

ABSTRAK

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam era informasi sekarang ini. Salah satu solusi untuk mengatasinya adalah dengan melakukan enkripsi (penyandian) terhadap data yang akan dikirimkan dengan waktu penyandian yang tidak lama.

Dalam menyandikan suatu data dan menerjemahkannya kembali digunakan suatu data yang disebut kunci. Algoritma enkripsi yang didasarkan pada kunci secara garis besar dibedakan menjadi dua macam, yaitu algoritma simetrik dan algoritma kunci publik (algoritma asimetrik). Algoritma yang digunakan pada tugas akhir ini adalah algoritma simetrik yaitu penyandian dengan menggunakan kunci yang sama untuk enkripsi dan dekripsi data yang disebut dengan *secret key*.

Tugas Akhir ini akan merealisasikan suatu perangkat lunak pengaman data dengan algoritma simetrik menggunakan metode enkripsi RC2. Perangkat lunak ini dibuat dalam bahasa pemrograman *Borland Delphi*. Perangkat lunak yang direalisasikan mempunyai 7 Bagian utama yaitu : Inisialisasi RC2 dan *Mixing S-Box*, Enkripsi *Plaintext*, Pembangkit Kunci Tanda Tangan Digital, Validasi dan Tanda Tangan Digital, Dekripsi *Ciphertext*, *Open Deciphered Text*, dan membuat *plaintext* dan *ciphertext* data.

ABSTRACT

Nowadays in the age of information, the problems of data security and secrecy are one of the most important aspects on computer communication and networks. One of the solutions to handling these problems is data encoding (encryption) with a short time in encoding and decoding.

Some keys are used when encoding data and decoding it back to its original data. There are two general types of the algorithm, symmetric algorithm and public key algorithm. Algorithm used on this book is symmetric algorithm. Symmetric algorithm is designed so that the key use for encryption is the same as the key used for decryption which is called secret key.

Data protection software with symmetric algorithm using RC2 Encryption that realized in this book is made with Borland Delphi programming language. This software consists of 7 main parts which are: Initializes RC2 and Mixing S-Box, Plaintext encryption, Digital Signature key generator, Validation and Digital Signature, Cipher text decryption, Open Deciphered Text, and create *plaintext* and cipher text.

DAFTAR ISI

ABSTRAK.....	i
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 Pembahasan.....	2
BAB II TEORI PENUNJANG.....	4
2.1 Kriptologi, Kriptanalisis, dan Kriptografi.....	4
2.1.1 Tujuan Kriptografi.....	4
2.1.2 Enkripsi dan Dekripsi.....	5
2.1.3 Algoritma dan Kunci.....	6
2.1.3.1 Algoritma Simetrik.....	7
2.1.3.2 Algoritma Kunci Publik.....	8
2.2 Perbandingan antara algoritma simetrik dengan algoritma kunci publik.....	9
2.3 Teori Matematika.....	11
2.3.1 Bilangan Prima.....	11
2.3.2 Operasi Modulus.....	12
2.3.3 Algoritma Euclidean.....	12
2.3.4 Algoritma Extended Euclidean.....	13
2.3.5 Eksponensial Modulus.....	14
2.3.6 Fungsi XOR.....	15
2.3.7 Fungsi $\sim$	15
2.4 Algoritma RC2.....	16

2.5 Algoritma Validasi Data	17
2.6 Algoritma Tanda Tangan Digital	17
2.6.1 Algoritma Pembangkit Kunci Tanda Tangan Digital.....	18
2.6.2 Algoritma Tanda Tangan Digital.....	19
2.6.3 Algoritma Verifikasi Tanda Tangan Digital.....	20
BAB III IMPLEMENTASI DAN REALISASI PERANGKAT LUNAK	20
3.1 Program Pengaman Data.....	21
3.2 Bagian Utama.....	23
3.2.1 Program Inisialisasi RC2.....	23
3.2.2. Program Enkripsi Plaintext.....	24
3.2.3 Program Pembangkit Kunci Tanda Tangan Digital.....	25
3.2.3.1 Sub Program rdmprime dan rdmprime2.....	27
3.2.3.2 Sub Program gcd.....	27
3.2.4 Program Validasi dan Tanda Tangan Digital.....	29
3.2.4.1 Sub Program Pangkatmod.....	30
3.2.4.2 Sub Program DecimalToBinary.....	31
3.2.5 Program Dekripsi Ciphertext.....	31
3.2.6 Program Open Deciphered Text.....	33
3.2.7 Program perbandingan Tanda Tangan Digital	34
BAB IV HASIL PENGAMATAN.....	36
4.1 Hasil Pengamatan.....	36
4.1.1 Hasil Pengamatan 1.....	36
4.1.2 Hasil Pengamatan 2.....	37
4.1.3 Hasil Pengamatan 3.....	37
4.1.3.1 Hasil Pengamatan <i>File Text 1</i>	37
4.1.3.2 Hasil Pengamatan <i>File Text 2</i>	38
4.1.4 Hasil Pengamatan 4.....	39
4.1.4.1 Pengujian <i>dengan secret key sama 1</i>	39
4.1.4.1 Pengujian <i>dengan secret key sama 2</i>	39
4.1.5 Hasil Pengamatan 5.....	40
4.1.6 Hasil Pengamatan 6.....	40

4.1.7 Hasil Pengamatan 7	43
4.1.7.1 Pengamatan yang benar	43
4.1.7.2 Pengamatan penambahan ciphertext	43
4.1.7.3 Pengamatan pengurangan ciphertext	44
4.1.7.4 Pengamatan perubahan ciphertext	44
4.1.7.5 Pengamatan kesalahan Publik dan Private key	45
4.2 Analisa Hasil Pengamatan	45
BAB V KESIMPULAN DAN SARAN	47
5.1 Kesimpulan	47
5.2 Saran	47
DAFTAR PUSTAKA	48
LAMPIRAN A <i>LISTING</i> PROGRAM	A-1
LAMPIRAN B TAMPILAN PROGRAM PENGAMAN DATA	B-1

DAFTAR GAMBAR

Gambar 2.1 Diagram Blok Enkripsi.....	6
Gambar 2.2 Diagram Blok Dekripsi	6
Gambar 2.3 Diagram Blok Enkripsi Dengan Menggunakan Kunci.....	7
Gambar 2.4 Diagram Blok Dekripsi Dengan Menggunakan Kunci.....	7
Gambar 2.5 Diagram Blok Algoritma Simetrik.....	8
Gambar 2.6 Diagram Blok Enkripsi Pada Algoritma Kunci Publik.....	9
Gambar 2.7 Diagram Blok Dekripsi Pada Algoritma Kunci Publik.....	9
Gambar 3.1 Diagram Alir Program Pengaman Data.....	21
Gambar 3.2 Diagram Alir Program Inisialisasi RC2.....	23
Gambar 3.3 Diagram Alir Program Enkripsi Plaintext.....	24
Gambar 3.4 Diagram Alir Program Pembangkit Kunci Tanda Tangan Digital ..	25
Gambar 3.5 Diagram Alir Sub Program gcd.....	26
Gambar 3.6 Diagram Alir Sub Program euclid.....	27
Gambar 3.7 Diagram Alir Sub Program Validasi dan Tanda Tangan Digital.....	28
Gambar 3.8 Diagram Alir Sub Program Pangkatmod.....	29
Gambar 3.9 Diagram Alir Program DecimalToBinary.....	30
Gambar 3.10 Diagram Alir Sub Program Dekripsi CipherText.....	31
Gambar 3.11 Diagram Alir Program Dekripsi CipherText.....	33
Gambar 3.12 Diagram Alir Program Perbandingan Tanda Tangan Digital dengan Decipheredtext	34

DAFTAR TABEL

Tabel 2.1 Nilai Extended Euclidean.....	13
Tabel 4.1 Hasil Pengamatan Dengan Secret Key sama.....	35
Tabel 4.2 Hasil Pengamatan Dengan Karakter Plaintext Berbeda.....	36
Tabel 4.3 Hasil Pengamatan Ukuran File Ciphertext Dengan Plaintext Yang Berbeda dan Secret Key Sama.....	38
Tabel 4.5 Tabel 4.4 Hasil Pengamatan Ukuran File Ciphertext Dengan Plaintext Yang Berbeda dan Secret Key Berbeda-beda.....	38
Tabel 4.5 Hasil Pengamatan Ukuran File Ciphertext Dengan Plaintext Yang Berbeda dan Secret Key Berbeda-beda.....	38