

ABSTRAK

Kemajuan teknologi di bidang komputer dan informasi telah berkembang dengan sangat pesat. Dalam jaman serba komputer yang diarahkan pada realisasi sistem jaringan, teknologi keamanan informasi menjadi penting. Teknologi keamanan informasi akan menjaga dan melawan bahaya yang disebabkan oleh akses yang tidak diinginkan pada sumber-sumber yang berharga. Maka dari itu dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan suatu informasi, sehingga informasi tersebut dapat disimpan atau dikirim dengan aman.

Inti dari teknologi keamanan informasi adalah kriptografi. Peran utama dari kriptografi yaitu menjaga isi kerahasiaan informasi di antara semua yang berkepentingan. Kriptografi akan mengubah informasi menjadi sebuah pesan yang tidak memiliki makna dan tidak dimengerti.

Tugas Akhir ini akan merealisasikan suatu perangkat lunak pengaman data dengan algoritma simetri menggunakan metode enkripsi MISTY1. Perangkat lunak ini dirancang dalam bahasa pemrograman Borland Delphi 7. Perangkat lunak proteksi data dengan algoritma MISTY1 ini akan meliputi proses enkripsi dan dekripsi data, serta untuk menambah tingkat keamanannya dibuat program tambahan berupa tanda tangan digital dan validasi sehingga perangkat lunak dapat mendeteksi adanya perubahan informasi dan dapat menjamin keaslian pengirim informasi.

ABSTRACT

Nowadays progress of computer and information technology has developed very fast. As we have moved into an era of the computing trends aimed at the realization of networks system, information security technology becomes more and more important. Information security technology protects againsts danger of making unwarranted accesses to valuable resources. For the reason, a security system is needed and becomes more important to protect information secret, so that information can be kept or sent safely.

The core of technology of information security is cryptography. Primary role of the cryptography is to keep the content of information secret among all authorized entitites. Cryptography will change the information become unmeaning and unreadable.

This final report will realize software of data protection with symmetrical algorithm using method of encrypts MISTY1. This software is designed in Borland Delphi 7. Software of data protection using this MISTY1 algorithm will including process of encryption and decryption text file and to add its security level also included with additional program in the form of digital signature and validation, so that the software is able to detect the information changes and able to guarantee the originality of that sending information.

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	ix
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 Sistematika Penulisan	2
BAB II LANDASAN TEORI	3
2.1 Definisi Kriptografi	3
2.2 Istilah dalam Kriptografi	3
2.3 Aspek-aspek Penunjang Keamanan	4
2.4 Enkripsi Dekripsi	4
2.5 Algoritma Berdasarkan Jenis Kunci	6
2.5.1 Algoritma Simetri	6
2.5.1.1 Dua Kategori Algoritma Simetri	7
2.5.1.2 Mode Operasi Algoritma <i>Block Cipher</i>	7
2.5.1.2.1 Mode ECB	8
2.5.1.2.2 Mode CBC	9
2.5.1.2.3 Mode CFB	11
2.5.2 Algoritma Asimetri	13
2.5.3 Perbandingan Antara Algoritma Simetri Dengan Algoritma Asimetri ..	14
2.6 Teknik Kripanalisis	15
2.7 Proses Tanda Tangan Digital	18
2.7.1 Algoritma Pembangkit Kunci Tanda Tangan Digital	18
2.7.2 Algoritma Tanda Tangan Digital	19

2.8 Proses Validasi Data.....	19
2.9 Algoritma MISTY1	19
2.9.1 Struktur <i>Cipher</i> Algoritma MISTY1	20
2.9.1.1 Keterangan Fungsi dan Variabel	20
2.9.1.2 Prosedur Enkripsi	21
2.9.1.3 Prosedur Dekripsi	23
2.9.1.4 Penjadwalan Kunci.....	25
2.9.2 Komponen Penyusun MISTY1	26
2.9.2.1 Fungsi FL.....	26
2.9.2.2 Fungsi FL^{-1}	26
2.9.2.3 Fungsi FO	27
2.9.2.4 Fungsi FI.....	28
2.9.2.5 S-Box.....	30
2.10 Borland Delphi	33
2.10.1 Sekilas Tentang Borland Delphi.....	33
2.10.2 Komponen Borland Delphi.....	33
2.10.2.1 <i>Project</i>	33
2.10.2.2 <i>Form</i>	34
2.10.2.3 <i>Unit</i>	35
2.10.2.4 Program	35
2.10.2.5 <i>Property</i>	36
2.10.2.6 <i>Event</i>	37
BAB III PERANCANGAN DAN REALISASI PERANGKAT LUNAK.....	38
3.1 Realisasi Perangkat Lunak	38
3.2 Teknik Padding.....	42
3.3 Proses Enkripsi dan Dekripsi.....	43
3.3.1 Enkripsi MISTY1	44
3.3.2 Dekripsi MISTY1	47
3.4 Proses Tanda Tangan Digital.....	49
3.5 Proses Validasi	52

BAB IV DATA PENGAMATAN	54
4.1 Pengujian Perangkat Lunak	55
4.1.1 Pengujian 1	55
4.1.2 Pengujian 2	57
4.1.3 Pengujian 3	58
4.1.3.1 Penambahan Karakter Pada <i>Ciphertext</i>	58
4.1.3.2 Pengurangan Karakter Pada <i>Ciphertext</i>	59
4.1.3.3 Penggantian (<i>Replace</i>) Karakter Pada <i>Ciphertext</i>	60
4.1.4 Pengujian 4	61
4.1.5 Pengujian 5	63
4.1.6 Pengujian 6	66
4.1.7 Pengujian 7	67
4.1.8 Pengujian 8	69
4.1.9 Pengujian 9	70
4.1.10 Pengujian 10	71
4.2 Analisa dan Hasil Pengamatan	71
BAB V KESIMPULAN DAN SARAN	73
5.1 Kesimpulan	73
5.2 Saran	73
 DAFTAR PUSTAKA	
LAMPIRAN A <i>LISTING</i> PROGRAM	A-1
LAMPIRAN B TAMPILAN PROGRAM	B-1
LAMPIRAN C TABEL CRC	C-1