

## **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 Newdes yang dirancang menjadi sebuah perangkat lunak pada tugas akhir ini. Informasi yang dikirim melalui jaringan atau disimpan dalam suatu media penyimpanan dapat dienkrif 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 used 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 attempted to make sended information or message through network cannot be used by outsiders. Cryptography convert sended information to a worthless message which cannot be understood by anyone.

One of the cryptography algorithm known as Newdes will be implemented into a software. Information sended through network or saved on a storage can be encrypted into a worthless message using this software. Only the real owner can use the message.

# DAFTAR ISI

ABSTRAK.....	i
KATA PENGANTAR.....	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	vii
DAFTAR TABEL.....	ix
BAB I PENDAHULUAN.....	1
1.1 LatarBelakang.....	1
1.2 Identifikasi Masalah.....	2
1.3 Tujuan.....	2
1.4 Pembatasan Masalah.....	2
1.5 Sistematika Penulisan.....	2
BAB II LANDASAN TEORI.....	3
2.1 Jaringan.....	4
2.1.1 LAN (Local Area Network).....	4
2.1.2 MAN (Metropolitan Area Network).....	4
2.1.3 WAN (Wide Area Network).....	4
2.1.4 Jaringan Internet.....	5
2.2 Komunikasi.....	7
2.3 Kriptografi.....	7
2.3.1 Kriptosistem.....	8
2.3.1.1 Algoritma Simetri.....	9
2.3.1.2 Algoritma Asimetri.....	10
2.3.2 Kriptanalisis.....	11
2.4 Tanda Tangan Digital.....	14
BAB III PERANCANGAN PERANGKAT LUNAK.....	15
3.1 Newdes.....	15
3.1.1 Enkripsi.....	15

3.1.2 Dekripsi.....	19
3.2 Tanda Tangan Digital Elgamal.....	22
3.2.1 Otentikasi tanda tangan Digital Elgamal.....	23
3.2.2 Flowchart menu tanda tangan Digital Elgamal.....	25
BAB IV PENGUJIAN PERANGKAT LUNAK.....	26
4.1 Menu utama perangkat lunak.....	26
4.2 Perangkat lunak enkripsi.....	27
4.3 Perangkat lunak dekripsi.....	27
4.4 Perangkat lunak <i>Digital Signature</i> .....	28
4.5 Perangkat lunak <i>About</i> .....	28
4.6 Hasil enkripsi dan dekripsi.....	29
4.6.1 Pengujian 1.....	29
4.6.2 Pengujian 2.....	32
4.6.3 Pengujian 3.....	34
4.6.4 Pengujian 4.....	36
4.6.5 Pengujian 5.....	38
BAB V KESIMPULAN DAN SARAN.....	42
5.1 Kesimpulan.....	42
5.2 Saran.....	42
DAFTAR PUSTAKA.....	x
LAMPIRAN.....	L

## DAFTAR GAMBAR

Gambar 2.1 Skema algoritma simetri .....	9
Gambar 2.2 Skema algoritma asimetri .....	11
Gambar 3.1 Flowchart eksekusi Enkripsi .....	16
Gambar 3.2 Flowchart algoritma enkripsi Newdes .....	18
Gambar 3.3 Flowchart eksekusi Dekripsi .....	19
Gambar 3.4 Flowchart algoritma dekripsi Newdes .....	21
Gambar 3.5 Skema Tanda Tangan Digital Elgamal .....	23
Gambar 3.6 Skema Otentikasi Tanda Tangan Digital Elgamal .....	24
Gambar 3.7 Flowchart menu Digital Signature .....	25
Gambar 4.1 Tampilan menu utama .....	26
Gambar 4.2 Tampilan menu enkripsi .....	27
Gambar 4.3 Tampilan menu dekripsi .....	27
Gambar 4.4 Tampilan menu Digital Signature .....	28
Gambar 4.5 Tampilan menu About .....	28
Gambar 4.6 File yan bernama cm0304 sebelum dienkripsi .....	29
Gambar 4.7 hasil enkripsi file yang bernama cm0304 .....	29
Gambar 4.8 File yang bernama Acak sebelum dienkripsi .....	30
Gambar 4.9 Hasil enkripsi file yang bernama Acak .....	30
Gambar 4.10 File yang bernama Coba1 sebelum dienkripsi .....	31
Gambar 4.11 Hasil enkripsi file yang bernama Coba1 .....	31
Gambar 4.12 File yang bernama Dogwalk .....	32
Gambar 4.13 File yang bernama Shrek2 .....	33
Gambar 4.14 File yang bernama Tokyo .....	33
Gambar 4.15 File yang bernama av .....	34
Gambar 4.16 File yang bernama rockman .....	35
Gambar 4.17 File yang bernama thaifood .....	36
Gambar 4.18 File yang bernama motor kanzen .....	36
Gambar 4.19 File yang bernama 022090modul5 .....	37
Gambar 4.20 File yang bernama Task home take modul5 .....	38

Gambar 4.20 File yang bernama Jessica-simson-01 .....	39
Gambar 4.22 File yang bernama Break dance battle .....	39
Gambar 4.23 File yang bernama Break dance-mr(1)(1).....	40

## DAFTAR TABEL

Tabel 4.1 Hasil uji file. Text .....	32
Tabel 4.2 Hasil uji file . JPG .....	34
Tabel 4.3 Hasil uji file.BMP .....	36
Tabel 4.4 Hasil uji file .doc.....	38
Tabel 4.5 Hasil ujian filr.mpg .....	40
Tabel 4.6 Hasil uji file .....	41