

ABSTRAK

Kriptografi memegang peranan yang penting di tengah penggunaan jaringan antar komputer yang semakin luas secepat teknologi dan produk jaringan baru diperkenalkan. Teknologi jaringan terus dikembangkan sehingga akan terus menyediakan solusi dan efisiensi dalam hal perpindahan data.

Kriptografi merupakan salah satu tindakan 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.

Salah satu algoritma kriptografi adalah algoritma SAFER (Secure and Fast Encryption Routine) yang dirancang menjadi sebuah perangkat lunak pada tugas akhir ini. Informasi yang dikirim melalui jaringan atau disimpan dalam suatu media penyimpanan dapat dienkrip dengan menggunakan perangkat lunak yang dirancang menjadi suatu pesan yang tak memiliki makna. Hanya pemilik dan penerima informasi yang sebenarnya yang dapat memanfaatkan pesan tersebut.

ABSTRACT

Cryptography is an important aspect in use of computer network expanded almost as rapidly as new network technologies and products were introduced. The network technologies continually emerged, while providing solution and efficiency in data mobility.

Cryptography is an attempt to make sent information or message through network cannot be used by outsiders. Cryptography convert sent information to a worthless message which cannot be understood by anyone.

One of the cryptography algorithm known as SAFER (Secure and Fast Encryption Routine) will be implemented into a software. Information sent through network or saved on a storage can be encrypted into a worthless message using this software. Only authority can use the message.

DAFTAR ISI

ABSTRAK.....	i
KATA PENGANTAR.....	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	viii
DAFTAR TABEL.....	ix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	2
1.2 Identifikasi Masalah.....	2
1.3 Tujuan.....	2
1.4 Pembatasan Masalah.....	2
1.5 Sistematika Penulisan.....	3
BAB II LANDASAN TEORI.....	4
2.1 Sekilas Mengenai Jaringan.....	3
2.1.1 Jaringan Data.....	3
2.1.2 Local-Area Network (LAN).....	5
2.1.3 Metropolitan-Area Network (MAN).....	5
2.1.4 Wide-Area Network (WAN).....	5
2.1.5 Storage-Area Networks (SAN).....	6
2.1.6 Virtual Private Network (VPN).....	6
2.1.7 Jaringan Internet.....	8
2.2 Komunikasi.....	10
2.3 Kriptografi.....	11
2.3.1 Kriptosistem.....	11
2.3.1.1 Algoritma Simetri.....	13
2.3.1.1.1 Mode Operasi Algoritma Block Cipher.....	14
2.3.1.2 Algoritma Asimetri.....	19
2.3.2 Kriptoanalisis.....	20
2.4 SAFER (Secure and Fast Encryption Routine).....	23
2.4.1 SAFER K-64.....	23

2.4.2 SAFER K-128.....	31
BAB III PERANCANGAN PERANGKAT LUNAK.....	35
3.1 Visual Basic.....	35
3.1.1 Integrated Development Environtment.....	36
3.1.2 Aspek-aspek Pemrograman.....	36
3.2 Perancangan.....	38
3.2.1 Padding dan Mode Operasi.....	40
3.2.2 Enkripsi.....	41
3.2.2.1 SAFER K-64.....	43
3.2.2.2 SAFER K-128.....	48
3.2.3 Dekripsi.....	52
3.2.3.1 SAFER K-64.....	52
3.2.3.2 SAFER K-128.....	57
BAB IV HASIL PENGAMATAN.....	61
4.1 Pengujian Perangkat Lunak.....	61
4.1.1 SAFER K-64.....	61
4.1.1.1 Pengujian 1.....	61
4.1.1.2 Pengujian 2.....	64
4.1.2 SAFER K-128.....	67
4.2.1.1 Pengujian 3.....	67
4.2.1.2 Pengujian 4.....	69
4.1.3 SAFER K-64 dan SAFER K-128.....	71
4.1.3.1 Pengujian 5.....	71
4.1.3.2 Pengujian 6.....	74
4.1.3.3 Pengujian 7.....	75
4.1.3.4 Pengujian 8.....	77
4.2 Analisa dan Pengamatan.....	79
BAB V KESIMPULAN DAN SARAN.....	81
5.1 Kesimpulan.....	81
5.2 Saran.....	81
DAFTAR PUSTAKA.....	x
LAMPIRAN A.....	L1

LAMPIRAN B.....	L2
LAMPIRAN C.....	L3

DAFTAR GAMBAR

Gambar 2.1 Skema algoritma simetri.....	13
Gambar 2.2 Enkripsi dan dekripsi mode ECB.....	15
Gambar 2.3 Enkripsi dan dekripsi mode CBC.....	17
Gambar 2.4 Enkripsi dan dekripsi mode CFB.....	18
Gambar 2.5 Skema algoritma asimetri.....	19
Gambar 2.6 Skema algoritma enkripsi SAFER.....	25
Gambar 2.7 Skema algoritma dekripsi SAFER.....	30
Gambar 3.1 Tampilan form utama.....	40
Gambar 3.2 Flowchart eksekusi enkripsi.....	42
Gambar 3.3 Flowchart fungsi EnkripsiSK64.....	47
Gambar 3.4 Flowchart fungsi EnkripsiSK128.....	51
Gambar 3.5 Flowchart eksekusi dekripsi.....	53
Gambar 3.6 Flowchart fungsi DekripsiSK64.....	56
Gambar 3.7 Flowchart fungsi DekripsiSK128.....	60

DAFTAR TABEL

Tabel 2.1 Skema penjadwalan Kunci SAFER K-64.....	27
Tabel 2.2 S-box Eksponen 45.....	28
Tabel 2.3 S-box Logaritma 45.....	29
Tabel 2.4 Skema penjadwalan Kunci SAFER K-128.....	33
Tabel 3.1 Kontrol pada form utama.....	39
Tabel 4.1 Hasil pengamatan SAFER K-64 dengan 8 iterasi.....	77
Tabel 4.2 Hasil pengamatan SAFER K-128 dengan 8 iterasi.....	78
Tabel 4.3 Hasil pengamatan SAFER K-64 dengan 16 iterasi.....	78
Tabel 4.4 Hasil pengamatan SAFER K-64 dengan 32 iterasi.....	79