

ABSTRAK

Dalam dunia sekarang ini, kemajuan teknologi di bidang komputer dan telekomunikasi berkembang sangat pesat. Lalu lintas pengiriman data dan informasi yang semakin global, serta konsep *open system* dari suatu jaringan memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat membuat proses pengiriman data menjadi tidak aman dan dapat saja dimanfaatkan oleh pihak lain yang tidak bertanggung jawab, yang mengambil informasi atau data yang dikirimkan tersebut di tengah perjalanan. Maka dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan suatu data, sehingga data tersebut dapat dikirimkan dengan aman. Salah satu solusi untuk menjaga keamanan dan kerahasiaan pada proses pengiriman data dengan menggunakan teknik kriptografi.

Kriptografi telah menjadi suatu bagian yang tidak dapat dipisahkan dari sistem keamanan jaringan antar komputer yang juga merupakan salah satu solusi agar informasi atau pesan yang dikirim dalam suatu jaringan tidak dapat dimanfaatkan oleh pihak lain. Kriptografi akan mengubah informasi yang dikirim menjadi suatu pesan yang tidak memiliki makna, dan tidak dapat dimengerti oleh pihak lain selain penerima.

Dalam tugas akhir ini penulis merealisasikan suatu perangkat lunak enkripsi dan dekripsi file teks dengan menggunakan algoritma kriptografi yaitu FEAL. Di samping itu untuk meningkatkan keamanan pada perangkat lunak disertakan juga proses validasi dan proses *digital signature*, sehingga perangkat lunak dapat mendeteksi adanya perubahan data atau informasi yang dikirimkan serta menjamin keaslian pengirim informasi. Perangkat lunak ini dibuat dengan menggunakan bahasa pemrograman Microsoft Visual Basic 6.0.

ABSTRACT

In the world today, the development of technology in the sector of computer and telecommunication has grown fast. The traffic of sending data and global information, also open system concept from a certain network make someone easier to go into that network. It can make a data shipping process does not save and can be exploited by other side who do not have any responsibility, who take an information or data which will be sent on the way. So, it is needed a security system able to take care of data secret, so that the data can be sent safely. One of the solution to take care of secret and security at process delivery of data by using a cryptography technique.

Cryptography has become certain parts which cannot be separated from a network security system between computer and also a part of solution in order that information or message which is sent in a network cannot be exploited by other people. Cryptography will change a sending information become an unmeaning message, and cannot be understood by other people but receiver.

In this final thesis, encryption and decryption file using FEAL algorithm has realized.. Beside that, not only to improve the security level, in the software also included validation and digital signature process, so that software is able to detect the text changes and able to guarantee the originality of sender of message. The software of FEAL is made by using Microsoft Visual Basic 6.0 language program.

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	2
1.3 Tujuan	2
1.4 Pembatasan Masalah	2
1.5 Sistematika Penulisan	2
BAB II TEORI PENUNJANG	3
2.1 Sekilas Mengenai Keamanan dan Kerahasiaan Data Dalam Jaringan Komputer	3
2.2 Kriptologi, Kriptanalisis, dan Kriptografi	6
2.2.1 Kriptanalisis	7
2.2.2 Algoritma dan Kunci	9
2.2.2.1 Algoritma Simetris	10
2.2.2.1.1 Mode Operasi Algoritma Block Cipher	11
2.2.2.2 Algoritma Asimetris	16
2.3 Perbandingan Antara Algoritma Simetrik Dengan Algoritma Kunci Publik	17
2.4 Algoritma FEAL	19
2.5 Tanda Tangan Digital (<i>Digital Signature</i>)	23
2.5.1 Algoritma Pembangkit Kunci Tanda Tangan Digital	23
2.5.2 Algoritma Tanda Tangan Digital	24
2.5.3 Algoritma Verifikasi Tanda Tangan Digital	24

2.6 Visual Basic	24
2.6.1 Sekilas Tentang Visual Basic.....	24
2.6.2 Lingkungan Visual Basic	25
2.6.2.1 Control Menu	25
2.6.2.2 Menu	25
2.6.2.3 Toolbar	26
2.6.2.4 Form Window	26
2.6.2.5 Toolbox	26
2.6.2.6 Project Explorer	26
2.6.2.7 Jendela Properties	26
2.6.2.8 Form Layout Window	27
2.6.2.9 Jendela Code	27
2.6.3 Komponen Pemrograman Visual Basic	28
BAB III IMPLEMENTASI ALGORITMA DAN REALISASI PERANGKAT	
LUNAK.....	33
3.1 Program Pengamanan Data FEAL.....	33
3.1.1 Padding dan Mode Operasi	36
3.2 Program Utama	36
3.2.1 Program Enkripsi <i>Plaintext</i>	37
3.2.1.1 Sub Program CRCCheck	38
3.2.1.2 Sub Program Enkripsi FEAL	39
3.2.2 Program Dekripsi <i>Ciphertext</i>	43
3.2.2.1 Sub Program Dekripsi FEAL.....	44
3.2.3 Program Tanda Tangan Digital.....	48
3.2.3.1 Sub Program Pangkatmod.....	48
3.2.4 Program Perbandingan Tanda Tangan Digital	
dengan <i>Decipheredtext</i>	50
BAB IV HASIL PENGAMATAN	51
4.1 Pengujian Perangkat Lunak	51
4.1.1 Pengujian 1.....	51
4.1.2 Pengujian 2.....	54
4.1.3 Pengujian 3.....	56

4.1.3.1 Penambahan Karakter Pada <i>Ciphertext</i>	56
4.1.3.2 Pengurangan Karakter Pada <i>Ciphertext</i>	57
4.1.3.3 Penggantian (<i>Replace</i>) Karakter Pada <i>Ciphertext</i>	59
4.1.4 Pengujian 4.....	60
4.1.5 Pengujian 5.....	64
4.1.6 Pengujian 6.....	66
4.1.7 Pengujian 7.....	68
4.1.8 Pengujian 8.....	70
4.1.9 Pengujian 9.....	71
4.1.10 Pengujian 10.....	71
4.2 Analisa dan Hasil Pengamatan.....	72
BAB V KESIMPULAN DAN SARAN.....	74
5.1 Kesimpulan	74
5.2 Saran.....	74
DAFTAR PUSTAKA	
LAMPIRAN A LISTING PROGRAM.....	A-1
LAMPIRAN B DIAGRAM ALIR SUB PROGRAM	B-1
LAMPIRAN C TAMPILAN PROGRAM.....	C-1

DAFTAR GAMBAR

Gambar 2.1 Skema Enkripsi dan Dekripsi Pada Kriptografi Simetris.....	10
Gambar 2.2 Enkripsi dan Dekripsi Mode ECB.....	12
Gambar 2.3 Enkripsi dan Dekripsi Mode CBC	14
Gambar 2.4 Enkripsi dan Dekripsi Mode CFB.....	15
Gambar 2.5 Skema Enkripsi dan Dekripsi Pada Kriptografi Asimetris.....	17
Gambar 2.6 Diagram Alir Algoritma FEAL.....	20
Gambar 2.7 Diagram Alir Fungsi f	21
Gambar 2.8 Diagram Alir Kunci FEAL.....	22
Gambar 2.9 Diagram Alir Fungsi f_K	22
Gambar 2.10 Lingkungan Kerja Visual Basic	25
Gambar 2.11 Jendela Kode	28
Gambar 2.12 Kontrol pada Visual Basic.....	30
Gambar 2.13 Jendela Properties.....	31
Gambar 3.1 Diagram Alir Program Pengamanan Data.....	34
Gambar 3.2 Tampilan Form Utama Bagian Enkripsi	35
Gambar 3.3 Tampilan Form Utama Bagian Dekripsi	35
Gambar 3.4 Diagram Alir Eksekusi Enkripsi	37
Gambar 3.5 Diagram Alir CRCCheck	38
Gambar 3.6 Diagram Alir Sub Program Enkripsi FEAL.....	40
Gambar 3.7 Diagram Alir Eksekusi Dekripsi	43
Gambar 3.8 Diagram Alir Sub Program Dekripsi FEAL.....	45
Gambar 3.9 Diagram Alir Program Tanda Tangan Digital.....	48
Gambar 3.10 Diagram Alir Sub Program Pangkatmod	49
Gambar 3.11 Diagram Alir Program Perbandingan Tanda Tangan Digital dengan Decipheredtext.....	50
Gambar 4.1 super_1024.jpg (286 KB).....	71

DAFTAR TABEL

Tabel 4.1 Hasil pengamatan ukuran file sebelum dan sesudah proses enkripsi dan dekripsi serta waktu untuk setiap proses dengan menggunakan algoritma FEAL.....	69
Tabel 4.2 Hasil pengamatan ukuran file sebelum dan sesudah proses enkripsi dan dekripsi serta waktu untuk setiap proses dengan menggunakan algoritma LOKI	69