



## DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN.....	ii
PERNYATAAN.....	iii
HALAMAN PERSEMBAHAN .....	iv
PRAKATA.....	v
DAFTAR ISI.....	vii
DAFTAR GAMBAR .....	ix
DAFTAR TABEL.....	xi
INTISARI.....	xii
ABSTRACT.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang dan Permasalahan .....	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Keaslian Penulisan .....	3
1.7 Metodologi Penelitian .....	3
1.8 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA.....	6
BAB III LANDASAN TEORI.....	10
3.1 Kriptografi.....	10
3.2 Tujuan Kriptografi.....	10
3.3 Enkripsi Simetris dan Asimetris.....	11
3.4 Mode Enkripsi dan Dekripsi .....	13
3.5 Algoritma Blowfish.....	16
3.5.1 Kotak Permutasi .....	18
3.5.2 Enkripsi Algoritma Blowfish .....	19
3.5.3 Dekripsi Algoritma Blowfish.....	22
3.6 Pemilihan Algoritma Blowfish.....	24
3.7 Keunggulan Cryptosystem yang dibangun .....	25
3.8 Pemrosesan pada PHP Hypertext Preprocessor (PHP).....	26
BAB IV PERANCANGAN SISTEM.....	31
4.1 Deskripsi sistem .....	31
4.2 Masukan <i>Cryptosystem</i> .....	32
4.3 Pemrosesan Masukan .....	32
4.3.1 Proses Pengkopian Isi Folder Masukan .....	32
4.3.2 Proses Enkripsi.....	33
4.3.2 Proses Dekripsi.....	35
4.5 Desain Pengujian.....	37
4.5.1 Pengujian Berbagai Masukan.....	37
4.5.2 Pengujian Kunci Enkripsi.....	38



4.5.3 Pengujian PHP <i>Extension</i> .....	38
4.5.4 Pengujian Keterbacaan Kode Di Memori .....	40
4.5.5 Pengujian Waktu Eksekusi .....	41
<b>BAB V IMPLEMENTASI.....</b>	<b>42</b>
5.1 PHP <i>Extension</i> .....	42
5.2 Alur Kerja PHP <i>Extension</i> .....	46
5.3 Implementasi Algoritma Blowfish .....	50
<b>BAB VI HASIL PENELITIAN DAN PEMBAHASAN.....</b>	<b>64</b>
6.1 Pengujian Berbagai Masukan.....	64
6.2 Pengujian Kunci Enkripsi.....	65
6.3 Pengujian PHP <i>Extension</i> .....	69
6.4 Pengujian Keterbacaan Kode Di Memori .....	70
6.5 Pengujian Waktu Eksekusi .....	70
<b>BAB VII KESIMPULAN DAN SARAN .....</b>	<b>73</b>
7.1 Kesimpulan.....	73
7.2 Saran.....	73
<b>DAFTAR PUSTAKA .....</b>	<b>74</b>



## DAFTAR GAMBAR

Gambar 3.1 Proses Kriptografi Kunci Simetris .....	12
Gambar 3.2 Proses Kriptografi Kunci Publik .....	12
Gambar 3.3 Blok Algoritma pada Mode CBC (Arius, 2008) .....	13
Gambar 3.4 Jaringan Feistel.....	21
Gambar 3.5 Tahapan Fungsi F .....	22
Gambar 3.6 Diagram Skema Dekripsi Algoritma Blowfish .....	24
Gambar 3.7 Alur Eksekusi Kode PHP.....	25
Gambar 3.8 Langkah Pemrosesan File PHP sampai Output (Sklar, 2004).....	27
Gambar 4.1 Gambaran Umum <i>Cryptosystem</i> .....	29
Gambar 4.2 Proses Enkripsi .....	34
Gambar 4.3 Proses Dekripsi.....	35
Gambar 4.4 Alur Pengolahan Data dengan PHP <i>Extension</i> .....	39
Gambar 5.1 Proses phpize pada Komputer Server.....	43
Gambar 5.2 Proses Perintah ./configure.....	43
Gambar 5.3 Proses Perintah make .....	44
Gambar 5.4 Hasil Kompilasi menggunakan make.....	45
Gambar 5.5 Penambahan PHP <i>extension</i> pada File php.ini .....	45
Gambar 5.6 PHP <i>Extension Blowfish Protector</i> sudah aktif.....	46
Gambar 5.7 Pemanggilan File yang Dibutuhkan Dalam Fungsi Dekripsi.....	47
Gambar 5.8 Fungsi untuk Mengambil Masukan .....	48
Gambar 5.9 Fungsi PHP_MINFO_FUNCTION .....	48
Gambar 5.10 Fungsi bfprotector_decrypt .....	49
Gambar 5.11 Variabel Konstan .....	50
Gambar 5.12 Variabel Konstan Mode Padding .....	50
Gambar 5.13 Fungsi Blowfish .....	51
Gambar 5.14 <i>Function Encrypt</i> .....	52
Gambar 5.15 Pengecekan Mode CBC .....	52
Gambar 5.16 Inisiasi Awal Fungsi <i>Encrypt</i> .....	52
Gambar 5.17 Perulangan Pembagian Blok Enkripsi.....	57
Gambar 5.18 Fungsi <i>Decrypt</i> .....	54
Gambar 5.19 Inisiasi Awal Fungsi <i>Decrypt</i> .....	54
Gambar 5.20 Perulangan dan Pembagian Blok Dekripsi.....	54
Gambar 5.21 Fungsi Feistel .....	55
Gambar 5.22 Array P-Box .....	56
Gambar 5.23 S-Box yang Pertama.....	57
Gambar 5.24 S-Box yang Kedua .....	58
Gambar 5.25 S-Box yang Ketiga .....	59
Gambar 5.26 S-Box yang Keempat .....	60
Gambar 5.27 Kode Program untuk Mengkopi File.....	61
Gambar 5.28 Kode Program untuk Membaca Folder .....	62
Gambar 6.1 Grafik Waktu Eksekusi Proses Enkripsi .....	65
Gambar 6.2 Kode untuk membuat Kunci .....	66



Gambar 6.3 Kode Sebelum Enkripsi dengan Kunci 1 .....	66
Gambar 6.4 Keluaran pada <i>Web Browser</i> dengan Kunci 1 .....	66
Gambar 6.5 Kode Asli Sebelum Enkripsi .....	68
Gambar 6.6 Kode Setelah Enkripsi .....	69
Gambar 6.7 Keluaran File PHP Terenkripsi .....	69
Gambar 6.8 Hasil Baca Memori menggunakan Ltrace .....	69
Gambar 6.9 Pengujian dengan PHPUnit .....	70
Gambar 6.10 Grafik Perbandingan Waktu Eksekusi .....	71



## DAFTAR TABEL

Tabel 2.1 Daftar Perbandingan Penelitian Sebelumnya.....	8
Tabel 3.1 <i>Throughput</i> dari DES, 3DES, AES, dan Blowfish, (Mandal, 2012).....	25
Tabel 6.1 Hasil Pengujian Masukan .....	64
Tabel 6.2 Hasil Pengujian Penggunaan Berbagai Kunci .....	66
Tabel 6.3 Hasil Perbandingan Waktu Eksekusi .....	71



## DAFTAR RUMUS

Rumus 4.1 Rumus <i>Throughput</i> .....	25
---	----