



**PENERAPAN ALGORITMA KOMPRESI LZW DAN
ALGORITMA KRIPTOGRAFI *TWOFISH* DALAM
PENGAMANAN *FILE* DIGITAL**

SKRIPSI

CLARISSA NABILA

1710511042

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN

JAKARTA

2021



**PENERAPAN ALGORITMA KOMPRESI LZW DAN
ALGORITMA KRIPTOGRAFI *TWOFISH* DALAM
PENGAMANAN *FILE* DIGITAL**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar
Sarjana Komputer**

CLARISSA NABILA

1710511042

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN

JAKARTA

2021

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Clarissa Nabila

NIM : 1710511042

Tanggal : 14 Juni 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 14 Juni 2021

Yang Menyatakan,



SEPUULUH RIBU RUPIAH
TEL
20
METERAI
TEMPEL
BC19AJX262580453
(Clarissa Nabila)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Clarissa Nabila

NIM : 1710511042

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

**Penerapan Algoritma Kompresi LZW dan Algoritma Kriptografi *Twofish*
dalam Pengamanan *File Digital***

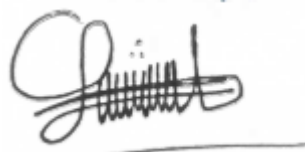
Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 14 Juni 2021

Yang menyatakan,



(Clarissa Nabila)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

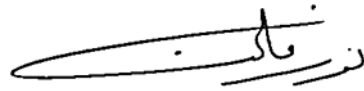
Nama : Clarissa Nabila
NIM : 1710511042
Program Studi : Informatika
Judul : Penerapan Algoritma Kompresi LZW dan Algoritma Kriptografi *Twofish* dalam Pengamanan *File* Digital

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S-1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Yuni Widiastiwi, S.Kom., M.SI.

Penguji 1



Noor Falih, S.Kom., M.T.

Penguji 2



Henki Bayu Seta, S.Kom., M.TI.

Pembimbing 1



Ing. Artambo B. Pangaribuan, M.Eng.

Pembimbing 2



Dr. E. Matita, M.Kom.

Dekan Fakultas Ilmu Komputer



Yuni Widiastiwi, S.Kom., M.SI.

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Persetujuan : 20 Juli 2021



PENERAPAN ALGORITMA KOMPRESI LZW DAN ALGORITMA KRIPTOGRAFI *TWOFISH* DALAM PENGAMANAN *FILE* DIGITAL

Clarissa Nabila

ABSTRAK

Pada era digitalisasi ini penggunaan berkas tidak hanya berwujud cetak, namun dapat berbentuk *file* digital yang memiliki keuntungan salah satunya dalam kemudahan untuk menyimpan *file* ke dalam perangkat penyimpanan *file* digital secara *offline* maupun *online*. Namun, menyimpan *file* yang belum diberi perlindungan dapat mengancam keamanan terhadap kerahasiaan informasi dari *file* tersebut. Oleh karena itu, dalam penelitian ini menggunakan metode algoritma kompresi LZW untuk mengurangi redundansi data dan kriptografi *Twofish* untuk memberikan perlindungan keamanan terhadap kerahasiaan dari isi *file* digital. Dalam hasil penelitian ini memperoleh hasil bahwa penggabungan algoritma kompresi LZW dan kriptografi *Twofish* berhasil mengamankan isi dari *file* digital berupa *file* teks (*.txt), *Word*, *Excel*, dan PDF dengan menghasilkan *ciphertext* yang acak berdasarkan pengujian *frequency test*. Ukuran dari *file* digital yang diproses mempengaruhi waktu komputasi yang diperlukan untuk proses *encode* dan *decode*. Proses *encode* berhasil merubah *file* menjadi tidak terbaca maknanya, serta proses *decode* berhasil mengembalikan *file* hasil *encode* menjadi seperti aslinya sehingga dapat terbaca maknanya.

Kata Kunci: Kompresi, Kriptografi, LZW, *Twofish*, *File* digital

**IMPLEMENTATION OF LZW COMPRESSION ALGORITHM
AND TWOFISH CRYPTOGRAPHY ALGORITHM IN SECURING
DIGITAL FILE**

Clarissa Nabila

ABSTRACT

In this era of digitalization, the use of files is not only in the form of print, but can be in the form of digital files, one of which has the advantage of being able to store files into digital file storage devices offline and online. However, storing files that have not been given protection can threaten the security of the confidentiality of the information from the file. Therefore, this study uses the LZW compression algorithm method to reduce data redundancy and Twofish cryptography to provide security protection against the confidentiality of digital file contents. The results of this study show that the combination of the LZW compression algorithm and the Twofish cryptography has succeeded in securing the contents of digital files in the form of text files (.txt), Word, Excel, and PDF by generating random ciphertext based on the frequency test. The size of the processed digital files affects the computation time required for the encode and decode processes. The encoding process succeeded in changing the file to illegible meaning, and the decoding process succeeded in returning the encoded file to its original state so that its meaning could be read.*

Keywords: *Compression, Cryptography, LZW, Twofish, Digital File*

KATA PENGANTAR

Dengan ini penulis panjatkan puji dan syukur terhadap Allah SWT atas rahmat yang sudah diberikan, sehingga penulis bisa selesai mengerjakan Skripsi ini dengan judul “Penerapan Algoritma Kompresi LZW dan Algoritma Kriptografi *Twofish* dalam Pengamanan *File* Digital”. Dalam pengerjaan Skripsi ini tak lepas dari bimbingan, saran, serta doa dari beragam pihak. Pada kesempatan ini, penulis hendak menuturkan ucapan terima kasih kepada:

- a. Ibu Dr. Ermatita, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
- b. Ibu Yuni Widiastiwi, S.Kom., M.Si., selaku Ketua Program Studi S1 Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
- c. Bapak Henki Bayu Seta, S.Kom., M.TI., selaku dosen pembimbing I.
- d. Bapak Ing. Artambo B. Pangaribuan, M.Eng., selaku dosen pembimbing II.
- e. Orang tua dan keluarga yang selalu memberikan dukungan dan doa terhadap penulis agar dapat mengerjakan Skripsi dengan baik.
- f. Seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah memberikan ilmunya kepada penulis.
- g. Seluruh pihak yang belum disebutkan penulis yang sudah memberikan dukungan dan bantuan, sehingga Skripsi ini dapat dikerjakan dan diselesaikan dengan baik.

Jakarta, 20 Juli 2021

Penulis

DAFTAR ISI

HALAMAN SAMBUL	i
HALAMAN JUDUL.....	ii
PERNYATAAN ORISINALITAS	iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI	iv
LEMBAR PENGESAHAN	v
ABSTRAK	vi
<i>ABSTRACT</i>	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL.....	xv
DAFTAR SIMBOL.....	xvi
DAFTAR LAMPIRAN.....	xviii
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Rumusan Masalah.....	4
I.3 Ruang Lingkup Penelitian.....	4
I.4 Tujuan Penelitian	4
I.5 Manfaat Penelitian	5
I.6 Luaran yang diharapkan.....	5
I.7 Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
II.1 Keamanan Informasi	7
II.2 Kompresi Data	8
II.2.1 Kompresi <i>Lossy</i>	8
II.2.2 Kompresi <i>Lossless</i>	8
II.3 Algoritma Lempel-Ziv-Welch (LZW).....	8
II.4 Rasio Kompresi	10
II.5 Kriptografi.....	11
II.5.1 Struktur Sistem Kriptografi.....	11
II.5.2 Kriptografi Kunci Publik (Asimetris)	12

II.5.3	Kriptografi Kunci Privat (Simetris).....	12
II.6	Algoritma Kriptografi <i>Twofish</i>	13
II.6.1	Tabel Permutasi q_0 dan q_1	17
II.6.2	Penjadwalan kunci.....	18
II.6.3	Perluasan Kunci.....	20
II.6.4	Fungsi F	20
II.6.5	Fungsi h	21
II.7	<i>Cipher Block Chaining</i> (CBC).....	23
II.8	<i>Frequency Test</i>	25
II.9	Penelitian Relevan	26
BAB III	METODOLOGI PENELITIAN.....	30
III.1	Kerangka Berpikir	30
III.2	Metode Penelitian.....	31
III.2.1	Identifikasi Masalah.....	31
III.2.2	Pengumpulan Data	31
III.2.3	Analisis	31
III.2.4	Perancangan	32
III.2.5	Implementasi.....	34
III.2.6	Pengujian.....	34
III.2.7	Hasil dan Kesimpulan	35
III.3	Alat dan Bahan Penelitian	36
III.3.1	Alat Penelitian.....	36
III.3.2	Bahan Penelitian	36
III.4	Jadwal Penelitian	36
BAB IV	HASIL DAN PEMBAHASAN	38
IV.1	Identifikasi Masalah.....	38
IV.2	Analisis Proses <i>Encode</i>	38
IV.3	Analisis Proses <i>Decode</i>	90
IV.4	Analisis Kebutuhan Aplikasi	131
IV.5	Gambaran Umum Aplikasi	132
IV.6	Perancangan Aplikasi.....	133
IV.6.1	<i>Use Case Diagram</i>	133
IV.6.2	<i>Activity Diagram</i>	137
IV.6.3	<i>Sequence diagram</i>	140

IV.6.4	Perancangan <i>User Interface</i> (Antarmuka Pengguna)	142
IV.7	Implementasi.....	145
IV.8	Pengujian.....	154
IV.8.1	Pengujian Pencocokan	154
IV.8.2	Pengujian Rasio Kompresi dan Waktu Komputasi.....	158
IV.8.3	Pengujian <i>Frequency Test</i>	163
BAB V	PENUTUP.....	166
V.1	Kesimpulan	166
V.2	Saran	167
DAFTAR	PUSTAKA	168
DAFTAR	RIWAYAT HIDUP.....	170
LAMPIRAN	171

DAFTAR GAMBAR

Gambar 2.1 Kriptografi Kunci Publik (Asimetris)	12
Gambar 2.2 Kriptografi Kunci Privat (Simetris).....	13
Gambar 2.3 Struktur Desain Algoritma Twofish.....	14
Gambar 2.4 <i>S-box</i> Permutasi q_0	18
Gambar 2.5 <i>S-box</i> Permutasi q_1	18
Gambar 2.6 Skema Enkripsi Mode CBC	23
Gambar 2.7 Skema Dekripsi Mode CBC.....	24
Gambar 3.1 Kerangka Berpikir	30
Gambar 3.2 Skema Proses Kompresi-Enkripsi.....	33
Gambar 3.3 Skema Proses Dekripsi-Dekompresi.....	34
Gambar 4.1 Proses Kompresi LZW	39
Gambar 4.2 Isi dari <i>File Input</i>	40
Gambar 4.3 Isi dari <i>File</i> dalam <i>Hexa</i>	40
Gambar 4.4 Hasil Kompresi.....	44
Gambar 4.5 Hasil Kompresi dengan Panjang 12-bit.....	46
Gambar 4.6 String Biner Hasil Kompresi	47
Gambar 4.7 Hasil Akhir Proses Kompresi LZW	49
Gambar 4.8 Proses Penjadwalan dan Perluasan Kunci	51
Gambar 4.9 Kunci dalam <i>Hexa</i>	52
Gambar 4.10 Hasil Perluasan Kunci	62
Gambar 4.11 Proses Enkripsi <i>Twofish</i> mode CBC	63
Gambar 4.12 <i>Plaintext</i> untuk Proses Enkripsi	64
Gambar 4.13 Blok <i>Plaintext</i> 128-bit	64
Gambar 4.14 Operasi XOR <i>Plaintext</i> dengan IV	64
Gambar 4.15 Blok <i>Ciphertext</i> 1	87
Gambar 4.16 Blok <i>Plaintext</i> 2 XOR Blok <i>Ciphertext</i> 1.....	87
Gambar 4.17 Blok <i>Ciphertext</i> 2	87
Gambar 4.18 Blok <i>Plaintext</i> 3 XOR Blok <i>Ciphertext</i> 2.....	88
Gambar 4.19 Blok <i>Ciphertext</i> 3	88
Gambar 4.20 Blok <i>Plaintext</i> 4 XOR Blok <i>Ciphertext</i> 3.....	88
Gambar 4.21 Blok <i>Ciphertext</i> 4	88
Gambar 4.22 Blok <i>Plaintext</i> 5 XOR Blok <i>Ciphertext</i> 4.....	89



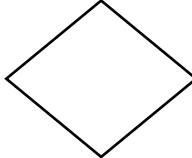






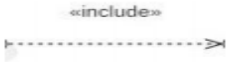
Gambar 4.23 Blok <i>Ciphertext</i> 5	89
Gambar 4.24 <i>Padding</i> Blok <i>Plaintext</i> 6	89
Gambar 4.25 Blok <i>Plaintext</i> 6 XOR Blok <i>Ciphertext</i> 5.....	90
Gambar 4.26 Blok <i>Ciphertext</i> 6	90
Gambar 4.27 Keseluruhan Hasil <i>Ciphertext</i>	90
Gambar 4.28 Proses Dekripsi <i>Twofish</i> CBC.....	92
Gambar 4.29 <i>Ciphertext</i> dalam <i>Hexa</i>	92
Gambar 4.30 Blok <i>Ciphertext</i> 128-bit.....	93
Gambar 4.31 Blok <i>Plaintext</i> 1.....	117
Gambar 4.32 Operasi XOR Blok <i>Plaintext</i> 1 dengan IV	117
Gambar 4.33 Blok <i>Plaintext</i> 2.....	118
Gambar 4.34 Blok <i>Plaintext</i> 2 XOR Blok <i>Ciphertext</i> 1.....	118
Gambar 4.35 Blok <i>Plaintext</i> 3.....	118
Gambar 4.36 Blok <i>Plaintext</i> 3 XOR Blok <i>Ciphertext</i> 2.....	119
Gambar 4.37 Blok <i>Plaintext</i> 4.....	119
Gambar 4.38 Blok <i>Plaintext</i> 4 XOR Blok <i>Ciphertext</i> 3.....	119
Gambar 4.39 Blok <i>Plaintext</i> 5.....	119
Gambar 4.40 Blok <i>Plaintext</i> 5 XOR Blok <i>Ciphertext</i> 4.....	120
Gambar 4.41 Blok <i>Plaintext</i> 6.....	120
Gambar 4.42 Blok <i>Plaintext</i> 6 XOR Blok <i>Ciphertext</i> 5.....	120
Gambar 4.43 Hasil <i>Unpadding</i> Blok <i>Plaintext</i> 6	120
Gambar 4.44 Keseluruhan Hasil <i>Plaintext</i>	121
Gambar 4.45 Skema Proses Dekompresi LZW	122
Gambar 4.46 Isi <i>File</i> Hasil <i>Decode</i> dalam <i>Hexa</i>	123
Gambar 4.47 <i>String</i> Biner	125
Gambar 4.48 <i>Output</i> Hasil Dekompresi.....	130
Gambar 4.49 <i>Output</i> Hasil <i>Decode</i>	130
Gambar 4.50 Gambaran Umum Aplikasi	133
Gambar 4.51 <i>Use Case Diagram</i>	134
Gambar 4.52 <i>Activity Diagram Encode</i>	138
Gambar 4.53 <i>Activity Diagram Decode</i>	139
Gambar 4.54 <i>Sequence Diagram Encode</i>	141
Gambar 4.55 <i>Sequence Diagram Decode</i>	142
Gambar 4.56 Rancangan <i>Form Encode</i> dan <i>Decode</i>	143



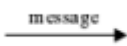


Gambar 4.57 Rancangan Tampilan <i>Menu Help</i>	144
Gambar 4.58 Rancangan Tampilan <i>Menu About</i>	144
Gambar 4.59 Tampilan Awal Aplikasi	146
Gambar 4.60 Tampilan Saat Memilih <i>File</i>	146
Gambar 4.61 Tampilan Saat Telah <i>Input File</i> dan <i>Key</i>	147
Gambar 4.62 Tampilan <i>Show Key</i>	148
Gambar 4.63 Tampilan Saat Proses <i>Encode</i> atau <i>Decode</i>	148
Gambar 4.64 Tampilan Saat Proses <i>Encode</i> Selesai.....	149
Gambar 4.65 Tampilan Saat Proses <i>Decode</i> Selesai.....	150
Gambar 4.66 Tampilan Peringatan Kolom <i>File Kosong</i> Pada Proses <i>Encode</i> ...	151
Gambar 4.67 Tampilan Peringatan Kolom <i>File Kosong</i> Pada Proses <i>Decode</i> ...	151
Gambar 4.68 Tampilan Peringatan Kolom Kunci Kosong	151
Gambar 4.69 Tampilan Peringatan Salah <i>Input File Encode</i>	152
Gambar 4.70 Tampilan Peringatan Salah <i>Input File Decode</i>	152
Gambar 4.71 Tampilan Peringatan <i>Input File</i> Lebih dari 50 MB.....	152
Gambar 4.72 Tampilan Saat <i>Input</i> Kunci Lebih dari 32 Karakter.....	153
Gambar 4.73 Tampilan <i>Menu Help</i>	153
Gambar 4.74 Tampilan <i>Menu About</i>	154
Gambar 4.75 Isi <i>File Plaintext</i>	154
Gambar 4.76 Isi dari <i>File Plaintext</i> dalam <i>Hexa</i>	155
Gambar 4.77 <i>Ciphertext</i> Hasil Perhitungan Manual	155
Gambar 4.78 <i>Ciphertext</i> dari Hasil Aplikasi.....	155
Gambar 4.79 Isi <i>Ciphertext</i> dari Hasil Aplikasi.....	156
Gambar 4.80 Isi dari <i>File Ciphertext</i> dalam <i>Hexa</i>	156
Gambar 4.81 <i>Plaintext</i> Bentuk <i>Hexa</i> Hasil Perhitungan Manual	157
Gambar 4.82 <i>Plaintext</i> Bentuk <i>Char</i> Hasil Perhitungan Manual.....	157
Gambar 4.83 <i>Plaintext</i> Bentuk <i>Hexa</i> dari Hasil Aplikasi	158
Gambar 4.84 <i>Plaintext</i> Bentuk <i>Char</i> dari Hasil Aplikasi	158
Gambar 4.85 Hasil Pengujian <i>Encode</i>	159
Gambar 4.86 Hasil Pengujian <i>Decode</i>	162
Gambar 4.87 Hasil Pengujian <i>Frequency Test</i>	164

DAFTAR TABEL

Tabel 3.1 Jadwal Penelitian.....	37
Tabel 4.1 Langkah 3 Kompresi LZW	41
Tabel 4.2 Langkah 4 Kompresi LZW	41
Tabel 4.3 Langkah 5 Kompresi LZW	41
Tabel 4.4 Langkah 6 & 7 Kompresi LZW	42
Tabel 4.5 Keseluruhan Proses Kompresi LZW.....	42
Tabel 4.6 Bit Hasil Akhir Proses Kompresi.....	48
Tabel 4.7 <i>Input</i> Data Proses Dekompresi.....	123
Tabel 4.8 Kode <i>Index</i> untuk <i>Input</i> Proses Dekompresi.....	125
Tabel 4.9 Proses Pengambilan <i>Input</i> Pertama.....	126
Tabel 4.10 Terjemahan Kode <i>Index</i> Pertama.....	127
Tabel 4.11 <i>Output</i> Hasil Terjemahan	127
Tabel 4.12 Proses Pengambilan Kode <i>Index</i> Selanjutnya.....	127
Tabel 4.13 Terjemahan Kode <i>Index</i> Selanjutnya	127
Tabel 4.14 <i>Output</i> Nilai <i>Current</i>	128
Tabel 4.15 Penambahan Nilai Kombinasi ke Kamus	128
Tabel 4.16 Perubahan Nilai <i>Previous</i>	128
Tabel 4.17 Keseluruhan Proses Dekompresi LZW	128
Tabel 4.18 <i>Use Case Encode</i>	134
Tabel 4.19 <i>Use Case Decode</i>	136
Tabel 4.20 Contoh Kompresi LZW	161

DAFTAR SIMBOL

Nama Komponen	Keterangan	Simbol
<i>Terminal</i>	Simbol yang berfungsi untuk permulaan atau akhir dari suatu kegiatan.	
<i>Process</i>	Simbol yang berfungsi untuk menyatakan suatu proses yang dilakukan oleh komputer.	
<i>Decision</i>	Simbol yang berfungsi untuk menunjukkan suatu kondisi tertentu yang akan menghasilkan dua kemungkinan jawaban yaitu ya atau tidak.	
<i>Input / Output</i>	Simbol yang berfungsi untuk menyatakan proses <i>input / output</i> tanpa tergantung jenis peralatannya.	
<i>Predefine Process</i>	Simbol yang berfungsi untuk pelaksanaan suatu bagian (<i>sub-program</i>) atau prosedur.	
<i>Flowline</i>	Simbol yang berfungsi untuk menunjukkan bagian instruksi selanjutnya.	
<i>Use Case</i>	Penjelasan dari fungsi kegunaan sistem yang dirancang.	
<i>Actor</i>	Memvisualisasikan peran yang berinteraksi dengan sistem.	
<i>Association</i>	Menghubungkan antara komponen <i>actor</i> dan <i>use case</i> .	
<i>Include</i>	Menunjukkan bahwa suatu <i>use case</i> merupakan bagian dari <i>use case</i> lain.	

<i>Lifeline</i>	Mengindikasikan keberadaan sebuah <i>object</i> dalam basis waktu.	
<i>Activation</i>	Mengindikasikan sebuah <i>object</i> yang akan melakukan sebuah aksi.	
<i>Message</i>	Mengindikasikan komunikasi antar <i>object</i> .	
<i>Initial Node</i>	Simbol yang menunjukkan kegiatan aktivitas dimulai.	
<i>Activity Final Node</i>	Simbol yang menunjukkan kegiatan aktivitas berakhir.	

DAFTAR LAMPIRAN

Lampiran 1	Tabel ASCII	171
Lampiran 2	Tabel Awal Kamus	173
Lampiran 3	Tabel Permutasi q_0 dan q_1	175
Lampiran 4	Tabel Nilai ERFC	179
Lampiran 5	Hasil Cek Turnitin	180