

ABSTRACT

Nowadays in the age of information, many people using internet for communication and transferring data. The security aspect in data transaction is one of the most important aspects. One of the solutions to handle this is with data encoding or encryption.

The encryption method encodes the data, so anyone can not read the information of data except the owner. There are two general types of encryption algorithm, symmetric algorithm and asymmetric algorithm. The Algorithm which used in this book is symmetric algorithm. Symmetric algorithm encodes and decodes with the same key.

In this project has successfully built an encryption software using Camellia algorithm with Delphi as programming language.

ABSTRAK

Pada saat ini penggunaan jaringan internet sudah merupakan suatu kebutuhan yang cukup vital. Jaringan internet sangat rawan tingkat keamanannya, sehingga data tidak hanya diterima oleh penerima data tetapi orang lain yang ingin mengetahui data tersebut dapat mengambilnya juga.

Salah satu solusi untuk mengamankan data yang dikirimkan adalah dengan melakukan enkripsi (penyandian) pada data. Enkripsi dibagi menjadi dua bagian yaitu algoritma simetrik dan algoritma asimetrik. Pada tugas akhir ini algoritma yang dipakai adalah algoritma simetrik, yaitu penyandian dengan menggunakan kunci yang sama. Data yang dikirimkan adalah data hasil penyandian atau disebut juga *ciphertext*, setelah data diterima maka data akan diolah kembali menjadi data sebenarnya atau disebut juga *plaintext*.

Tugas akhir ini telah berhasil merealisasikan perangkat lunak pengaman data dengan algoritma simetrik metoda Camellia menggunakan bahasa pemrograman Dephi.

DAFTAR ISI

ABSTRACT.....	i
ABSTRAK.....	ii
KATA PENGANTAR.....	iii
DAFTAR ISI.	v
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xi
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah.....	2
1.3 Tujuan.....	2
1.4 Pembatasan Masalah.....	2
1.5 Spesifikasi Hardware.....	2
1.6 Sistematika Pembahasan.....	3
BAB II TEORI PENUNJANG.....	4
2.1 Kriptografi.....	4
2.1.1 Teori Kriptografi.....	4
2.2 Algoritma Simetris dan Asimetris.....	6
2.2.1 Algoritma Simetris.....	6
2.2.2 Algoritma Asimetris.....	7
2.2.3 Block Cipher dan Stream Cipher.....	8
2.3 Mode Operasi dalam Block Cipher.....	9

2.3.1 Electronic Codebook (ECB)	9
2.3.2 Cipher Block Chaining (CBC)	10
2.4 Teori Matematika.....	11
2.4.1 Bilangan Prima.....	11
2.4.2 Operasi Modulus.....	12
2.4.3 Algoritma Euclidean.....	12
2.4.4 Algoritma Extended Euclidean.....	13
2.4.5 Exponensial Modulus.....	14
2.4.6 Fungsi XOR.....	15
2.5 Enkripsi dan Dekripsi Dengan Algoritma Camellia.....	15
2.5.1 Enkripsi Dengan Algoritma Camellia.....	15
2.5.2 Dekripsi Dengan Algoritma Camellia.....	16
2.5.3 Panjang dari Kunci yang Bervariasi.....	17
2.5.4 Penjadwalan Kunci.....	17
2.6 Komponen-Komponen Camellia.....	21
2.6.1 Fungsi – F.....	21
2.6.2 Fungsi – P.....	21
2.6.3 Fungsi – S.....	22
2.6.4 S – box.....	22
2.6.5 Fungsi FL.....	25
2.6.6 Fungsi FL^{-1}	25
2.7 Algoritma Validasi Data.....	26
2.8 Tanda Tangan Digital.....	26

2.8.1 Algoritma Pembangkit Kunci Tanda Tangan Digital	27
2.8.2 Algoritma Tanda Tangan Digital.....	27
2.8.3 Algoritma Verifikasi Tanda Tangan Digital.....	27
BAB III PERANCANGAN DAN REALISASI PERANGKAT LUNAK.....	28
3.1 Realisasi Perangkat Lunak.....	28
3.2 Program Utama	31
3.3 Program Enkripsi.....	31
3.4 Program Dekripsi.....	36
3.5 Program Timer.....	41
3.6 Program Pembangkit Tanda Tangan Digital.....	41
3.6.1 Sub Program rdmprime.....	43
3.6.2 Sub Program gcd.....	44
3.6.3 Sub Program Euclid.....	44
3.6.4 Sub Program Validasi.....	46
3.6.5 Program Pencocokan Tanda Tangan Digital.....	46
BAB IV HASIL PENGAMATAN.....	48
4.1 Hasil Pengamatan Sederhana Program Enkripsi dan Dekripsi Camellia.....	48
4.1.1 Pengamatan Enkripsi Camellia Dengan Plain Text Berbeda dan Kunci Yang Sama.	48
4.1.2 Pengamatan Enkripsi Camellia Dengan Plain Text Yang Sama dan Berbeda Dengan Kunci Yang Berbeda.....	49
4.2 Hasil Pengamatan Program Enkripsi dan Dekripsi Camellia Terhadap File Text Dengan Menggunakan Kunci Yang Berbeda.....	49

4.2.1 Proses Enkripsi dan Dekripsi Camellia Terhadap File Text Dengan Kunci Yang Pertama “elektromarnat”	49
4.2.2 Proses Enkripsi dan Dekripsi Camellia Terhadap File Text Dengan Kunci Yang Kedua “ukm”	51
4.3 Hasil Pengamatan Waktu Dan Ukuran File Proses Enkripsi dan Dekripsi Camellia.....	52
4.3.1 Pengamatan Waktu Enkripsi dan Dekripsi Dengan Kunci Yang Sama....	52
4.4 Pengamatan Enkripsi dan Dekripsi Dengan Kunci Yang Salah.....	53
4.5 Hasil Pengamatan Proses Enkripsi dan Dekripsi Camellia Dalam Proses Validasi.....	54
4.6 Hasil Pengamatan Proses Tanda Tangan Digital.....	56
4.6.1 Pengamatan Proses Tanda Tangan Digital Dengan Public Key Yang Sama.....	56
4.6.2 Pengamatan Proses Tanda Tangan Digital Dengan Public Key Yang Salah.....	56
4.7 Analisa Hasil Pengamatan.....	57
BAB V KESIMPULAN DAN SARAN.....	58
5.1 Kesimpulan.....	58
5.2 Saran.....	58
Daftar Pustaka.....	59
Lampiran A Listing Program	A-1
Lampiran B Subtitution Box.....	B-1
Lampiran C Tampilan Program.....	C-1

DAFTAR GAMBAR

Gambar 2.1	Diagram Proses Enkripsi dan Dekripsi.....	5
Gambar 2.2	Diagram Proses Enkripsi dan Dekripsi Algoritma Simetris.....	6
Gambar 2.3	Diagram Proses Enkripsi dan Dekripsi Algoritma Asimetris.....	7
Gambar 2.4	Skema Mode Operasi ECB.....	9
Gambar 2.5	Skema Mode Operasi CBC.....	10
Gambar 2.6	Penjadwalan Kunci.....	19
Gambar 2.7	Fungsi – F.....	21
Gambar 2.8	Fungsi FL.....	25
Gambar 2.9	Fungsi FL^{-1}	26
Gambar 3.1	Tampilan Program Membuat Plain Text.....	28
Gambar 3.2	Tampilan Program Enkripsi.....	29
Gambar 3.3	Tampilan Program Dekripsi.....	30
Gambar 3.4	Diagram Alir Program Pengaman Data.....	30
Gambar 3.5	Diagram Alir Pengolahan Plain Text.....	31
Gambar 3.6	Prosedur Enkripsi Camellia Untuk Kunci 128 - bit.....	33
Gambar 3.7	Prosedur Enkripsi Camellia Untuk Kunci 192/256 – bit.....	34
Gambar 3.8	Diagram Alur Program Enkripsi	35
Gambar 3.9	Prosedur Dekripsi Camellia Untuk Kunci 128 - bit.....	38
Gambar 3.10	Prosedur Dekripsi Camellia Untuk Kunci 192/256 – bit.....	39
Gambar 3.11	Diagram Alur Program Dekripsi	35
Gambar 3.12	Diagram Alir Program Pembangkit Tanda Tangan Digital.....	42

Gambar 3.13 Diagram Alir Sub Program RdmPrime.....	43
Gambar 3.14 Diagram Alir Sub Program gcd.....	44
Gambar 3.15 Diagram Alir Sub Program Euclid.....	45
Gambar 3.16 Diagram Alir Sub Program Data Validasi.....	46
Gambar 3.17 Diagram Alir Sub Program Pencocokan Tanda Tangan Digital.....	46
Gambar 3.18 Diagram Alir Sub Program Pangkatmod.....	47
Gambar 4.1 Pengecekan Dengan menggunakan Kunci Yang Berbeda.....	54
Gambar 4.2 Pengecekan Validasi.....	55
Gambar 4.3 Pengecekan Tanda Tangan Digital.....	57

DAFTAR TABEL

Tabel 2.1 Nilai Extended Euclidean	13
Tabel 2.2 Penjadwalan Kunci Yang Konstan.....	18
Tabel 2.3 Kunci Rahasia Untuk Subkey 128-bit dan 182/256-bit.....	20
Tabel 2.4 S – Box1.....	23
Tabel 2.5 S – Box2.....	23
Tabel 2.6 S – Box3.....	24
Tabel 2.7 S – Box4.....	24
Tabel 4.1 Enkripsi dan Dekripsi Dengan Kunci Yang Sama, PlainText Berbeda.....	48
Tabel 4.2 Enkripsi dan Dekripsi Dengan PlainText Yang Sama dan Berbeda Dengan Kunci Yang Berbeda.....	49
Tabel 4.3 Hasil Pengamatan Proses Enkripsi Camellia.....	52
Tabel 4.4 Hasil Pengamatan Proses Dekripsi Camellia.....	53