BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

Tahap implementasi dan pengujian sistem adalah suatu tahap realisasi dari perancangan sistem yang telah dibuat seperti yang telah diuraikan pada bab III. Pada bab ini pembangunan sistem, menggunakan beberapa perangkat lunak, perangkat keras yang dibutuhkan, serta membangun database yang akan digunakan dalam mengoperasikan sistem.

Dengan melakukan pengujian sistem, akan diketahui tingkat keberhasilan dari pembangunan sistem ini. Pengujian dilakukan baik pada saat pembangunan maupun pengimplementasian sistem, meliputi uji kesalahan yan terjadi dan performansi sistem.

4.1 Implementasi

4.1.1 Perangkat Lunak Pendukung

Perangkat lunak yang digunakan terbagi menjadi dua kategori, yaitu perangkat lunak yang digunakan pada saat membangun sistem dan perangkat lunak yang digunakan untuk mengoperasikan sistem.

Pada saat pembangunan sistem, menggunakan perangkat lunak sebagai berikut :

1. Sistem Operasi Windows Vista Home Basic SP 2
2. Notepad++ 5.6.8
3. Paint.NET 3.5.1
4. Mozilla FireFox 3.5.9

5. XAMPP 1.7.1
6. Cerberus FTP Server 1.71
7. MDaemon 4.0.2

Dalam pembangunan sistem ini mempergunakan perangkat lunak yang memiliki lisensi resmi ataupun perangkat lunak yang *freeware*.

Sedangkan untuk pengoperasian membutuhkan perangkat lunak sebagai berikut :

1. Tidak memerlukan spesifikasi khusus untuk sistem operasi, karena aplikasi ini berbasis *web*, sehingga dapat dijalankan pada *multiplatform*.
2. *Internet browser*; seperti Microsoft Internet Explorer, Mozilla Firefox, Opera, Safari, Google Chrome, dan masih banyak lagi, dengan syarat *JavaScript Enabled*, dan mendukung CSS 2.1.

Aplikasi yang dibangun menggunakan PHP sebagai bahasa pemrograman. Selain PHP, bahasa pemrograman JavaScript dan CSS juga digunakan sebagai bahasa pendukung yang menjadikan sistem lebih mudah untuk dipergunakan.

4.1.2 Perangkat Keras

Perangkat keras yang digunakan dalam proses pembangunan sistem :

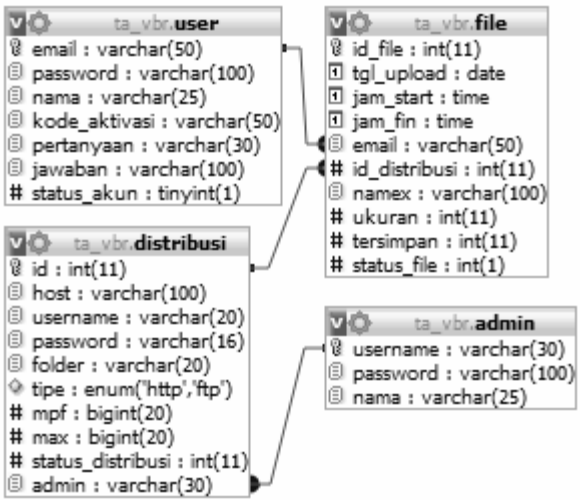
1. Prosesor Intel Dual Core
2. Monitor dengan resolusi 1280 x 800
3. Keyboard dan mouse

Sedangkat untuk pengoperasian sistem membutuhkan perangkat sebagai berikut :

1. Prosesor minimal 1.81 GHz
2. Monitor dengan resolusi minimal 800 x 600. Rekomendasi pada resolusi 1024 x 768 tampilan terbaik. Untuk resolusi dibawah 800 x 600, sistem masih dapat dijalankan, namun kenyamanan dalam penggunaan sistem akan berkurang.
3. Keyboard dan mouse
4. Modem atau *Lan Card* untuk koneksi internet.

4.1.3 Implementasi *Database*

Database yang dipakai adalah MySQL yang terdapat dalam paket XAMPP versi 1.7.1. Pembuatan dan pengolahan awal menggunakan phpMyAdmin 3.1.3.1.



Gambar 4.1 Implementasi *database*

4.1.4 Implementasi Pengguna

Pengguna yang dapat menggunakan sistem bisa siapa saja, dengan syarat mendaftarkan diri dengan menggunakan alamat *email* sebagai *username*. Tidak

ada pembatasan usia dan jenis kelamin dalam menggunakan sistem. Namun pengguna harus bisa berbahasa Indonesia, karena sistem hanya menggunakan satu bahasa. Pengguna juga harus sudah bisa menggunakan komputer dan *internet*, serta sedikit tahu mengenai istilah-istilah yang ada dalam dunia *internet*. Hanya ada satu jenis *user* yang bertindak sebagai pengguna sistem, memiliki hak untuk menyimpan *file* secara *online* setelah melakukan proses *log in* dengan benar. Seorang *user* pengguna hanya bisa mengelola *file* miliknya, tidak dapat mengelola *file* milik *user* yang lain.

Untuk *user* sebagai *administrator*, memiliki kewenangan untuk menambah , mengubah, dan menghapus data lokasi distribusi *file*. Setiap lokasi distribusi akan ditandai sehingga diketahui siapa yang menambahkan lokasi tersebut. Lokasi distribusi yang memiliki data *file* didalamnya tidak dapat diubah ataupun dihapus.

4.1.5 Implementasi Data

Data yang digunakan dalam sistem dapat dikategorikan menjadi dua, yaitu data pribadi dan data file. Data pribadi meliputi alamat *email*, nama, password dan sepasang pertanyaan dengan jawabannya. Sedangkan data *file* adalah *file* yang akan disimpan dalam penyimpanan *online*, dienkripsi, yang memiliki ukuran dan tipe *file*. Untuk ukuran *file* dibatasi maksimal 20MB, sedangkan tipe *file* tidak ada pembatasan.

4.1.6 Implementasi Antarmuka

Antarmuka yang telah dirancang pada bab III, diimplementasikan dengan mengadopsi warna-warna bernuansa *black and white*. Penggunaan CSS 2.1

membuat tampilan antarmuka lebih baik. Namun tampilan dapat berubah apabila *internet browser* yang digunakan tidak mendukung CSS 2.1.

Berikut adalah gambar-gambar tampilan antarmuka aplikasi penyimpanan *file online*.



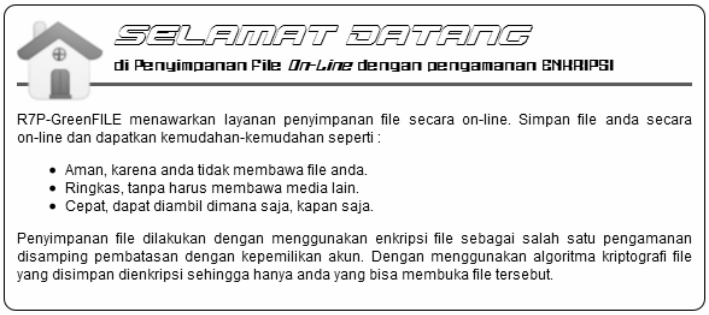
Gambar 4.2 Tampilan Utama (sebelum *Log In*)



Gambar 4.3 Form *Log In*



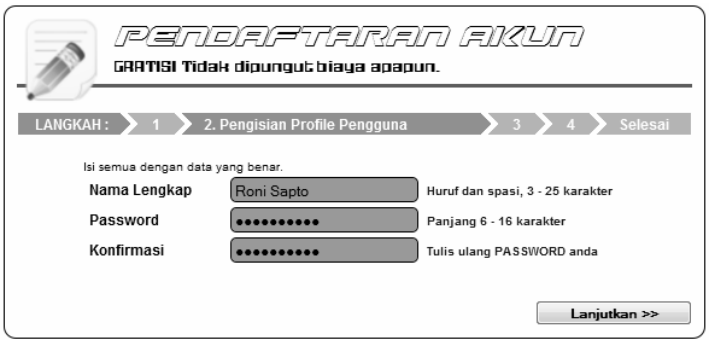
Gambar 4.4 Menu mengadopsi sistem *Drop Down*



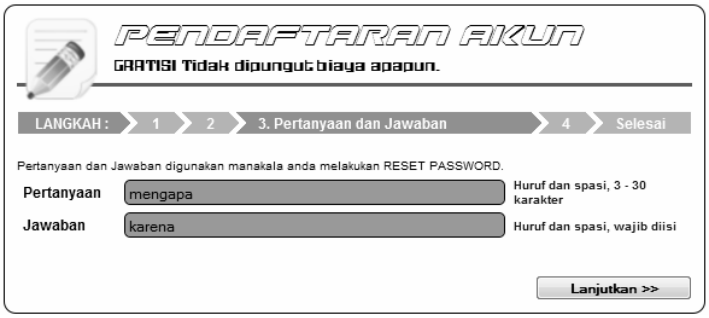
Gambar 4.5 Tampilan *Home*



Gambar 4.6 Tampilan Pendaftaran, memasukkan *email*



Gambar 4.7 Tampilan Pendaftaran, memasukkan Nama dan *Password*



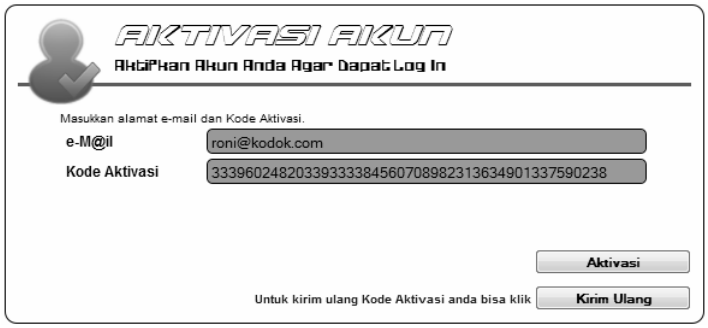
Gambar 4.8 Tampilan Pendaftaran, memasukkan pertanyaan dan jawaban



Gambar 4.9 Tampilan Pendaftaran, konfirmasi akhir data *user*



Gambar 4.10 Tampilan Pendaftaran sukses



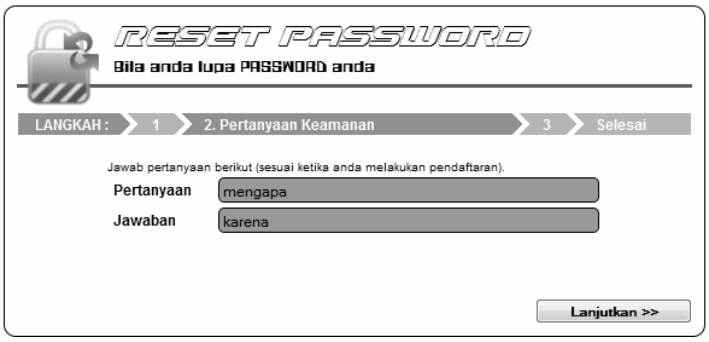
Gambar 4.11 Tampilan Aktivasi akun



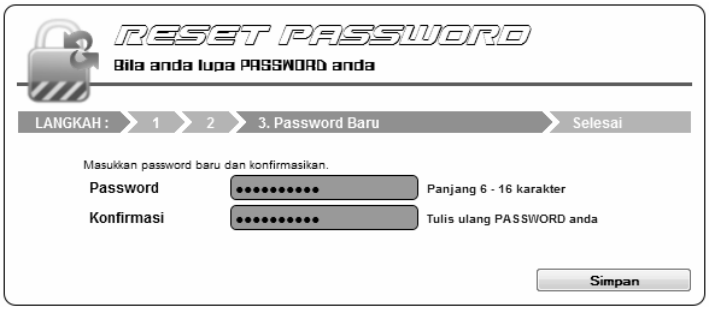
Gambar 4.12 Tampilan Aktivasi akun sukses



Gambar 4.13 Tampilan *Reset Password*, memasukkan *email*



Gambar 4.14 Tampilan *Reset Password*, memasukkan jawaban



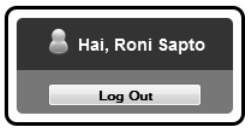
Gambar 4.15 Tampilan *Reset Password*, memasukkan *password* baru



Gambar 4.16 Tampilan *Reset Password* sukses



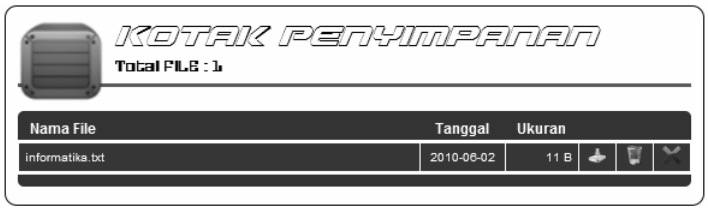
Gambar 4.17 Tampilan Utama (setelah *Log In* sebagai *user* pengguna)



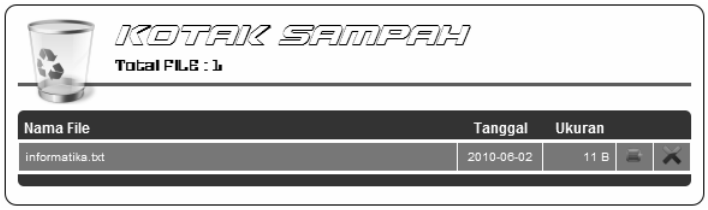
Gambar 4.18 Nama *user* ditampilkan dan terdapat tombol *Log Out*



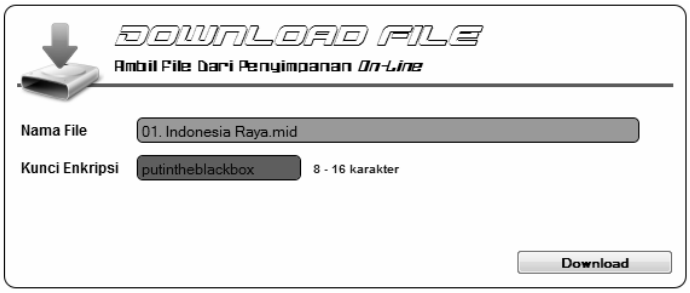
Gambar 4.19 Tampilan *Upload file*



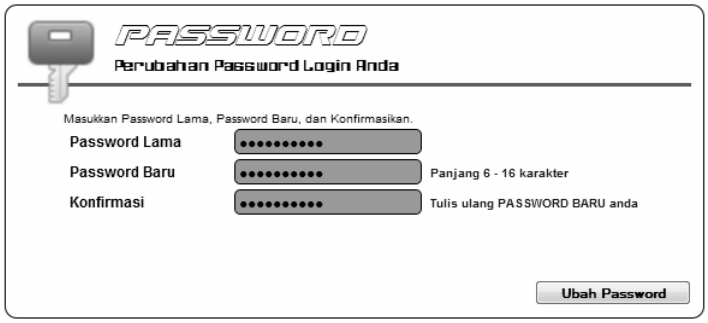
Gambar 4.20 Tampilan daftar *file* dalam kotak penyimpanan



Gambar 4.21 Tampilan daftar *file* dalam kotak sampah



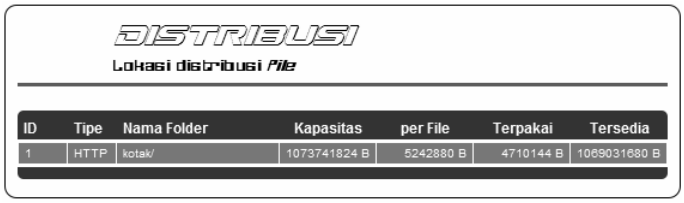
Gambar 4.22 Tampilan *download file*



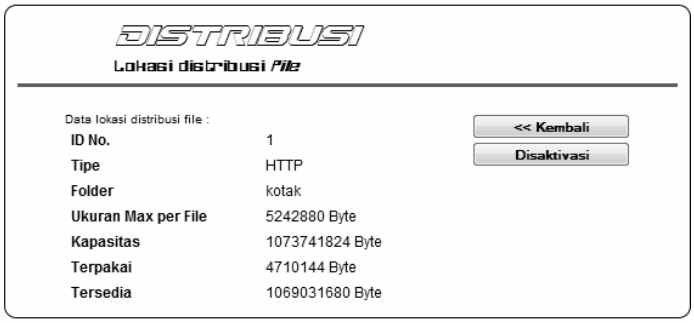
Gambar 4.23 Tampilan perubahan *password*



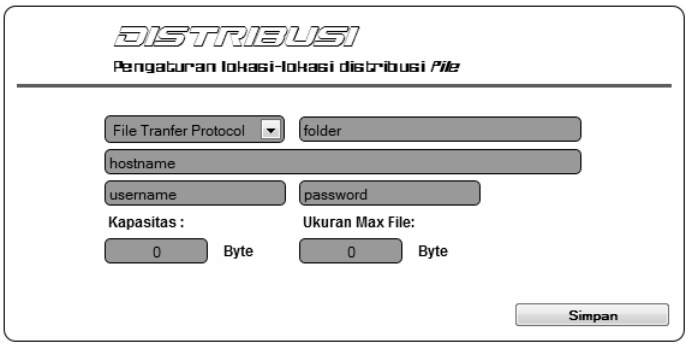
Gambar 4.24 Tampilan *Home* (*Log In* sebagai *user administrator*)



Gambar 4.25 Tampilan daftar distribusi



Gambar 4.26 Tampilan detail distribusi



Gambar 4.27 Tampilan tambah atau ubah distribusi

4.2 Pengujian Sistem

4.2.1 Pengujian Terhadap Masukan

Pengujian ini dilakukan menggunakan metoda *blackbox*. Dengan merencanakan masukkan, baik masukkan yang benar maupun yang salah, lalu akan dibandingkan antara harapan keluaran dan hasil pengamatan.

1. Proses Log In

Tabel 4.1 *Blackbox* proses *Log In*

Masukkan	Harapan	Hasil Pengamatan	Kesimpulan
email kosong	kursor mengarah pada field e-M@il	kursor mengarah pada field e-M@il	sesuai harapan
password kosong	kursor mengarah pada field password	kursor mengarah pada field password	sesuai harapan
email dan password terisi dengan benar	proses login sukses	proses login sukses	sesuai harapan

2. Proses Pendaftaran

Tabel 4.2 *Blackbox* proses Pendaftaran

Masukkan	Harapan	Hasil Pengamatan	Kesimpulan
email kosong	muncul pesan “Alamat e-M@il belum diisi”	muncul pesan “Alamat e-M@il belum diisi”	sesuai harapan
format penulisan email salah	muncul pesan “Masukkan alamat e-M@il yang benar”	muncul pesan “Masukkan alamat e-M@il yang benar”	sesuai harapan
Nama lengkap kosong	muncul pesan “Nama lengkap belum	muncul pesan “Nama lengkap belum	sesuai harapan

	diisi”	diisi”	
panjang nama kurang dari tiga huruf	muncul pesan “Panjang nama lengkap adalah 3 – 30 karakter”	muncul pesan “Panjang nama lengkap adalah 3 – 30 karakter”	sesuai harapan
Password kosong	muncul pesan “Password belum diisi”	muncul pesan “Password belum diisi”	sesuai harapan
panjang password kurang dari delapan huruf	muncul pesan “Panjang password adalah 6 – 16 karakter”	muncul pesan “Panjang password adalah 6 – 16 karakter”	sesuai harapan
Konfirmasi kosong	muncul pesan “Konfirmasi Password berbeda dengan Password”	muncul pesan “Konfirmasi Password berbeda dengan Password”	sesuai harapan
Konfirmasi berbeda dengan password	muncul pesan “Konfirmasi Password berbeda dengan Password”	muncul pesan “Konfirmasi Password berbeda dengan Password”	sesuai harapan
Pertanyaan kosong	muncul pesan “Pertanyaan belum diisi”	muncul pesan “Pertanyaan belum diisi”	sesuai harapan
panjang pertanyaan kurang dari tiga huruf	muncul pesan “Panjang pertanyaan adalah 3 – 30 karakter”	muncul pesan “Panjang pertanyaan adalah 3 – 30 karakter”	sesuai harapan
Jawaban kosong	muncul pesan “Jawaban belum diisi”	muncul pesan “Jawaban belum diisi”	sesuai harapan

3. Proses Aktivasi Akun

Tabel 4.3 *Blackbox* proses Aktivas Akun

Masukkan	Harapan	Hasil Pengamatan	Kesimpulan
email kosong	muncul pesan “Email wajib diisi”	muncul pesan “Email wajib diisi”	sesuai harapan
format penulisan email salah	muncul pesan “Masukkan alamat e-M@il yang benar”	muncul pesan “Masukkan alamat e-M@il yang benar”	sesuai harapan
Kode aktivasi kosong	muncul pesan “Anda belum mengisi kode aktivasi”	muncul pesan “Anda belum mengisi kode aktivasi”	sesuai harapan

4. Proses *Reset Password*

Tabel 4.4 *Blackbox* proses *Reset Password*

Masukkan	Harapan	Hasil Pengamatan	Kesimpulan
email kosong	muncul pesan “Alamat e-mail belum diisi”	muncul pesan “Alamat e-mail belum diisi”	sesuai harapan
format penulisan email salah	muncul pesan “Masukkan alamat e-mail yang benar”	muncul pesan “Masukkan alamat e-mail yang benar”	sesuai harapan

Jawaban kosong	muncul pesan "Anda belum mengisi jawaban"	muncul pesan "Anda belum mengisi jawaban"	sesuai harapan
Password kosong	muncul pesan "Password belum diisi"	muncul pesan "Password belum diisi"	sesuai harapan
panjang password kurang dari delapan huruf	muncul pesan "Panjang password adalah 6 – 16 karakter"	muncul pesan "Panjang password adalah 6 – 16 karakter"	sesuai harapan
Konfirmasi kosong	muncul pesan "Konfirmasi Password berbeda dengan Password"	muncul pesan "Konfirmasi Password berbeda dengan Password"	sesuai harapan
Konfirmasi berbeda dengan password	muncul pesan "Konfirmasi Password berbeda dengan Password"	muncul pesan "Konfirmasi Password berbeda dengan Password"	sesuai harapan

5. Proses *Upload File*

Tabel 4.5 *Blackbox* proses *Upload File*

Masukkan	Harapan	Hasil Pengamatan	Kesimpulan
alamat file kosong	muncul pesan "Anda belum memilih file"	muncul pesan "Anda belum memilih file"	sesuai harapan
Kunci kosong	muncul pesan "Kunci belum diisi"	muncul pesan "Kunci belum diisi"	sesuai harapan
panjang kunci kurang dari delapan huruf	muncul pesan "Panjang kunci adalah 8 – 16 karakter"	muncul pesan "Panjang kunci adalah 8 – 16 karakter"	sesuai harapan

6. Proses *Download File*

Tabel 4.6 *Blackbox* proses *Download File*

Masukkan	Harapan	Hasil Pengamatan	Kesimpulan
Kunci kosong	muncul pesan "Kunci belum diisi"	muncul pesan "Kunci belum diisi"	sesuai harapan
panjang kunci kurang dari delapan huruf	muncul pesan "Panjang kunci adalah 8 – 16 karakter"	muncul pesan "Panjang kunci adalah 8 – 16 karakter"	sesuai harapan

4.2.2 Pengujian Keamanan Berdasarkan *Avalanche Effect*

Avalanche Effect dihitung dengan membandingkan perbedaan bit pada cipherteks 1 dan cipherteks 2. Ada 2 macam eksperimen yang dilakukan. Pertama, melakukan 2 eksperimen pada plainteks yang sama dengan kunci yang berbeda 1

bit. Kedua, melakukan 2 eksperimen pada plainteks yang berbeda 1 bit dengan kunci yang sama.

Dalam eksperimen ini akan melibatkan 6 buah *file* sebagai plainteks yang akan dienkripsi dalam beberapa kondisi. *File-file* tersebut adalah null_16.exv, null_64.exv, dan null_128.exv yang berisikan karakter *null* dengan ukuran *file* masing-masing 16 byte, 64 byte dan 128 byte. Dan *file-file* random_16.exv, random_64.exv, dan random_128.exv yang berisikan karakter-karakter acak dengan ukuran *file* masing-masing 16 byte, 64 byte dan 128 byte.

Tabel 4.7 Daftar *file* eksperimen

Nama File	Ukuran	Jumlah *SubBlock*
null_16.exv	16 byte	1 buah *SubBlock*
null_64.exv	64 byte	4 buah *SubBlock*
null_128.exv	128 byte	8 buah *SubBlock*
random_16.exv	16 byte	1 buah *SubBlock*
random_64.exv	64 byte	4 buah *SubBlock*
random_128.exv	128 byte	8 buah *SubBlock*

Dan untuk plainteks yang berbeda 1 bit, akan diubah bit terakhir dari masing-masing *file*.

Untuk kunci akan digunakan 2 buah kunci, yaitu kunci 1 yang terdiri dari 16 karakter *null*, dan kunci 2 yang berupa kata ‘putintheblackbox’. Untuk pengujian *Avalanche Effect* dengan kunci berbeda, juga akan dilakukan pengubahan 1 bit pada akhir kunci.

4.2.2.1 Pengujian dengan Kunci Berbeda 1 Bit

Dilakukan eksperimen-eksperimen dengan mengubah bit terakhir dari kunci, baik pada eksperimen yang menggunakan kunci 1 maupun pada eksperimen yang menggunakan kunci 2. Selain melakukan eksperimen dengan file-file yang berbeda dan 2 buah kunci yang berbeda, eksperimen juga dilakukan dengan mengubah jumlah *round* (*Full Round*) pada proses enkripsi. Dilakukan mulai dari 1 *round* hingga 10 *round*. Hasil dari eksperimen dapat dilihat pada tabel 4.7.

Tabel 4.8 Eksperimen dengan perbedaan bit pada kunci

			plainteks						Nilai Rata-Rata
			NULL			*random*			
			16 byte	64 byte	128 byte	16 byte	64 byte	128 byte	
Jumlah *ROUND*	1	Kunci 1	3,91 %	5,47 %	5,47 %	21,88 %	10,94 %	10,94 %	7,55 %
		Kunci 2	2,34 %	3,13 %	6,25 %	5,47 %	3,91 %	10,94 %	
	2	Kunci 1	15,63 %	28,52 %	31,45 %	47,66 %	42,58 %	46,48 %	34,20 %
		Kunci 2	7,81 %	44,34 %	39,26 %	22,66 %	38,67 %	45,31 %	
	3	Kunci 1	34,38 %	49,22 %	46,48 %	46,88 %	50,20 %	52,54 %	45,04 %
		Kunci 2	17,97 %	51,17 %	54,10 %	39,06 %	51,76 %	46,68 %	
	4	Kunci 1	48,44 %	53,71 %	50,00 %	42,97 %	51,17 %	53,52 %	50,31 %
		Kunci 2	55,47 %	50,59 %	46,88 %	52,34 %	50,00 %	48,63 %	
	5	Kunci 1	53,91 %	51,76 %	47,85 %	46,88 %	50,39 %	46,68 %	48,94 %
		Kunci 2	53,13 %	44,73 %	44,73 %	42,97 %	51,76 %	52,54 %	
	6	Kunci 1	49,22 %	50,39 %	51,56 %	53,13 %	50,00 %	50,78 %	49,24 %
		Kunci 2	42,97 %	51,95 %	47,27 %	50,00 %	49,61 %	43,95 %	
	7	Kunci 1	50,78 %	47,66 %	50,39 %	57,03 %	48,44 %	52,15 %	50,29 %
		Kunci 2	47,66 %	49,61 %	50,39 %	53,91 %	47,66 %	47,85 %	
	8	Kunci 1	46,09 %	52,73 %	52,93 %	52,34 %	50,20 %	49,61 %	50,02 %
		Kunci 2	44,53 %	48,24 %	50,59 %	51,56 %	48,24 %	53,13 %	
	9	Kunci 1	57,03 %	47,07 %	55,08 %	47,66 %	46,68 %	46,88 %	49,82 %
		Kunci 2	46,88 %	51,37 %	51,17 %	48,44 %	47,66 %	51,95 %	
	10	Kunci 1	52,34 %	45,70 %	49,80 %	50,00 %	50,00 %	46,68 %	49,76 %
		Kunci 2	53,13 %	45,31 %	51,95 %	49,22 %	51,37 %	51,56 %	

4.2.2.2 Pengujian dengan Plainteks Berbeda 1 Bit

Dilakukan eksperimen-eksperimen seperti pada pengujian dengan kunci berbeda 1 bit, namun kali ini yang berbeda adalah plainteks. Hasil dari eksperimen dapat dilihat pada tabel 4.8.

Tabel 4.9 Eksperimen dengan perbedaan bit pada plainteks

			plainteks						Nilai
			NULL			*random*			
			16 byte	64 byte	128 byte	16 byte	64 byte	128 byte	Rata-Rata
Jumlah *ROUND*	1	Kunci 1	3,13 %	3,13 %	2,73 %	6,25 %	7,03 %	7,03 %	5,79 %
		Kunci 2	4,69 %	5,47 %	4,69 %	10,16 %	7,42 %	7,71 %	
	2	Kunci 1	16,41 %	20,90 %	25,20 %	14,06 %	38,48 %	39,55 %	30,48 %
		Kunci 2	21,88 %	40,63 %	35,16 %	28,91 %	41,02 %	43,55 %	
	3	Kunci 1	45,31 %	50,98 %	51,86 %	43,75 %	50,20 %	46,09 %	49,39 %
		Kunci 2	51,56 %	51,56 %	48,44 %	46,88 %	52,34 %	53,71 %	
	4	Kunci 1	46,88 %	47,85 %	48,63 %	46,09 %	47,07 %	53,03 %	48,41 %
		Kunci 2	53,91 %	47,66 %	47,46 %	42,97 %	52,34 %	46,97 %	
	5	Kunci 1	46,88 %	47,66 %	51,37 %	53,91 %	50,98 %	50,68 %	49,51 %
		Kunci 2	51,56 %	48,24 %	49,41 %	40,63 %	52,34 %	50,49 %	
	6	Kunci 1	52,34 %	50,39 %	49,41 %	49,22 %	54,10 %	51,86 %	51,09 %
		Kunci 2	44,53 %	51,17 %	46,39 %	54,69 %	56,05 %	52,93 %	
	7	Kunci 1	46,88 %	52,15 %	53,42 %	40,63 %	52,54 %	50,59 %	49,99 %
		Kunci 2	50,78 %	49,80 %	50,59 %	50,78 %	49,80 %	51,95 %	
	8	Kunci 1	44,53 %	50,20 %	49,71 %	53,91 %	48,63 %	50,78 %	49,01 %
		Kunci 2	44,53 %	48,44 %	51,27 %	47,66 %	50,98 %	47,46 %	
	9	Kunci 1	57,03 %	50,39 %	49,22 %	48,44 %	51,17 %	51,66 %	51,64 %
		Kunci 2	54,69 %	47,66 %	51,37 %	55,47 %	51,56 %	51,07 %	
	10	Kunci 1	43,75 %	48,63 %	50,88 %	49,22 %	53,13 %	49,80 %	50,00 %
		Kunci 2	46,09 %	50,78 %	48,34 %	52,34 %	55,27 %	51,76 %	

4.2.3 Pengujian Pada Sistem Operasi 32 Bit dan Sistem Operasi 64 Bit

Selain dilakukan pengujian aplikasi secara prosedural dan pengujian keamanan algoritma kriptografi VBR 32 bit menggunakan avalanche effect sebagai parameter, juga dilakukan pengujian implementasi algoritma kriptografi VBR 32 bit pada operating sistem yang berbeda. Dalam hal ini digunakan 2 sistem operasi dengan bit yang berbeda, yaitu Microsoft Widows Vista 32 bit dan Linux openSUSE 64 bit.

Pengujian dilakukan menggunakam plainteks “INFORMATIKA” dengan kunci “putintheblackbox”, dengan jumlah *round* mulai dari 1 hingga 10. Data dari hasil uji sistem operasi dapat dilihat pada tabel 4.9.

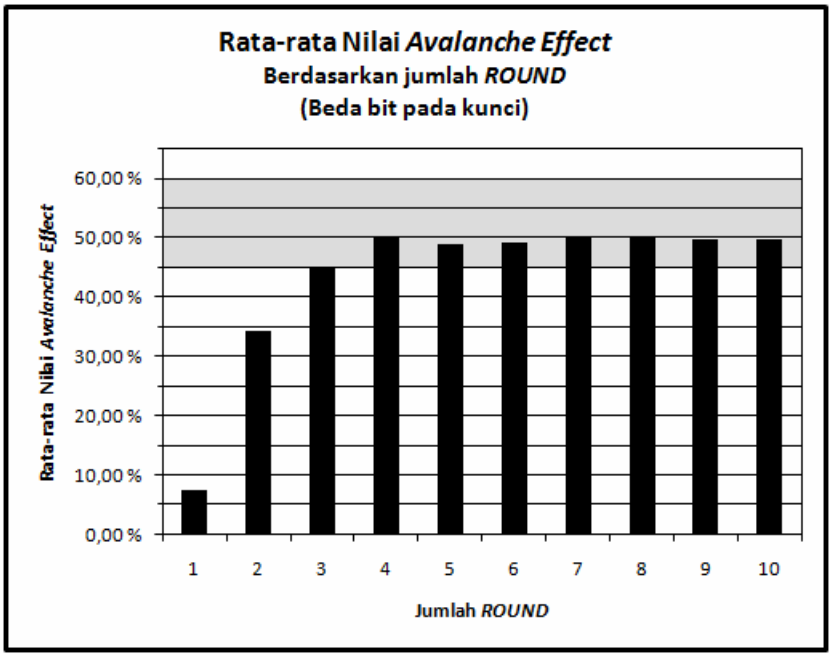
Tabel 4.9 Data pengujian algoritma kriptografi VBR 32 bit pada sistem operasi 32 bit dan sistem operasi 64 bit

JUMLAH ROUND	HASIL HARAPAN	VISTA 32 bit		openSUSE 64 bit	
		HASIL	STATUS	HASIL	STATUS
1	0DF6CBD2 5CA6D7D3 F822F7E7 CD85C01F	0DF6CBD2 5CA6D7D3 F822F7E7 CD85C01F	Sukses	0DF6CBD2 5CA6D7D3 F822F7E7 CD85C01F	Sukses
2	B7ADB70A 37C368C1 7F59445D 714A1E57	B7ADB70A 37C368C1 7F59445D 714A1E57	Sukses	B7ADB70A 37C368C1 7F59445D 714A1E57	Sukses
3	63FD6FB6 0B33F49E EC90D6BA E6274F11	63FD6FB6 0B33F49E EC90D6BA E6274F11	Sukses	63FD6FB6 0B33F49E EC90D6BA E6274F11	Sukses
4	A7E553A5 50DEC7D7 7A181F6F BD9D6DE8	A7E553A5 50DEC7D7 7A181F6F BD9D6DE8	Sukses	A7E553A5 50DEC7D7 7A181F6F BD9D6DE8	Sukses
5	E0A4BEA4 F6C0AE36 5D6E4D53 311482B0	E0A4BEA4 F6C0AE36 5D6E4D53 311482B0	Sukses	E0A4BEA4 F6C0AE36 5D6E4D53 311482B0	Sukses
6	B9F068D5 41F5EADD 0B9DA64D BB4C011D	B9F068D5 41F5EADD 0B9DA64D BB4C011D	Sukses	B9F068D5 41F5EADD 0B9DA64D BB4C011D	Sukses
7	A852FEF3 4AAE22ED 04DB21A0 CA78065E	A852FEF3 4AAE22ED 04DB21A0 CA78065E	Sukses	A852FEF3 4AAE22ED 04DB21A0 CA78065E	Sukses
8	8F476469 A63398A3 FCCF7459 C5AE63E7	8F476469 A63398A3 FCCF7459 C5AE63E7	Sukses	8F476469 A63398A3 FCCF7459 C5AE63E7	Sukses
9	62A81C4E E4C10442 E23A43D2 D7B72A84	62A81C4E E4C10442 E23A43D2 D7B72A84	Sukses	62A81C4E E4C10442 E23A43D2 D7B72A84	Sukses
10	AC3DC986 8F53C01B 3A90A0E0 0076EAC0	AC3DC986 8F53C01B 3A90A0E0 0076EAC0	Sukses	AC3DC986 8F53C01B 3A90A0E0 0076EAC0	Sukses

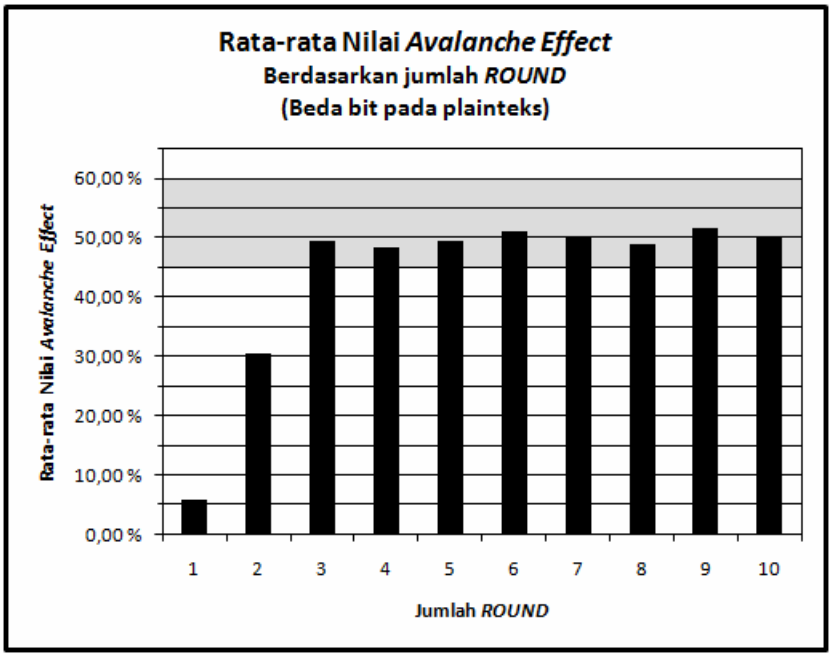
4.3 Analisa Data Eksperimen (Nilai *Avalanche Effect*)

Eksperimen-eksperimen yang dilakukan menghasilkan nilai-nilai *Avalanche Effect* yang akan dijadikan sebagai parameter untuk menilai tingkat keamanan Algoritma Kriptografi VBR. Dari nilai-nilai yang didapatkan dicari rata-rata nilai *Avalanche Effect* berdasarkan jumlah *round*. Dari nilai rata-rata tersebut dapat

dibuat sebuah diagram seperti pada gambar 4.2 untuk eksperimen dengan beda bit pada kunci dan gambar 4.3 untuk beda bit pada plainteks.



Gambar 4.28 Rata-rata nilai *Avalanche Effect* (beda bit pada kunci)



Gambar 4.29 Rata-rata nilai *Avalanche Effect* (beda bit pada plainteks)

Terlihat bahwa nilai *Avalanche Effect* sangat rendah yaitu 7,55 % dengan beda bit pada kunci dan 5,79 % dengan beda bit pada plainteks ketika jumlah *round* yang dipakai adalah 1. Untuk enkripsi dengan 2 *round*, nilai *avalanche effect* mulai naik namun belum mencapai nilai yang baik. Seperti telah disebutkan pada bab II bahwa algoritma kriptografi dikatakan baik bila memiliki nilai *avalanche effect* sekitar 45% hingga 60%, dan data eksperimen menunjukkan hal tersebut tercapai ketika jumlah *round* yang digunakan adalah 3 hingga 10 *round*.

4.4 Analisa Modifikasi Algoritma Kriptografi VBR 32 Bit

Modifikasi pada algoritma kriptografi VBR 32 bit dapat memperbaiki tingkat keamanan algoritma tersebut. Modifikasi tersebut adalah :

1. Modifikasi ukuran tabel bit

   Modifikasi ukuran tabel bit menjadikan algoritma kriptografi VBR 32 bit memiliki jumlah baris maksimal 32 baris, sehingga besar maksimal rotasi yang dilakukan adalah 32 bit. Hal ini memungkinkan algoritma kriptografi VBR 32 bit berjalan pada sistem operasi 32 bit dan sistem operasi 64 bit.

2. Modifikasi Kunci (*K*)

   Penambahan panjang kunci dari 8 byte menjadi 16 byte dapat menambah ketahanan algoritma kriptografi VBR 32 bit terhadap serangan kriptanalis. Selain itu standard untuk panjang kunci pada saat ini adalah 16 byte.

3. Penambahan proses *padding*

   Proses *padding* berguna agar blok penyandian yang ukurannya kurang dari yang telah ditentukan dapat tetap disandikan.

4. Penambahan proses *Add Key* dan *Add SubKey*

   Penambahan proses *Add Key* dan *Add Subkey* bertujuan agar kunci memiliki peran yang besar dalam penyandian selain untuk membangkitkan variabel rotasi.

5. Penambahan proses *Byte Substitution*

   Sebelum dimodifikasi, algoritma kriptografi VBR mengandalkan pergeseran bit untuk penyandian, menyebabkan bit tidak pernah berubah dan hanya berpindah tempat. Faktor ini yang menyebabkan nilai avalanche effect menjadi rendah.

   Penambahan proses *Byte Substitution* oleh *Substitution Box* (*S-Box*) dapat meningkatkan nilai *avalanche effect* pada algoritma kriptografi VBR 32 bit karena bit pada plainteks selain berpindah tempat juga mengalami perubahan.

6. Adanya *Round* pada algoritma kriptografu VBR 32 bit

   Adanya *round* pada algoritma kriptografi VBR 32 bit menambah kompleksitas dari penyandian. Selain itu jumlah dari round yang digunakan dapat bervariasi sehingga menambah tingkat kesulitan seorang kriptanalis dalam memecahkan penyandian menggunakan algoritma kriptografi VBR 32 bit.