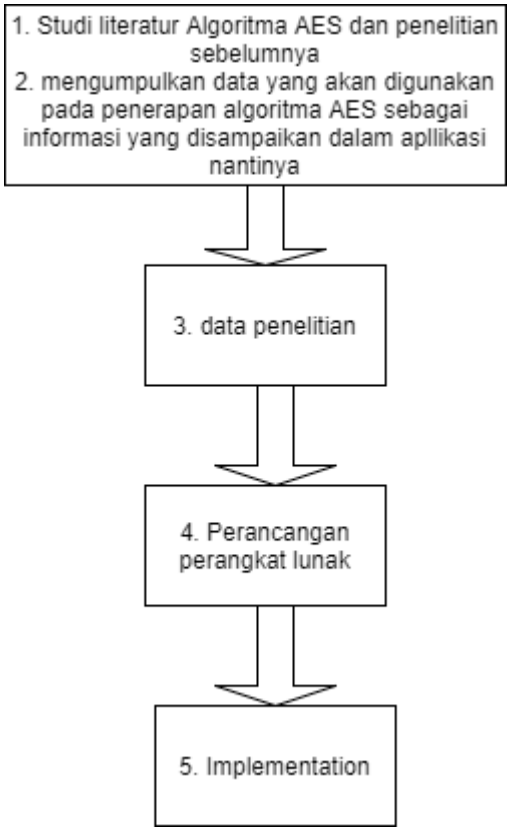
BAB III
MODEL/ PERANCANGAN SISTEM

3.1. Desain Penelitian

Desain penelitian merupakan tahapan yang mempresentasikan langkah-langkah yang akan dilakukan dalam melaksanakan penelitian tujuannya untuk memudahkan peneliti dalam melakukan penelitian.

Berikut adalah tahapan penelitian yang dilakukan penulis dalam proses penelitian dengan judul "Enkripsi Dekripsi teks dan gambar berbasis android menggunakan Algoritma AES" dengan metode pengembangan sistem *parallel*,



Gambar 3.1. desain penelitian

Tahapan-tahapan penelitian yang peneliti lakukan adalah:

1. Studi literature yang mempelajari Algoritma AES dan penelitian sebelumnya yang terkait dengan judul peneliti.
2. Mengumpulkan data yang akan digunakan pada penerapan Algoritma AES dalam proses enkripsi dekripsi.
3. Data penelitian.

4. Masalah penelitian adalah mengamankan file dengan format JPG untuk format teks dan gambar. Oleh Karena itu perancangan perangkat lunak untuk melakukan proses enkripsi dan dekripsi.
5. Implementasi.

3.2. Metode penelitian

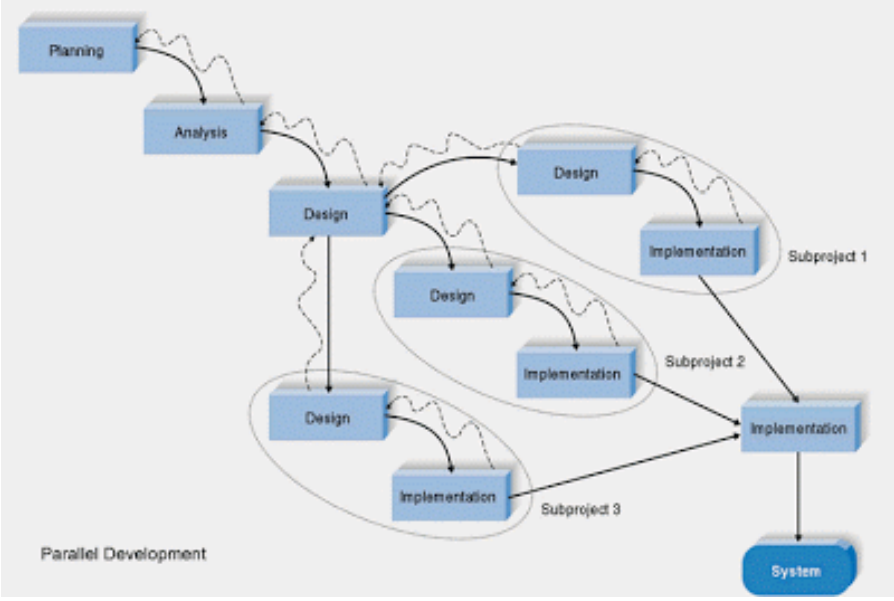
Metode yang diterapkan dalam penelitian ini meliputi metode pengumpulan data dan metode pengembangan sistem.

3.2.1. Metode Pengumpulan Data yang digunakan dalam penelitian

Yaitu metode yang digunakan untuk mempelajari dan mengumpulkan literature yang berkaitan dengan penerapan algoritma AES untuk proses enkripsi dekripsi. Dan mempelajari penelitian sebelumnya terkait dengan enkripsi dekripsi. Metode ini bersumber dari jurnal-jurnal ilmiah, makalah, artikel, buku, serta ilmiah lainnya

3.2.2. Metode Pengembangan Sistem

Metode pengembangan sistem meliputi proses-proses terstruktur antara lain *planning, analysis, design, implementation* yang dituangkan dalam satu metode dengan nama parallel.



Gambar 3.2 metode parallel

a. Planning

Pada tahap rencana kebutuhan peneliti mencari penelitian sebelumnya yang berkaitan dengan enkripsi/dekripsi dengan menggunakan metode AES dan android studio.

1. Kebutuhan fungsional sistem meliputi:

a. kebutuhan perangkat keras

Prosessor : AMD A8

RAM : 4GB

Hardisk : 500GB

b. Kebutuhan telepon pintar

OS : Android

Merk : Lenovo A369i

Versi OS : 4.2.2 (Jelly Bean)

c. Kebutuhan perangkat lunak

Operating System menggunakan Windows, aplikasi pengembang sistem menggunakan Android Studio 2.2.1

2. Kebutuhan informasi sistem meliputi:

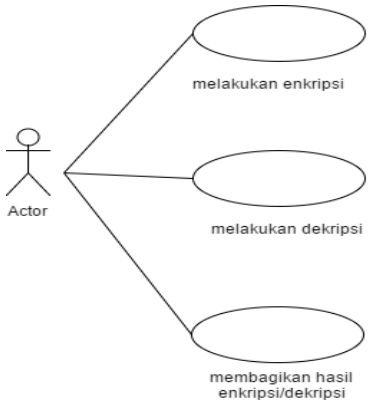
a. Bagikan

Kebutuhan yang ditambahkan pada aplikasi untuk menginformasikan media yang akan digunakan untuk mengirim hasil dari enkripsi/dekripsi.

b. Design

Pada tahap ini peneliti mulai mendesain sistem / aplikasi sesuai dengan kebutuhan user yang Keluaran dari tahapan ini adalah spesifikasi software yang meliputi organisasi sistem secara umum, struktur data dan yang lain.

1. Use case Diagram



Gambar 3.3 Use Case Diagram

- **Spesifikasi Use Case Diagram enkripsi**

Brief Description	*Use case* ini digunakan oleh aktor untuk melakukan enkripsi.
Primary Actor	Pengguna
Supporting Actor	-
Basic Flow	1. *Use case* dimulai setelah aktor membuka aplikasi 2. Aplikasi akan menampilkan menu utama 3. Pengguna dapat memilih file dari memori handphone 4. Pengguna dapat memasukkan kunci untuk keamanan filenya 5. Pengguna dapat melihat hasil dari enkripsinya 6. *Use case* ini selesai.
Alternative Flow	-
Error Flow	Aplikasi tidak akan memproses ketika ada menu yang belum di isi/pilih
PreConditions	Aktor berhasil memasuki sistem.

PostConditions	Aktor membuka aplikasi dan dapat menggunakan fungsi-fungsi dalam aplikasi sesuai dengan tata cara penggunaan

- **Spesifikasi Use Case Diagram dekripsi**

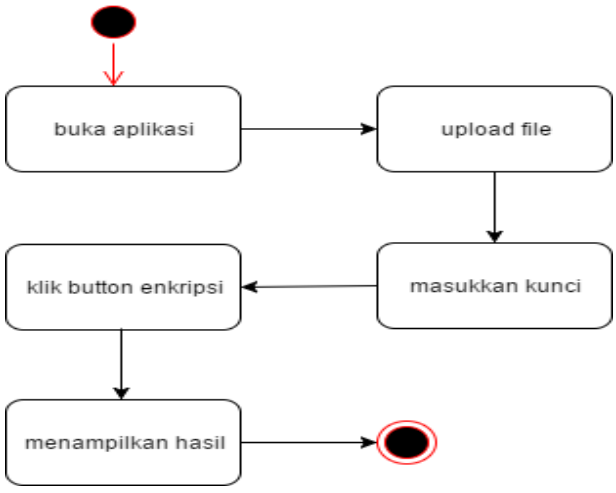
Brief Description	*Use case* ini digunakan oleh aktor untuk melakukan proses dekripsi.
Primary Actor	Pengguna
Supporting Actor	-
Basic Flow	*1.* *Use case* dimulai setelah aktor membuka aplikasi *2.* Aplikasi akan menampilkan menu utama *3.* Pengguna dapat memilih file dari memori handphone *4.* Pengguna dapat memasukkan kunci untuk keamanan filenya *5.* Pengguna dapat melihat hasil dari dekripsinya *6.* *Use case* ini selesai.
Alternative Flow	-
Error Flow	Aplikasi tidak akan memproses ketika ada menu yang belum di isi/pilih
PreConditions	Aktor berhasil memasuki sistem.
PostConditions	Aktor membuka aplikasi dan dapat menggunakan fungsi-fungsi dalam aplikasi sesuai dengan tata cara penggunaan

- **Spesifikasi Use Case Diagram bagikan**

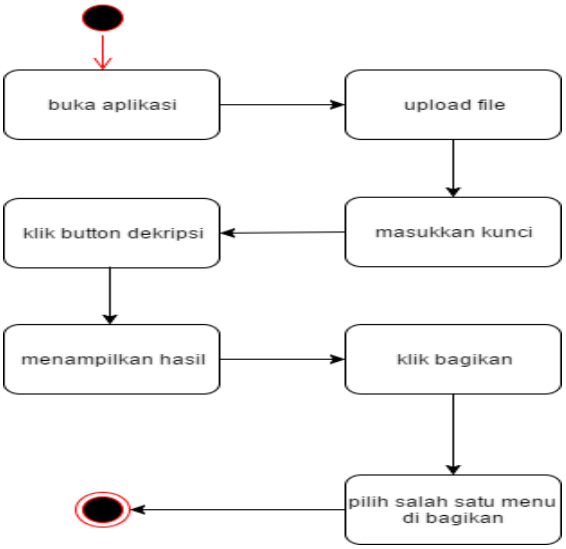
Brief Description	*Use case* ini digunakan oleh aktor untuk melakukan pengiriman dari hasil enkripsi/dekripsi
Primary Actor	Pengguna

Supporting Actor	-
Basic Flow	1. *Use case* dimulai setelah aktor melakukan proses enkripsi/dekripsi 2. Aplikasi akan menampilkan beberapa menu media yang ada di handphone untuk proses pengiriman. 3. Pengguna dapat mengirim hasil dari proses enkripsi/dekripsi ke orang yang inginkan. 4. *Use case* ini selesai.
Alternative Flow	-
Error Flow	Aplikasi tidak akan memproses ketika tidak ada file yang akan dikirimkan.
PreConditions	Aktor berhasil memasuki sistem.
PostConditions	Aktor membuka aplikasi dan dapat menggunakan fungsi-fungsi dalam aplikasi sesuai dengan tata cara penggunaan

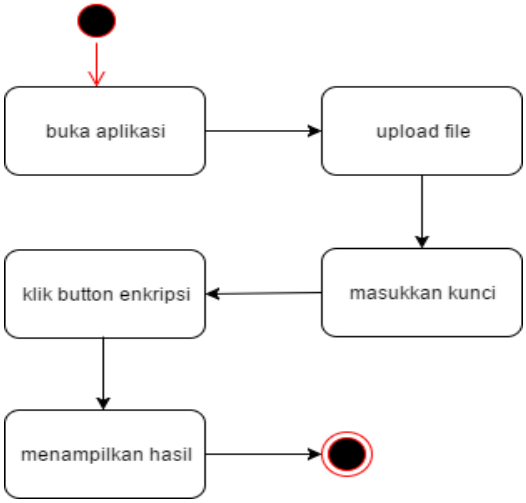
- **Diagram Activity**



Gambar 3.4 Activity diagram melakukan enkripsi

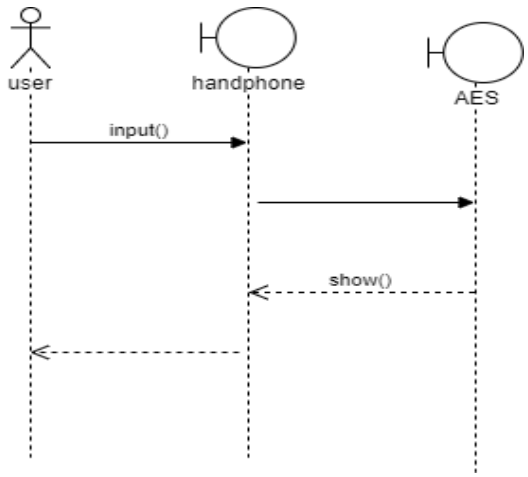


Gambar 3.5. Activity Diagram melakukan dekripsi

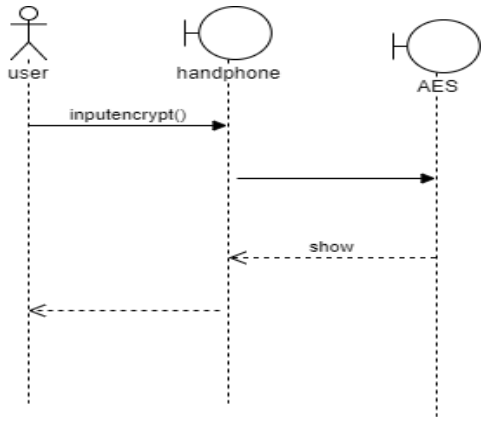


Gambar 3.6 Activity Diagram bagikan

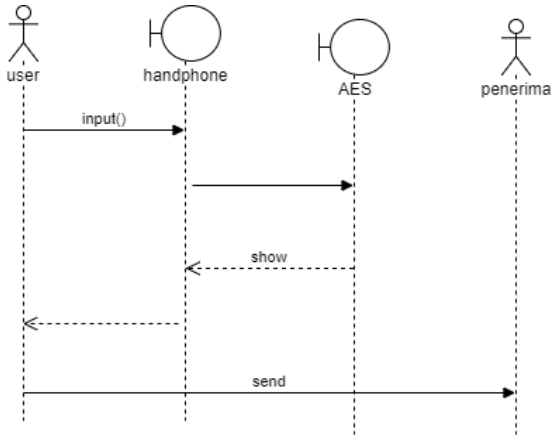
- **Sequence diagram**



Gambar 3.7. *sequence diagram* enkripsi



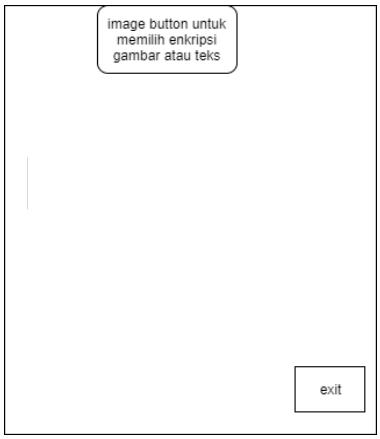
Gambar 3.8. *sequence diagram dekripsi*



Gambar 3.9. *sequence diagram* share

- **Desain *interface***

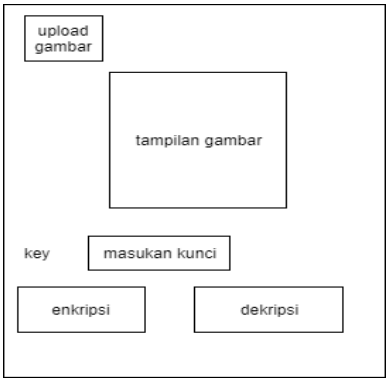
- Halaman awal



Gambar 3.10. tampilan awal

Pada tampilan awal terdapat image button yang akan memberikan dua pilihan *user* akan memilih teks atau gambar. Sedangkan exit untuk keluar dari aplikasi.

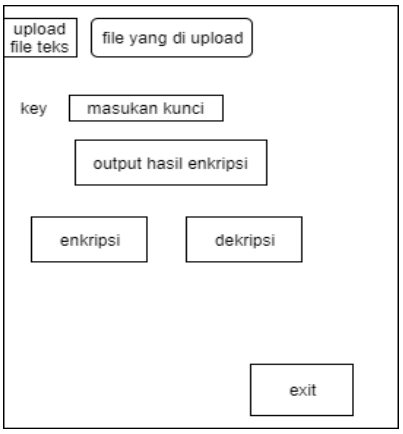
- Halaman enkripsi/dekripsi gambar



Gambar 3.11 tampilan gambar

Pada tampilan ini terdapat upload gambaryang akan mengambil gambar dari memori penyimpanan yang ada di handphone, setelah memilih akan menampilkan gambar yang dipilih tadi. Pada masukkan kunci *user* akan memasukkan kunci yang digunakan untuk proses enkripsi. Enkripsi/dekripsi adalah pilihan bagi user untuk melakukan proses enkripsi/dekripsi.

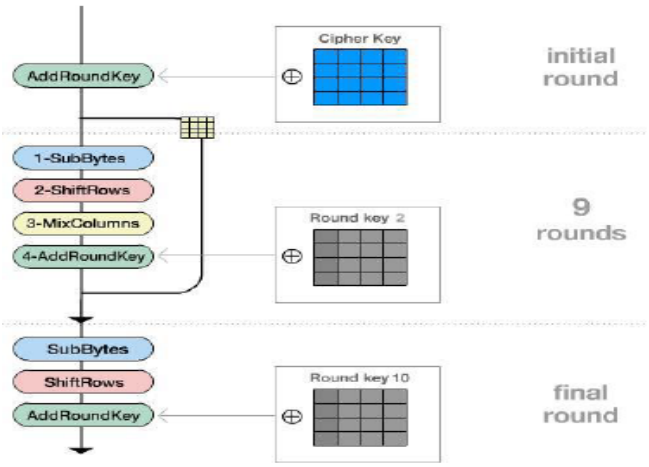
- halaman enkripsi/dekripsi teks



Gambar 3.12 tampilan teks

- upload file teks: adalah button dimana user akan memilih file dokumen/teks yang terdapat di memori handphone untuk dilakukan enkripsi.
- Masukan kunci: user memasukkan kunci untuk proses enkripsi/dekripsi.
- Output hasil enkripsi: adalah hasil dari proses enkripsi/dekripsi.
- Enkripsi/dekripsi: button untuk user memilih enkripsi atau deskripsi.
- Exit: button untuk user agar keluar dari aplikasi.

- **Design algoritma**



Gambar 3.13. Gambar desain algoritma aes

Contoh:

Plaintext :

Tabel 3.1. plaintext

Char	T	W	O		O	n	e		N	i	n	e		T	W	0
Hex	54	77	6F	20	4F	6E	65	20	4E	69	6E	65	20	54	77	6F

Key:

Tabel 3.2 key

Char	T	h	A	t	s		M	y		K	u	n	G		F	u
Hex	54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

Pemrosesan key schedule:

- Key pada Hex (128 bits) : 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
- w[0] = (54; 68; 61; 74); w[1] = (73; 20; 6D; 79); w[2] = (20; 4B; 75; 6E); w[3] = (67; 20; 46; 75)
- g(w[3]):
    - pergeseran satu ke kiri pada w[3] menjadi: (20; 46; 75; 67)
    - diubah ke tabel S-box: (B7; 5A; 9D; 85)
    - di proses dengan rcon (01; 00; 00; 00) dan menjadi (B6; 5A; 9D; 85)

- w[4] = w[0] ⊕ g(w[3]) = (E2; 32; F C; F1), w[5] = w[4] ⊕ w[1] = (91; 12; 91; 88), w[6] = w[5] ⊕ w[2] = (B1; 59; E4; E6), w[7] = w[6] ⊕ w[3] = (D6; 79; A2; 93)
- • hasil roundkey pertama: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

Tabel 3.3. *Generated key*

Round	Hasil proses round key
Round 0	54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
Round 1	E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
Round 2	56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA
Round 3	D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03 1E FB
Round 4	A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B
Round 5	B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69
Round 6	BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E
Round 7	CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A
Round 8	8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C
Round 9	BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
Round 10	28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

Round 0:

-addroundkey:

$$\begin{bmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{bmatrix} \oplus \begin{bmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{bmatrix} = \begin{bmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{bmatrix} \text{.....(1)}$$

Round 1:

- Sub-bytes

$$\begin{bmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{bmatrix} -SBox\rightarrow \begin{bmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{bmatrix} \text{.....(2)}$$

- Shift row

$$\begin{bmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{bmatrix} \text{—Shift Row} \rightarrow \begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix} \text{.....(3)}$$

- Mix columns

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix} = \begin{bmatrix} BA & 8A & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{bmatrix} \quad \text{.....(4)}$$

- Add-roundkey

$$\begin{bmatrix} BA & 8A & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{bmatrix} \oplus \begin{bmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{bmatrix} = \begin{bmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 15 & BA & E8 & CE \end{bmatrix} \quad \text{.....(5)}$$

Tabel 3.4. hasil tiap *round*

Round	Hasil round
Round 1	58 47 08 8B 15 B6 1C BA 59 D4 E2 E8 CD 39 DF CE
Round 2	43 0E 09 3D C6 57 08 F8 A9 C0 EB 7F 62 C8 FE 37
Round 3	78 70 99 4B 76 76 3C 39 30 7D 37 34 54 23 5B F 1
Round 4	B1 08 04 E7 CA FC B1 B2 51 54 C9 6C ED E1 D3 20
Round 5	9B 23 5D 2F 51 5F 1C 38 20 22 BD 91 68 F 0 32 56
Round 6	14 8F C0 5E 93 A4 60 0F 25 2B 24 92 77 E8 40 75
Round 7	53 43 4F 85 39 06 0A 52 8E 93 3B 57 5D F 8 95 BD
Round 8	66 70 AF A3 25 CE D3 73 3C 5A 0F 13 74 A8 0A 54
Round 9	09 A2 F 0 7B 66 D1 FC 3B 8B 9A E6 30 78 65 C4 89
Round 10 (hasil/ ciphertext)	29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A
output	vnlnHpTGyugmOpZ04IELX8fBo7LoT2Ww01/uZtwyYmE=

c. Implementation

Tahapan ini adalah tahapan pengujian terhadap aplikasi apakah ada kesalahan atau tidak sebelum di gunakan. Pengujian terhadap aplikasi dilakukan guna mengetahui lebih dini tentang kesiapan program dalam input data, olah data dan output yang dihasilkan. Selain itu juga dimaksudkan untuk mengetahui lebih lanjut apakah masih ada kesalahan-kesalahan dan kekurangan dari aplikasi.

a. Pengujian *Black-Box*

Black Box Testing berfokus pada spesifikasi fungsional dari perangkat lunak. Tester dapat mendefinisikan kumpulan kondisi input dan melakukan pengetesan pada spesifikasi fungsional program. Black Box Testing bukanlah solusi alternatif dari White Box Testing

tapi lebih merupakan pelengkap untuk menguji hal-hal yang tidak dicakup oleh White Box Testing. Black Box Testing cenderung untuk menemukan hal-hal berikut:

1. Fungsi yang tidak benar atau tidak ada.
2. Kesalahan antarmuka (interface errors).
3. Kesalahan pada struktur data dan akses basis data.
4. Kesalahan performansi (performance errors).
5. Kesalahan inisialisasi dan terminasi.