

# ABSTRACT

*Nowadays in the age of information, many people using internet for communication and transferring data. The security aspect in data transaction is one of the most important aspect. One of the solutions to handle this is with data encoding or encryption.*

*The encryption method encodes the data, so anyone can not read the information of data except the owner. There are two general types of encryption algorithm, symmetric algorithm and asymmetric algorithm. The Algorithm which used in this book is symmetric algorithm. Symmetric algorithm encodes and decodes with the same key.*

*In this project has successfully built an encryption software using CAST algorithm with Delphi as programming language.*

# DAFTAR ISI

ABSTRACT .....	i
ABSTRAK .....	ii
KATA PENGANTAR .....	iii
DAFTAR ISI .....	v
DAFTAR GAMBAR .....	<a href="#">ix</a>
DAFTAR TABEL .....	xi
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Identifikasi Masalah .....	1
1.3 Tujuan .....	2
1.4 Pembatasan Masalah .....	2
1.5 Spesifikasi Hardware .....	2
1.6 Spesifikasi Software .....	2
1.7 Sistematika Pembahasan .....	3
BAB II TEORI PENUNJANG .....	4
2.1 Kriptografi .....	4
2.1.1 Tujuan Kriptografi .....	7
2.2 Enkripsi dan Dekripsi Menggunakan Kunci .....	8
2.3 Algoritma Simetri Dan Algoritma Asimetri .....	9
2.3.1 Algoritma Simetri .....	9

2.3.2	Algoritma Asimetri .....	10
2.4	Mode Operasi Enkripsi Blok Cipher.....	12
2.5	Teori Matematika.....	13
2.5.1	Bilangan Prima.....	14
2.5.2	Operasi Modulus .....	15
2.5.3	Algoritma Euclidean .....	16
2.5.4	Algoritma <i>Extended Euclidean</i> .....	16
2.5.5	Eksponensial Modulus .....	17
2.5.6	Fungsi XOR .....	20
2.6	Enkripsi Dengan Algoritma CAST-128.....	20
2.6.1	Pasangan Kunci Round .....	22
2.6.2	Non-Identical <i>Rounds</i> .....	22
2.6.3	Substitution Box .....	23
2.6.4	Pengolahan Kunci .....	23
2.6.5	Masking dan Rotasi Sub Kunci.....	27
2.6.6	Panjang dari Kunci Yang Bervariasi.....	27
2.7	Algoritma Validasi Data .....	28
2.8	Tanda Tangan Digital.....	28
2.8.1	Algoritma Pembangkit Kunci Tanda Tangan Digital .....	29
2.8.2	Algoritma Tanda Tangan Digital .....	29
2.8.3	Algoritma Verifikasi Tanda Tangan Digital .....	29
BAB III	Perancangan dan Realisasi Perangkat Lunak.....	30

3.1	Pengolahan Kunci CAST-128.....	30
3.2	Program Enkripsi .....	32
3.3	Program Dekripsi .....	35
3.4	Program Pembangkit Kunci Tanda Tangan Digital .....	38
3.4.1	Sub Program rdmprime .....	39
3.4.2	Sub Program gcd .....	40
3.4.3	Sub Program Euclid .....	40
3.4.4	Program Tanda Tangan Digital .....	42
3.4.5	Program Validasi.....	42
3.4.6	Sub Program Pangkatmod.....	43
3.5	Realisasi Program .....	45
3.5.1	Tampilan Menu Utama .....	45
3.5.2	Program Enkripsi .....	46
3.5.3	Program Dekripsi .....	47
3.5.4	Program <i>Timer</i> .....	48
BAB IV Data Pengamatan .....		49
4.1	Hasil Pengamatan Sederhana Program Enkripsi dan Dekripsi CAST-128 .....	49
4.1.1	Pengamatan Enkripsi CAST-128 Dengan Kunci Yang Sama .....	49
4.1.2	Pengamatan Enkripsi CAST-128 Dengan Kunci Yang Berbeda..	52
4.2	Hasil Pengamatan Program Enkripsi dan Dekripsi CAST-128 Dengan Menggunakan File.....	55

4.2.1	Proses Enkripsi CAST-128 Dengan Menggunakan File.....	55
4.2.2	Proses Dekripsi CAST-128 Dengan Menggunakan File .....	59
4.3	Hasil Pengamatan Waktu Dan Ukuran File Proses Enkripsi Dan Dekripsi CAST-128 .....	62
4.3.1	Pengamatan Enkripsi Dan Dekripsi Dengan Menggunakan Kunci Yang Sama .....	62
4.3.2	Pengamatan Enkripsi Dan Dekripsi Dengan Menggunakan Kunci Yang Berbeda.....	63
4.4	Hasil Pengamatan Proses Tanda Tangan Digital .....	65
4.5	Pengamatan Hasil Proses Validasi .....	66
4.6	Analisa Hasil Pengamatan .....	70
BAB V Kesimpulan Dan Saran.....		72
5.1	Kesimpulan .....	72
5.2	Saran.....	72
Daftar Pustaka .....		73
Lampiran A Listing Program .....		A-1
Lampiran B Subtitution Box .....		B-1
Lampiran C Tampilan Program .....		C-1

## DAFTAR GAMBAR

Gambar 2.1.... Kriptografi dengan proses enkripsi dan dekripsi .....	6
Gambar 2.3 Kriptografi Asimetri .....	11
Gambar 3.1 Diagram Alur Pengolahan <i>Plaintext</i> .....	32
Gambar 3.2 Diagram Alur Proses Enkripsi .....	34
Gambar 3.3 Diagram Alur Proses Dekripsi .....	37
Gambar 3.4 Diagram Alur Program Pembangkit Kunci Tanda Tangan Digital .....	38
Gambar 3.5 Diagram Alir Sub Program RdmPrime .....	39
Gambar 3.6 Diagram Alir Sub Program gcd .....	40
Gambar 3.7 Diagram Alir Sub Program Euclid .....	41
Gambar 3.8 Diagram Alir Program Tanda Tangan Digital .....	42
Gambar 3.9 Diagram Alir Program Validasi .....	43
Gambar 3.10 Diagram Alir Sub Program pangkatmod .....	44
Gambar 3.11 Tampilan Menu Utama .....	45
Gambar 3.12 Tampilan Program Enkripsi .....	46
Gambar 3.13 Tampilan Program Dekripsi .....	47
Gambar 4.1 Tampilan program enkripsi algoritma <i>CAST-128</i> dengan <i>plaintext</i> “industri” kunci “enkripsi” .....	50
Gambar 4.2 Tampilan program dekripsi algoritma <i>CAST-128</i> dengan <i>plaintext</i> “industri” kunci “enkripsi” .....	51

Gambar 4.3	Tampilan program enkripsi algoritma <i>CAST-128</i> dengan <i>plaintext</i> “Algoritma”, kunci “test” .....	53
Gambar 4.4	Tampilan program enkripsi algoritma <i>CAST-128</i> dengan <i>plaintext</i> “Algoritma”, kunci “test” .....	54
Gambar 4.5	Tampilan program enkripsi dari <i>file plain.txt</i> dengan menggunakan kunci “cast-128”, disimpan dalam file <i>cipher.cip</i> .....	57
Gambar 4.6	Tampilan program dekripsi dari <i>file cipher.cip</i> dengan menggunakan kunci “cast-128”, disimpan dalam file <i>plain1.txt</i> .....	60
Gambar 4.7	Pengecekan Validasi .....	66

## DAFTAR TABEL

Tabel 2.1	Nilai <i>Extended Euclidean</i> .....	17
Tabel 4.1	Enkripsi dan dekripsi menggunakan kunci yang sama, <i>plaintext</i> yang berbeda-beda .....	49
Tabel 4.2	Enkripsi dan dekripsi menggunakan kunci yang sama, <i>plaintext</i> yang berbeda-beda .....	52
Tabel 4.3	Hasil Pengamatan Proses Enkripsi CAST-128 .....	61
Tabel 4.4	Hasil Pengamatan Proses Dekripsi CAST-128 .....	62
Tabel 4.5	Hasil pengamatan Enkripsi file menggunakan kunci yang berbeda, <i>plaintext</i> yang sama .....	63
Tabel 4.6	Hasil pengamatan Enkripsi file menggunakan kunci yang berbeda, <i>plaintext</i> yang sama .....	63