Keras (*Hardware*), perangkat keras merupakan perangkat yang digunakan untuk menjalankan dan implementasi aplikasi yang dirancang, yang terdiri dari.
   a. Komputer yang setara dengan *Intel pentium* 4.

b. *Mouse, Keyboard,* dan *Monitor.*

III.1.2. Analisa Metode Yang Digunakan

Blowfish diciptakan oleh seorang Cryptanalyst bernama Bruce Schneier, Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan cache data yang besar). Blowfish merupakan algoritma yang tidak dipatenkan dan licensefree, dan tersedia secara gratis untuk berbagai macam kegunaan.

Dalam penerapannya sering kali algortima ini menjadi tidak optimal. Karena strategi implementasi yang tidak tepat. Algoritma Blowfish akan lebih optimal jika digunakan untuk aplikasi yang tidak sering berganti kunci, seperti jaringan komunikasi atau enkripsi file otomatis. Selain itu, karena algoritma ini membutuhkan memori yang besar, maka algoritma ini tidak dapat diterapkan untuk aplikasi yang memiliki memori kecil seperti *smart card*. Panjang kunci yang digunakan, juga mempengaruhi keamanan penerapan algoritma ini.

Perhitungan manual ini disajikan untuk mempermudah pemahaman terhadap algoritma yang dibahas yaitu Blowfish. Pertama-tama adalah mendefinisikan P-array dan S-Box. P array dari algoritma Blowfish adalah sebagai berikut :

P[1] =H243F6A88 P[2] =85A308D3 P[3] =13198A2E P[4]=03707344P

[5] =A4093822 P[6] =299F31D0 P[7] =082EFA98 P[8] =EC4E6C89

P[9] =452821E6 P[10]=38D01377 P[11]=BE5466CF P[12]=34E90C6C

P[13]=C0AC29B7 P[14]=C97C50DD P[15]=3F84D5B5 P[16]=B5470917

P[17]=9216D5D9 P[18]=8979FB1B

Misalkan M adalah plaintext dan K adalah kunci.

M = TERAKHIR dalam bentuk hexa = 544552414B484952

K = SECURITY dalam bentuk hexa = 7365637572697479

Setelah key dimasukkan kemudian didapat P-array sebagai berikut :

P[1] =78C14389 P[2] =EBFC7DA1 P[3] =D07E9EFE P[4] =860E5E50

P[5] =E3BC4595 P[6] =6E85076A P[7] =D1CFF191 P[8] =F837889A

P[9] =ED545578 P[10]=DB83AF7 P[11]=FD2183BB P[12]=E94B787A

P[13]=ED545578 P[14]=327A140A P[15]=688FC31C P[16]=530429F4

P[17]=4E734A41 P[18]=1B510052

Kemudian M dibagi menjadi 2 bagian, bagian kiri (ML) dan bagian kanan (MR) yaitu :

ML=TERA (54455241) dan MR=KHIR (4B484952)

Iterasi 1 :

ML= ML⊕P1

=54455241⊕78C14389 = 2C8411C8

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = 2C = 00101100 = 32+8+4=44, S1,44 = 1141E8CE

b = 84 = 10000100 = 128+4=132, S2,132= EAC31F66

c = 11 = 00010001 = 16+1=17, S3,17 = 4D95FC1D

d = C8 = 11001000 = 128+64+8=200, S4,200 = 0FE3F11D

=[(1141E8CE + EAC31F66 mod 2^{32})⊕4D95FC1D]+0FE3F11D mod 2^{32}

=[(FC050834 mod 2^{32})⊕4D95FC1D] + 0FE3F11D mod 2^{32}

=[B190F429] + 0FE3F11D mod 2^{32}

= C174E546

M R= F(M L)⊕M R = C174E546⊕4B484952 = 8A3CAC14

Swap atau tukar ML dan MR, ML = 8A3CAC14 dan MR= 2C8411C8

Iterasi 2 :

ML= ML⊕P2

=8A3CAC14⊕EBFC7DA1 = 61C0D1B5

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = 61 = 01100001 = 64+32+1=97, S1,97= E06F75D8

b = C0 = 1100000 = 128+64=192, S2,192= EE7C3C73

c = D1 = 11010001 = 128+64+16+1=209, S3,209= DCB7DA83

d = B5 = 10110101 = 128+32+16+4+1=181, S4,181= 5366F9C3

=[(E06F75D8+EE7C3C73 mod 2^{32})⊕DCB7DA83]+5366F9C3 mod 2^{32}

=[(CEEBB24B mod 2^{32})⊕DCB7DA83] + 5366F9C3 mod 2^{32}

=[125C68C8] + 5366F9C3 mod 2^{32}

= 65C3628B

MR= F(ML)⊕MR

= 65C3628B⊕2C8411C8 = 49477343

Swap atau tukar ML dan MR, ML= 49477343 dan MR = 61C0D1B5

Iterasi 3 :

ML= ML⊕P3

=49477343⊕D07E9EFE = 9939EDBD

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = 99 = 10011001 = 128+16+8+1=153, S1,153= 3E00DF82

b = 39 = 00111001 = 32+16+8+1=57, S2,57= A9446146

c = ED = 11101101 = 128+64+32+8+4+1=237, S3,237= 86E3725F

d = BD = 10111101 = 128+32+16+8+4+1=189, S4,189= 9F1F9532

=[(3E00DF82+ A9446146 mod 2^{32})⊕86E3725F]+ 9F1F9532 mod 2^{32}

=[(E74540C8 mod 2^{32})⊕86E3725F]+ 9F1F9532 mod 2^{32}

=[61A63297] + 9F1F9532 mod 2^{32}

= 00C5C7C9M

R= F(ML)⊕MR

= 00C5C7C9⊕61C0D1B5 = 6105167C

Swap atau tukar ML dan MR, ML= 6105167C dan MR= 9939EDBD

Iterasi 4 :

ML= ML⊕P4

= 6105167C⊕860E5E50 = E70B482C

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = E7 = 11100111 = 128+64+32+4+2+1=231, S1,231= 207D5BA2

b = 0B = 00001011 = 8+2+1=11, S2,11= 5664526C

c = 48 = 01001000 = 64+8=72, S3,72= 9029317C

d = 2C = 00101100 = 32+8+4=44, S4,44= EF5562E9

=[(207D5BA2+ 5664526C mod 2^{32})⊕9029317C]+ EF5562E9 mod 2^{32}

=[(76E1AE0E mod 2^{32})⊕9029317C]+ EF5562E9 mod 2^{32}

=[E6C89F72] + EF5562E9 mod 2^{32}

= E78E673B

MR= F(ML) ⊕MR

= E78E673B⊕9939EDBD = 7EB78A86

Swap atau tukar ML dan MR, ML= 7EB78A86 dan MR= E70B482C

Iterasi 5 :

ML= ML⊕P5

=7EB78A86⊕E3BC4595= 9D0BCF13

F(ML) =[(S1,a+ S2,bmod 2^{32})⊕S3,c] + S4,dmod 2^{32}, dimana :

a = 9D = 10011101 = 128+16+8+4+1=148, S1,148= AD0552AB

b = 0B = 00001011 = 8+2+1=11, S2,11= 5664526C

c = CF = 11001111 = 128+64+8+4+2+1=207, S3,207= A186F20F

d = 13 = 00010011 = 16+2+1=19, S4,19= C6A376D2

=[(AD0552AB + 5664526C mod 2^{32})⊕A186F20F]+ C6A376D2 mod 2^{32}

=[(0369A517 mod 2^{32})⊕A186F20F]+ C6A376D2 mod 2^{32}

=[A2EF5718] + C6A376D2 mod 2^{32}

= 6992CDEAM

R= F(ML)⊕MR

=6992CDEA⊕E70B482C = 8E9985C6

Swap atau tukar MLdan MR, ML= 8E9985C6 dan MR= 9D0BCF13

Iterasi 6 :

ML= ML⊕P6

=8E9985C6⊕6E85076A = E01C82AC

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = E0 = 11100000 = 128+64+32=224, S1,224= 57B8E0AF

b = 1C = 00011100 = 16+8+4=28, S2,28= 021ECC5E

c = 82 = 10000010 = 128+2=130, S3,130= CEDB7D9C

d = AC = 10101100 = 128+32+8+4=172, S4,172= 27D9459C

=[(57B8E0AF+021ECC5E mod 2^{32})⊕CEDB7D9C]+ 27D9459C mod 2^{32}

=[(59D7AD0D mod 2^{32})⊕CEDB7D9C]+ 27D9459C mod 2^{32}

=[970CD091] + 27D9459C mod 2^{32}

= BEE6162DM

R= F(ML) ⊕MR

= BEE6162D⊕9D0BCF13= 23EDD93E

Swap atau tukar ML dan MR, ML = 23EDD93E dan MR= E01C82AC

Iterasi 7 :

ML= ML⊕P7

=23EDD93E⊕D1CFF191 = F22228AF

F(ML) =[(S1,a+ S2,bb mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = F2 = 11110010 = 128+64+32+16+2=242, S1,242= BC9BC6E4

b = 22 = 00100010 = 32+2=34, S2,34= 52A0E286

c = 28 = 00101000 = 32+8=40, S3,40= 7AF4D6B6

d = AF = 10101111 = 128+32+8+4+2+1=175, S4,175= 55464299

=[(BC9BC6E4+52A0E286 mod 2^{32})⊕7AF4D6B6]+ 55464299 mod 2^{32}

=[(0F3CA96Amod 2^{32})⊕7AF4D6B6]+ 55464299 mod 2^{32}

=[75C87FDC] + 55464299 mod 2^{32}

= CB0EC275

MR= F(ML)⊕MR

= CB0EC275⊕E01C82AC = 2B1240D9

Swap atau tukar MLdan MR, ML= 2B1240D9 dan MR= F22228AF

Iterasi 8 :

ML= ML⊕P8

=2B1240D9⊕F837889A = D325C843

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = D3 = 11010011 = 128+64+16+2+1=211, S1,211= 93CC7314

b = 25 = 00100101 = 32+4+1=37, S2,37= 3E07841C

c = C8 = 11001000 = 128+64+8=200, S3,200= C4324633

d = 43 = 01000011 = 64+2+1=67, S4,67= 1F9F25CF

=[(93CC7314 +3E07841C mod 2^{32})⊕C4324633]+ 1F9F25CF mod 2^{32}

=[(D1D3F730mod 2^{32})⊕C4324633]+ 1F9F25CF mod 2^{32}

=[15E1B103] + 1F9F25CF mod 2^{32}

= 3580D6D2M

R= F(ML)⊕MR

= 3580D6D2⊕F22228AF = F22228AF

Swap atau tukar ML dan MR, ML = F22228AF dan MR= D325C843

Iterasi 9 :

ML= ML⊕P9

=F22228AF⊕ED545578 = 1F767DD7

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = 1F = 00011111 = 16+8+4+2+1=31, S1,31= 6C9E0E8B

b = 76 = 01110110 = 64+32+16+4+2=118, S2,118= 5266C825

c = 7D = 01111101 = 64+32+16+8+4+1=125, S3,125= F1290DC7

d = D7 = 11010111 = 128+64+16+4+2+1=215, S4,215= 6E163697

=[(6C9E0E8B+5266C825 mod 2^{32})⊕F1290DC7]+ 6E163697 mod 2^{32}

=[(BF04D6B0 mod 2^{32})⊕F1290DC7]+ 6E163697 mod 2^{32}

=[4E2DDB77] + 6E163697 mod 2^{32}

= BC44120E

MR= F(ML)⊕MR

= BC44120E⊕D325C843 = 6F61DA4D

Swap atau tukar ML dan MR, ML = 6F61DA4D dan MR= 1F767DD7

Iterasi 10 :

ML= ML⊕P10

=6F61DA4D⊕DB83AF7 = 62D9E0BA

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = 62 = 01100010 = 64+32+2=98, S1,98= 85C12073

b = D9 = 11011001 = 128+64+16+8+1=217, S2,217= 095BBF00

c = E0 = 11100000 = 128+64+32=224 S3,224= 30DC7D62

d = BA = 10111010 = 128+32+16+8+2=186, S4,186= 1698DB3B

=[(85C12073+095BBF00 mod 2^{32})⊕30DC7D62]+ 1698DB3B mod 2^{32}

=[(8F1CDF73 mod 2^{32})⊕30DC7D62]+ 1698DB3B mod 2^{32}

=[BFC0A211] + 1698DB3B mod 2^{32}

= D6597D4C

MR= F(ML)⊕MR

= D6597D4C⊕1F767DD7 = C92F009B

Swap atau tukar ML dan MR, ML= C92F009B dan MR= 62D9E0BA

Iterasi 11 :

ML= ML⊕P11

=C92F009B⊕FD2183BB = 340E8320

F(M L) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = 34 = 00110100 = 32+16+4=52, S1,52= B8DB38EF

b = 0E = 00001110 = 8+4+2=14, S2,14= 75094C29

c = 83 = 10000011 = 128+2+1=131 S3,131= A091CF0B

d = 20 = 00100000 = 32=32, S4,32= 9A86EE22

=[(B8DB38EF +75094C29 mod 2^{32})⊕A091CF0B]+ 9A86EE22 mod 2^{32}

=[(2DE48518 mod 2^{32})⊕A091CF0B]+ 9A86EE22 mod 2^{32}

=[8D754A13] + 9A86EE22 mod 2^{32}

= 27FC3835

MR= F(ML)⊕MR

= 27FC3835⊕62D9E0BA = 4525D88F

Swap atau tukar ML dan MR, ML= 4525D88F dan MR= 340E8320

Iterasi 12 :

ML= ML⊕P12

=4525D88F⊕E94B787A = AC6EA0F5

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = AC = 10101100 = 128+32+8+4=172, S1,172= 4BFB9790

b = 6E = 01101110 = 64+32+8+4+2= 110, S2,110= EAE96FB1

c = A0 = 10100000 = 128+32=160 S3,160= 64E4C3FE

d = F5 = 11110101 = 128+64+32+16+4+1=245, S4,245= 1948C25C

=[(4BFB9790+EAE96FB1 mod 2^{32})⊕64E4C3FE]+ 1948C25C mod 2^{32}

=[(36E50741 mod 2^{32})⊕64E4C3FE]+ 1948C25C mod 2^{32}

=[5201C4BF] + 1948C25C mod 2^{32}

= 6B4A871B

MR= F(ML)⊕MR

= 6B4A871B⊕62D9E0BA = 99367A1

Swap atau tukar MLdan MR, ML= 99367A1 dan MR= AC6EA0F5

Iterasi 13 :

ML= ML⊕P13

=99367A1⊕ED545578 = E4C732D9

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = E4 = 11100100 = 128+64+32+4=128, S1,128= AF5EBD09

b = C7 = 11000111 = 128+64+4+2+1=199, S2,199= DB6C4F15

c = 32 = 00110010 = 32+16+2=50 S3,50= 4B6D1856

d = D9 = 11011001 = 128+64+16+8+1=217, S4,217=DE966292

=[(AF5EBD09+DB6C4F15 mod 2^{32})⊕4B6D1856]+ DE966292 mod 2^{32}

=[(8ACB0C1E mod 2^{32})⊕4B6D1856]+ DE966292 mod 2^{32}

=[C1A61448] + DE966292 mod 2^{32}

= A03C76DA

MR= F(ML)⊕MR

= A03C76DA⊕AC6EA0F5 = C52D62F

Swap atau tukar ML dan MR, ML= C52D62F dan MR= E4C732D9

Iterasi 14 :

ML= ML⊕P14

=C52D62F⊕327A140A = 3E28C225

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = 3E = 00111110 = 32+16+8+4+2=62, S1,62= FB21A991

b = 28 = 00101000 = 32+8=40, S2,40= 5716F2B8

c = C2 = 11000010 = 128+64+2=194 S3,194= BB8205D0

d = 25 = 00100101 = 32+4+1=37, S4,37= 83C061BA

=[(FB21A991+5716F2B8 mod 2^{32})⊕BB8205D0]+ 83C061BA mod 2^{32}

=[(52389C49 mod 2^{32})⊕BB8205D0]+ 83C061BA mod 2^{32}

=[E9BA9999] + 83C061BA mod 2^{32}

= 6D7AFB53

MR= F(ML)⊕MR

= 6D7AFB53⊕E4C732D9 = 89BDC98A

Swap atau tukar ML dan MR, ML= 89BDC98A dan MR= 3E28C225

Iterasi 15 :

ML= ML⊕P15

=89BDC98A⊕3F84D5B5 = B6391C3F

F(ML) =[(S1,a+ S2,b mod 2^{32})⊕S3,c] + S4,d mod 2^{32}, dimana :

a = B6 = 10110110 = 128+32+16+4+2=184, S1,184= 6B93D5A0

b = 39 = 00111001 = 32+16+8+1=57, S2,57= A9446146

c = 1C = 00011100 = 16+8+4=28 S3,28= ABCA0A9A

d = 3F = 00111111 = 32+16+8+4+2+1=63, S4,63= 5AD6B472

=[(6B93D5A0+A9446146 mod 2^{32})⊕ABCA0A9A]+ 5AD6B472 mod 2^{32}

=[(14D836E6 mod 2^{32}) ABCA0A9A]+ 5AD6B472 mod 2^{32}

=[BF123C7C] + 5AD6B472 mod 2^{32}

= 19E8F0EE

MR= F(ML) MR

= 19E8F0EE 3E28C225 = 27C032CB

Swap atau tukar MLdan MR, ML= 27C032CB dan MR= B6391C3F

Iterasi 16 :

ML= ML P16

=27C032CB 530429F4 = 74C41B3F

F(M L) =[(S1,a+ S2,b mod 2^{32}) S3,c] + S4,d mod 2^{32} , dimana :

a = 74 = 01110100 = 64+32+16+4=116, S1,116= 04C006BA

b = C4 = 11000100 = 128+64+4=196, S2,196= 203E13E0

c = 1B = 00011011 = 16+8+2+1=27 S3,27= DA2547E6

d = 3F = 00111111 = 32+16+8+4+2+1=63, S4,63= 5AD6B472

=[(04C006BA +203E13E0 mod 2^{32}) DA2547E6]+ 5AD6B472 mod 2^{32}

=[(24FE1A9A mod 2^{32}) DA2547E6]+ 5AD6B472 mod 2^{32}

=[FEDB5D7C] + 5AD6B472 mod 2^{32}

= 59B211EE

MR= F(ML) MR

= 59B211EE B6391C3F = EF8B0DD1

Kemudian hasil dari ML P18 :

ML=74C41B3F 1B510052 = 6F951B6D

Dan hasil dari MR P17 :

MR= EF8B0DD1 4E734A41 = A1F84790

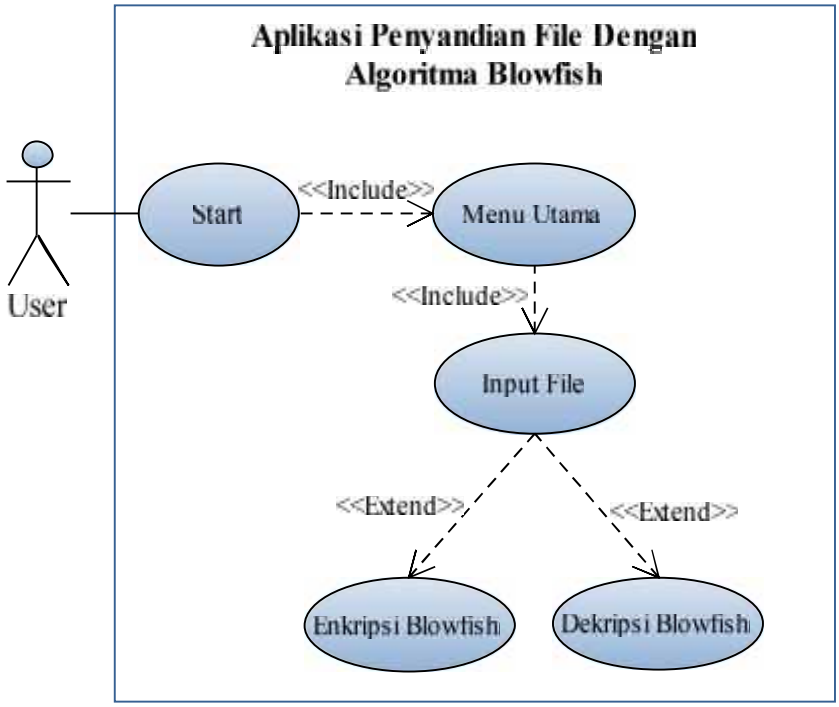
Kemudian ML digabungkan dengan MR menjadi *ciphertext* seperti ini“6F951B6D A1F84790”.

III.2. Desain Sistem

Desain sistem dibutuhkan sebagai gambaran langkah-langkah desain dan bagian-bagian yang dibutuhkan agar aplikasi dapat berjalan sesuai perancangan. Desain sistem merupakan gambaran perancangan yang akan dilakukan dan yang dihasilkan. Pada tahapan ini menggambarkan diagram alur kerja aplikasi dan desain *interface* yang akan dibuat. Adapun beberapa perancangan diagram dan desain yang akan dibuat dapat dijelaskan dibawah ini.

III.2.1. *Use case* Diagram

*Use case*diagram menggambarkan aktor yang menggunakan aplikasi dan perilaku pengguna, seperti pada gambar III.3 berikut.

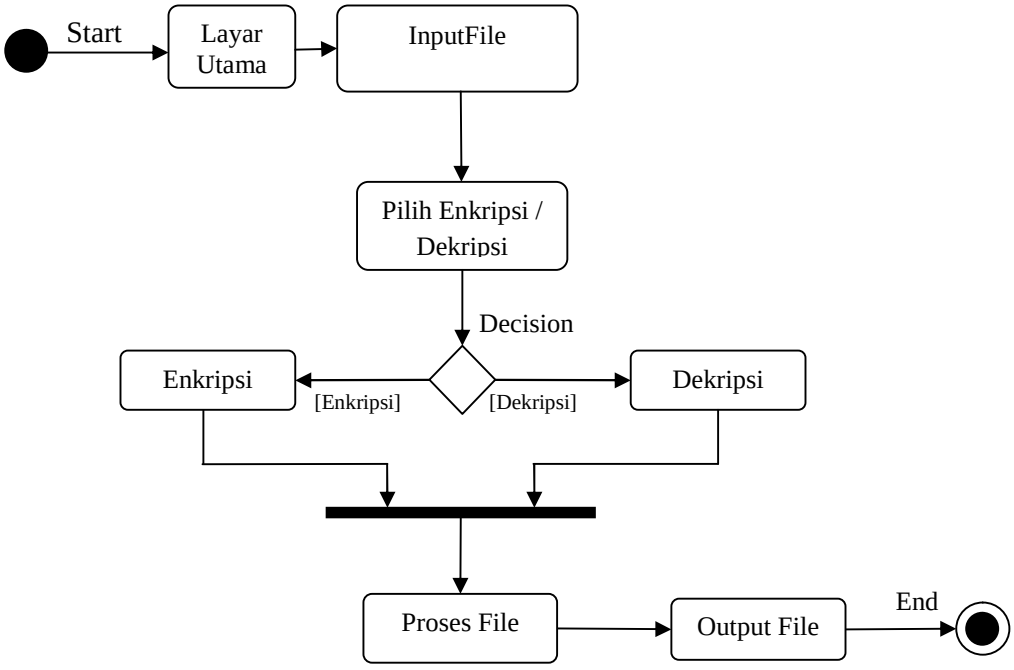


Gambar III.1. *Use Case* Diagram

Pada gambar III.1. di atas dapat dilihat proses yang berlangsung menunjukan tahapan penggunaan aplikasi yang dibangun. Pada tahapan ini penggunana mulai menjalankan aplikasi dan menemukan menu utama aplikasi, kemudian pengguna melakukan penginputan *file* dan memilih proses yang akan dilakukan apakah itu proses enkripsi *blowfish* atau proses dekripsi *blowfish*.

III.2.2.*Activity diagram*

Pada gambar dibawah ini adalah *activity* diagram aplikasi enkripsi dan dekripsi yang dirancang, dapat dilihat pada gambar III.4.

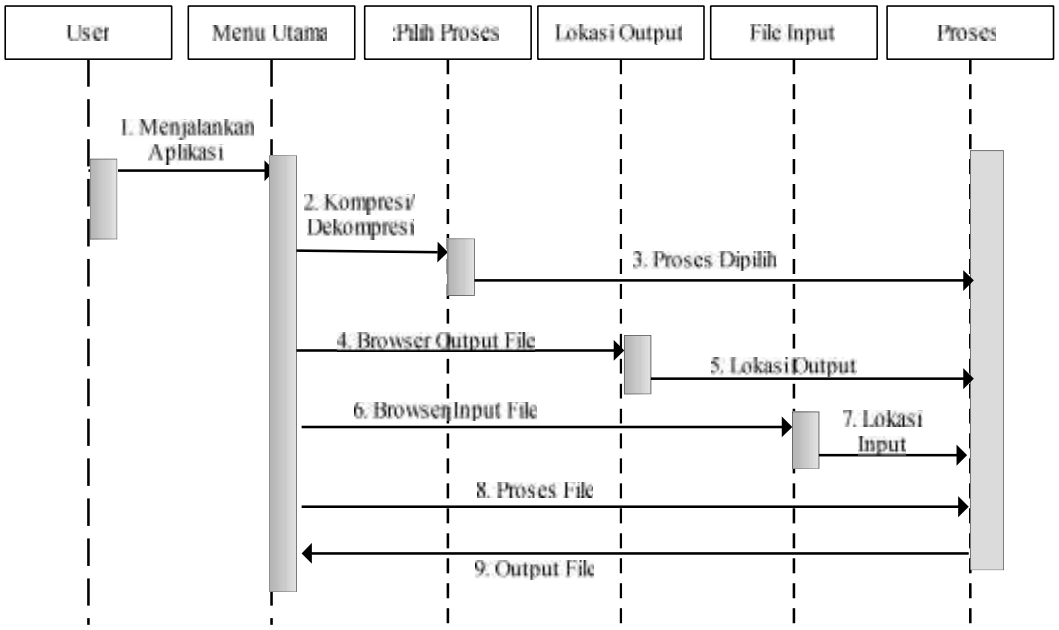


Gambar III.2. *Activity Diagram*

User atau pengguna akan menemukan menu utama saat program dijalankan, *user* memilih proses yang ingin dilakukan yaitu enkripsi atau dekripsi lalu menentukan lokas *output file* dan *input file*, setelah proses dijalankan secara otomatis aplikasi akan melakukan proses dan memberikan *output* dilokasi yang telah ditentukan oleh *user*.

III.2.3. *Sequence* diagram

Sequence diagram menggambarkan kegiatan dari skenario penggunaan aplikasi, *squence* diagram memilih proses yang dapat dilihat pada gambar III.5 berikut.

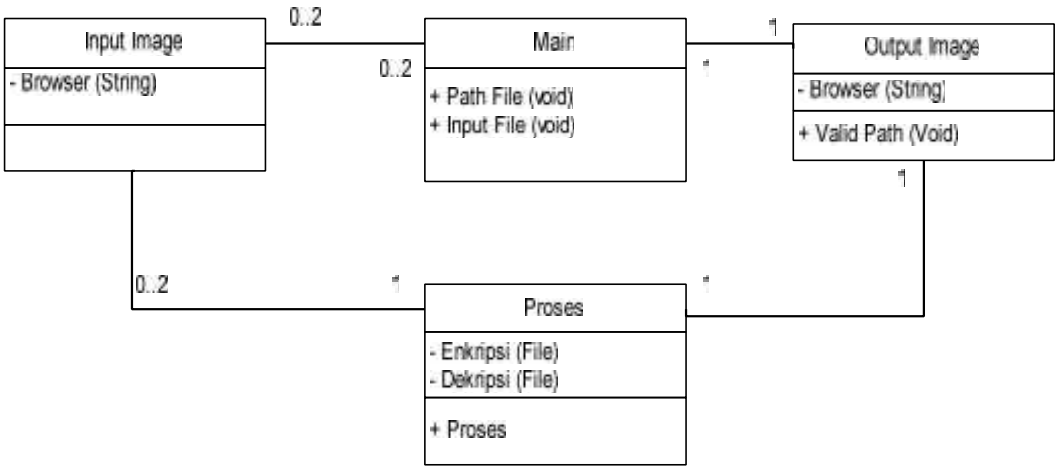


Gambar III.3. *Sequance* Diagram Pilihan Proses

Pengguna berinteraksi melalui pilihan proses yang ada pada menu utama, dapat dilihat pada *squence diagram* diatas, pengguna memilih proses yang disediakan yaitu proses enkripsi dan dekripsi. Setelah pilihan proses ditentukan oleh pengguna kembali pada menu utama.

III.2.4. *Class* diagram

Class diagram pada perancangan aplikasi ini, dapat dilihat pada gambar III.4. berikut.



Gambar III.4. *Class* Diagram

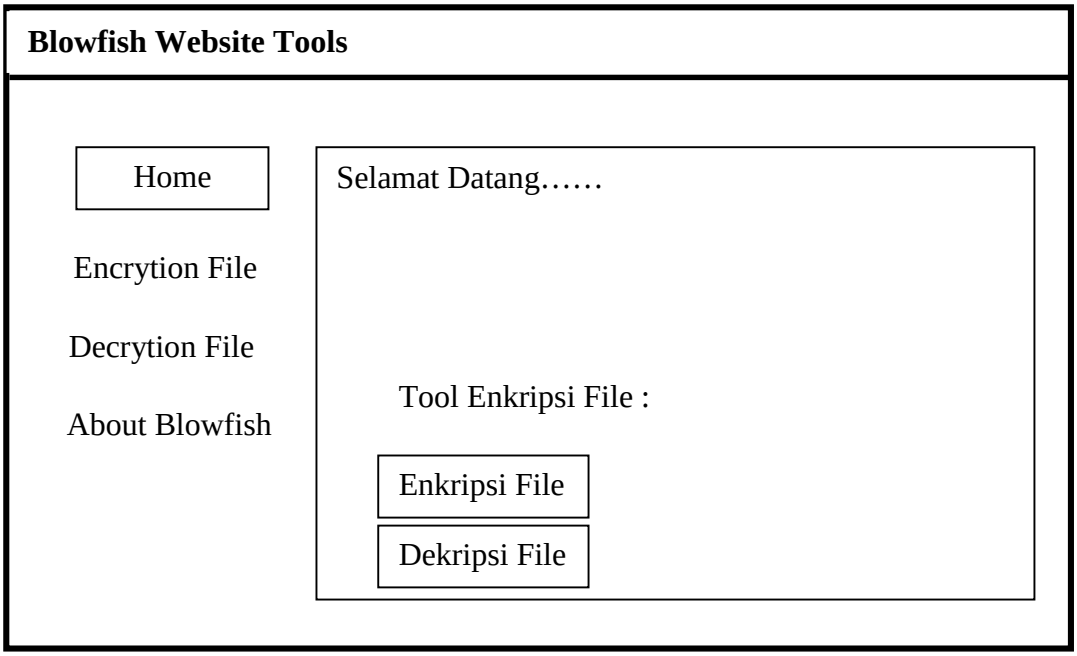
Class diagram adalah sebuah *class* yang menggambarkan struktur dan penjelasan *class*, paket, dan objek serta hubungan satu sama lain seperti *containment*, pewarisan, asosiasi, dan lain-lain. *Class* diagram juga menjelaskan hubungan antar *class* dalam sebuah sistem yang sedang dibuat dan bagaimana caranya agar mereka saling berkolaborasi untuk mencapai sebuah tujuan.

III.3. Perancangan *Interface*

Perancangan *interface* adalah gambaran tampilan layar yang akan didesain, hal ini berguna agar proses perancangan dapat dilakukan sesuai desain yang telah dilakukan. Implementasi tampilan hasil program aplikasi yang telah dapat dijalankan harus sesuai dengan desain yang telah dibuat.

III.3.1. Rancangan *Interface* Menu Utama

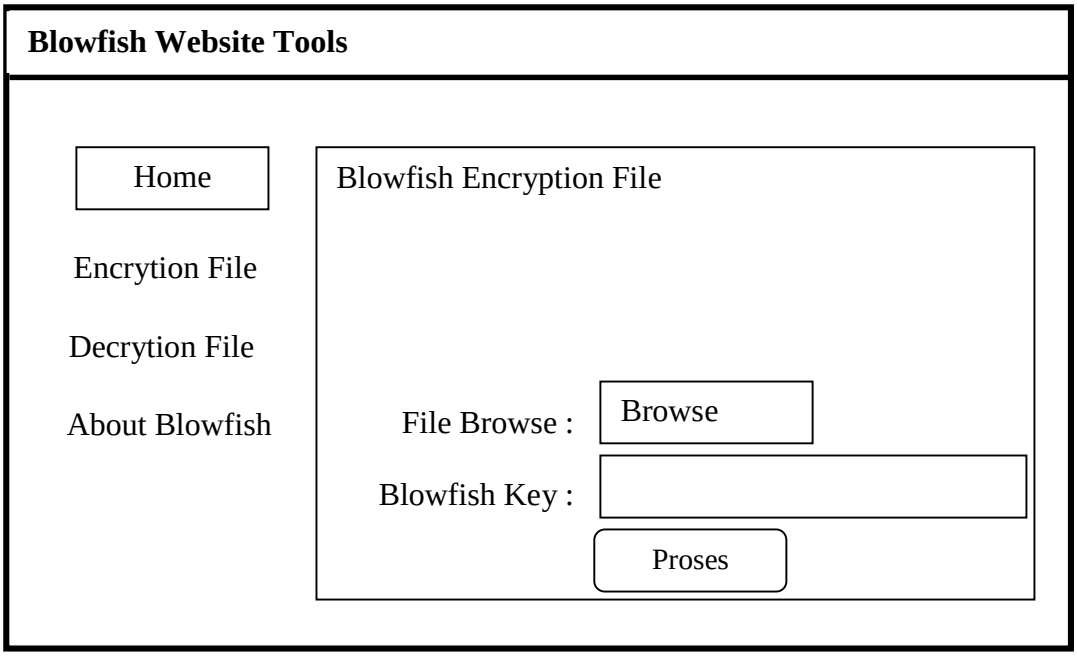
Rancangan Interface menu utama menjelaskan tampilan dimana terdapat menu dan fungsi *tools* yang digunakan untuk melakukan enkripsi maupun dekripsi *file*,yang dapat dilihat pada gambar III.5. berikut ini.



Gambar III.5. Rancangan *Interface* Menu Utama

III.3.2. Rancangan Enkripsi *File*

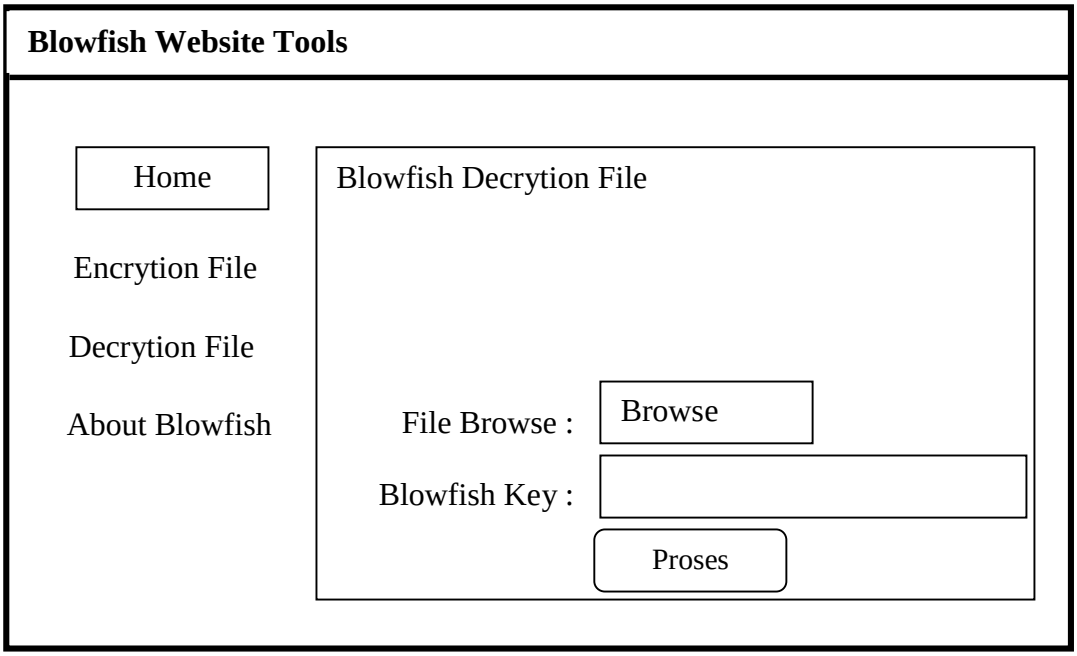
Pada desain tampilan enkripsi berfungsi untuk mengenkripsi file dengan terlebih dahulu menginputkan file dari menu enkripsi file yang ada. Dapat dilihat pada gambar III.6. berikut ini.



Gambar III.6. Rancangan *Interface* Enkripsi File

III.3.3. Rancangan Dekripsi *File*

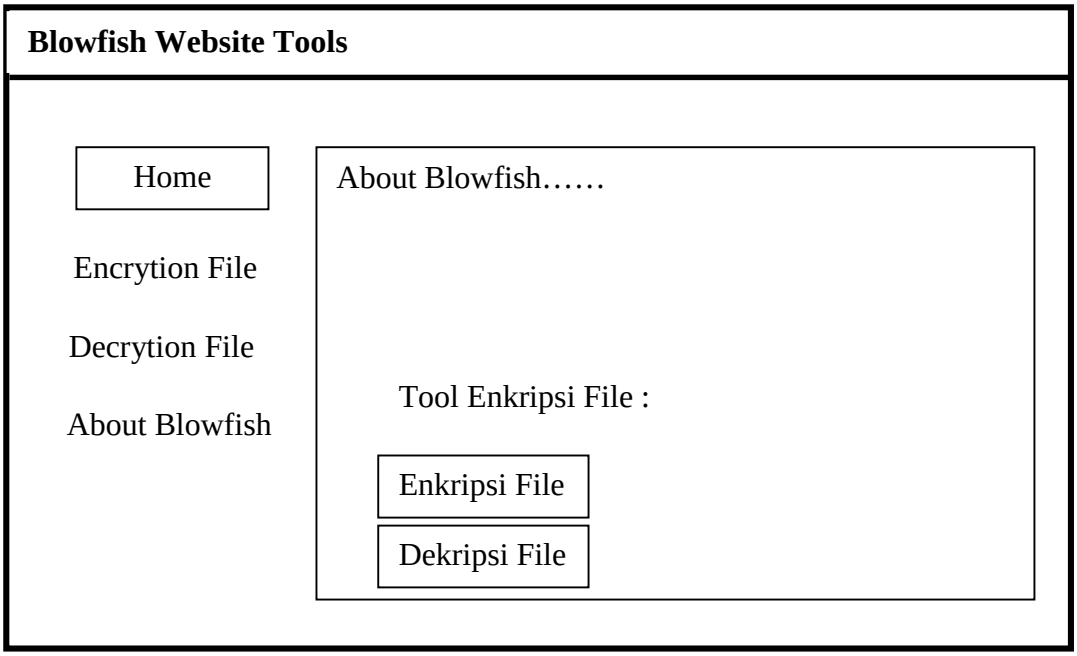
Pada desain tampilan dekripsi berfungsi untuk mendekripsi file dengan terlebih dahulu menginputkan file yang telah dienkripsi sebelumnya dari menu dekripsi file yang ada. Dapat dilihat pada gambar III.7. berikut ini.



Gambar III.7. Rancangan *Interface* Dekripsi File

III.3.4. Rancangan *Interface About Blowfish*

Pada desain tampilan *form about blowfish* ini berfungsi untuk memberikan informasi perancangan aplikasi untuk pengguna. Dapat dilihat pada gambar III.8.



Gambar III.8. Rancangan *Interface About*