

ABSTRACT

Nowadays, Information exchange become more easy as the technology progress growing fast. This could unite people from around the world without knowing time and place. Cryptography has become an important thing when there are trouble in information security.

Cryptography function that can protect information during transmission is an attempt to avoid information from non-important person. With cryptography, information will be convert to a worthless message which cannot be understood by anyone that have not relation with it. The message can be transmitted securely to receiver and then transform it again into the first message.

One of the cryptography algorithm known as MMB (Modular Multiplication-based Block cipher) will be implemented into a software. Information that formed as image can be encrypted into a worthless message using this software. Only the true sender and receiver can use the message.

From experiment result using MMB algorithm, file size and processor speed are the most factor that can influence time for encryption and decryption. While using key and specific color from the picture are not affect to much on processing duration.

DAFTAR ISI

	Halaman
ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR TABEL	vii
DAFTAR GAMBAR.....	viii
 BAB I PENDAHULUAN	
I.1 Latar Belakang	1
I.2 Identifikasi Masalah	2
I.3 Tujuan	2
I.4 Pembatasan Masalah	2
I.5 Sistematika Penulisan	3
 BAB II LANDASAN TEORI	
II.1 Komunikasi dalam Jaringan	4
II.2 Kriptografi	4
II.2.1 Algoritma Simetri	6
II.2.1.1 Mode ECB.....	9
II.2.1.2 Mode CBC	10
II.2.1.3 Mode CFB.....	11
II.2.2 Algoritma Asimetri	13
II.3 Kriptanalisis	14
II.4 Keamanan Algoritma	16
II.5 Cara Kerja MMB (Modular Multiplication-based Block Cipher)	17
II.6 Tanda Tangan Digital/ <i>Digital Signature</i>	23
 BAB III PERANCANGAN PERANGKAT LUNAK	
III.1 Visual Basic	25
III.1.1 <i>Integrated Development Environment</i>	26

III.1.2	Aspek-aspek Pemrograman.....	26
III.2	Perancangan	28
III.2.1	Enkripsi	28
III.2.1.1	Form Enkripsi	28
III.2.1.2	Teknik Enkripsi Menggunakan Algoritma MMB.....	33
III.2.2	Dekripsi	41
III.2.2.1	Form Dekripsi	41
III.2.2.2	Teknik Dekripsi Menggunakan Algoritma MMB.....	45
III.2.3	Pemakaian Algoritma ElGamal untuk <i>Digital Signature</i>	56
BAB IV DATA PENGAMATAN		
IV.1	Pengujian Perangkat Lunak.....	59
IV.1.1	Berdasarkan Pengaruh Besar File	59
IV.1.2	Berdasarkan Pengaruh Warna	64
IV.1.3	Berdasarkan Penggunaan Kunci yang Berbeda	69
IV.2	Analisis File	79
IV.2.1	Analisis Berdasarkan Pengaruh Besar File	79
IV.2.2	Analisis Berdasarkan Pengaruh Warna.....	80
IV.2.3	Analisis Berdasarkan Penggunaan Kunci yang Berbeda	80
BAB V KESIMPULAN DAN SARAN		
V.1	Kesimpulan	82
V.2	Saran.....	82
DAFTAR PUSTAKA		x
Lampiran A		L1
Lampiran B.....		L2
Lampiran C		L3

DAFTAR GAMBAR

Gambar II.1	Skema algoritma simetri	7
Gambar II.2	Enkripsi dan dekripsi mode ECB	9
Gambar II.3	Enkripsi dan dekripsi mode CBC	11
Gambar II.4	Enkripsi dan dekripsi mode CFB	12
Gambar II.5	Skema kriptografi asimetri	13
Gambar II.6	Pembagian sub blok teks dan kunci	18
Gambar II.7	Proses Enkripsi per sub-block	19
Gambar II.8	Proses Dekripsi per sub-block	22
Gambar III.1	Tampilan form enkripsi	31
Gambar III.2	Flowchart eksekusi proses enkripsi	32
Gambar III.3	Flowchart enkripsi dengan algoritma MMB	35
Gambar III.4	Flowchart fungsi F	38
Gambar III.5	Tampilan form dekripsi	43
Gambar III.6	Flowchart eksekusi proses dekripsi	44
Gambar III.7	Flowchart enkripsi dengan algoritma MMB	47
Gambar III.8	Flowchart fungsi G	53
Gambar III.9	Flowchart eksekusi tanda tangan digital	58
Gambar IV.1	Enkripsi Morning Light dengan kualitas <i>low</i>	60
Gambar IV.2	Dekripsi Morning Light dengan kualitas <i>low</i>	60
Gambar IV.3	Enkripsi Morning Light dengan kualitas <i>medium</i>	61
Gambar IV.4	Dekripsi Morning Light dengan kualitas <i>medium</i>	61
Gambar IV.5	Enkripsi Morning Light dengan kualitas <i>fine</i>	62
Gambar IV.6	Dekripsi Morning Light dengan kualitas <i>fine</i>	62
Gambar IV.7	Enkripsi Morning Light dengan kualitas <i>maximum</i>	63
Gambar IV.8	Dekripsi Morning Light dengan kualitas <i>maximum</i>	63
Gambar IV.9	Enkripsi dengan warna dominan merah	64
Gambar IV.10	Dekripsi dengan warna dominan merah	65
Gambar IV.11	Enkripsi dengan warna dominan hijau	65

Gambar IV.12	Dekripsi dengan warna dominan hijau.....	66
Gambar IV.13	Enkripsi dengan warna dominan biru	66
Gambar IV.14	Dekripsi dengan warna dominan biru	67
Gambar IV.15	Enkripsi dengan warna dominan hitam.....	67
Gambar IV.16	Dekripsi dengan warna dominan hitam.....	68
Gambar IV.17	Enkripsi dengan warna dominan putih.....	68
Gambar IV.18	Dekripsi dengan warna dominan putih	69
Gambar IV.19	Enkripsi Sungai.bmp dengan kunci 0.....	70
Gambar IV.20	Dekripsi Sungai.bmp dengan kunci 0	70
Gambar IV.21	Enkripsi Sungai.bmp dengan kunci 5.....	71
Gambar IV.22	Dekripsi Sungai.bmp dengan kunci 5	71
Gambar IV.23	Enkripsi Sungai.bmp dengan kunci 9.....	72
Gambar IV.24	Dekripsi Sungai.bmp dengan kunci 9	72
Gambar IV.25	Enkripsi Sungai.gif dengan kunci 0	73
Gambar IV.26	Dekripsi Sungai.gif dengan kunci 0	73
Gambar IV.27	Enkripsi Sungai.gif dengan kunci 5	74
Gambar IV.28	Dekripsi Sungai.gif dengan kunci 5	74
Gambar IV.29	Enkripsi Sungai.gif dengan kunci 9	75
Gambar IV.30	Dekripsi Sungai.gif dengan kunci 9	75
Gambar IV.31	Enkripsi Sungai.jpg dengan kunci 0.....	76
Gambar IV.32	Dekripsi Sungai.jpg dengan kunci 0	76
Gambar IV.33	Enkripsi Sungai.jpg dengan kunci 5.....	77
Gambar IV.34	Dekripsi Sungai.jpg dengan kunci 5	77
Gambar IV.35	Enkripsi Sungai.jpg dengan kunci 9.....	78
Gambar IV.36	Dekripsi Sungai.jpg dengan kunci 9	78