

ABSTRAK

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak yang tidak diinginkan dapat menimbulkan kerugian bagi pemilik informasi.

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

Pada tugas akhir ini berhasil direalisasikan sebuah perangkat lunak untuk pengaman data berbasis algoritma simetrik metoda XTEA dengan menggunakan bahasa pemrograman Dephi.

ABSTRACT

Security problem is one the most important aspect in an information system. Importance value of information is often makes the information wanted to be accessed by certain person only. Fall of information to the unwanted side can cause losses to info's owner.

Many solutions can be used to handle information's security problem. One of solutions to protect data is to encrypt the data. There are two general types of encryption algorithm, symmetric algorithm and asymmetric algorithm. The Algorithm that used in this project is XTEA, one of symmetric algorithm type that encodes and decodes using only one same key. Sent data is encrypted data or so called the ciphertext. After data is received, data will be processed back to the original data or so called the plaintext.

In this project has successfully built an encryption software base on Extended Tiny Encryption Algorithm by using Delphi as programming language.

DAFTAR ISI

ABSTRAK.....	i
ABSTRACT.....	ii
KATA PENGANTAR.....	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xi
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 Spesifikasi Hardware.....	2
1.6 Sistematika Pembahasan.....	3
BAB II TEORI PENUNJANG.....	4
2.1 Kriptografi.....	4
2.1.1 Tujuan Kriptografi.....	7
2.2 Enkripsi dan Dekripsi Menggunakan Kunci.....	8
2.3 Algoritma Simetri Dan Algoritma Asimetri.....	9
2.3.1 Algoritma Simetri.....	9
2.3.2 Algoritma Asimetri.....	10
2.4 Mode Operasi Enkripsi Blok Cipher.....	12
2.5 Teori Matematika.....	13

2.5.1 Fungsi XOR.....	14
2.5.2 Bilangan Prima.....	14
2.5.3 Operasi Modulus.....	15
2.5.4 Algoritma Euclidean.....	16
2.5.5 Algoritma <i>Extended Euclidean</i>	17
2.5.6 Eksponensial Modulus.....	18
2.6 Enkripsi Dengan Algoritma XTEA.....	20
2.7 Algoritma Validasi Data.....	22
2.8 Algoritma Pembangkit <i>Private Key</i> dan <i>Public Key</i>	22
2.9 <i>Feistel Cipher</i>	22
BAB III Perancangan dan Realisasi Perangkat Lunak.....	24
3.1 Pengolahan Kunci XTEA.....	24
3.2 Program Enkripsi.....	24
3.3 Program Dekripsi.....	28
3.4 Program Pembangkit <i>Privat Key</i> dan <i>Public Key</i>	30
3.4.1 Sub Program <i>rdmprime</i>	31
3.4.2 Sub Program <i>gcd</i>	32
3.4.3 Sub Program <i>Euclid</i>	32
3.4.4 Program Validasi.....	34
3.4.5 Sub Program <i>Pangkatmod</i>	34
3.5 Realisasi Program.....	36
3.5.1 Program Enkripsi.....	36
3.5.2 Program Dekripsi.....	37

3.5.3 Program <i>Timer</i>	38
BAB IV Data Pengamatan.....	39
4.1 Hasil Pengamatan Sederhana Program Enkripsi dan Dekripsi XTEA.....	39
4.1.1 Pengamatan Enkripsi XTEA Dengan Kunci Yang Sama.....	39
4.1.2 Pengamatan Enkripsi XTEA Dengan Kunci Yang Berbeda.....	45
4.2 Hasil Pengamatan Program Enkripsi dan Dekripsi Menggunakan File.....	49
4.2.1 Proses Enkripsi XTEA Dengan Menggunakan File.....	49
4.3 Hasil Pengamatan Waktu Dan Ukuran File.....	54
4.3.1 Pengamatan Enkripsi Dan Dekripsi Menggunakan Kunci Yang Sama..	54
4.3.2 Pengamatan Enkripsi Dan Dekripsi Menggunakan Kunci Yang Beda..	55
4.3.3 Pengamatan enkripsi Dan Dekripsi Menggunakan Kunci Delta Yang Berbeda.....	57
4.4 Pengamatan Hasil Proses Validasi.....	58
4.4.1 Pengamatan Terhadap Perubahan <i>Ciphertext</i>	58
4.4.2 Pengamatan Terhadap Perubahan <i>Public Key</i>	63
4.4.3 Pengamatan Terhadap Perubahan <i>File Validasi</i>	64
4.5 Analisa Hasil Pengamatan.....	65
BAB V Kesimpulan Dan Saran.....	67
5.1 Kesimpulan.....	67
5.2 Saran.....	67
Daftar Pustaka.....	68

Lampiran A Listing Program	A-1
Lampiran B Tampilan Program	B-1

DAFTAR GAMBAR

Gambar 2.1.... Kriptografi dengan proses enkripsi dan dekripsi	6
Gambar 2.2 Kriptografi Simetri Umum.....	9
Gambar 2.3 Kriptografi Asimetri Umum.....	11
Gambar 2.4 Diagram Umum Feistel Cipher	23
Gambar 3.1 Diagram Alur Pengolahan <i>Plaintext</i>	25
Gambar 3.2 Diagram Alur Proses Enkripsi	27
Gambar 3.3 Diagram Alur Proses Dekripsi	29
Gambar 3.4 Diagram Alur Program Pembangkit Kunci Tanda Tangan Digital	30
Gambar 3.5 Diagram Alir Sub Program RdmPrime	31
Gambar 3.6 Diagram Alir Sub Program gcd	32
Gambar 3.7 Diagram Alir Sub Program Euclid	33
Gambar 3.8 Diagram Alir Program Validasi	34
Gambar 3.9 Diagram Alir Sub Program pangkatmod	35
Gambar 3.10 Tampilan Program Enkripsi	36
Gambar 3.11 Tampilan Program Dekripsi	37
Gambar 4.1 Tampilan program enkripsi algoritma <i>XTEA</i> dengan <i>plaintext</i> “percobaan” kunci “kunci”	40
Gambar 4.2 Tampilan penyimpan hasil enkripsi	41
Gambar 4.3 Tampilan penyimpanan kode validasi.....	42
Gambar 4.4 Tampilan percobaan program dekripsi algoritma <i>XTEA</i>	43

Gambar 4.5	Isi dari <i>teks01dekrip.txt</i>	44
Gambar 4.6	Tampilan program enkripsi algoritma <i>XTEA</i> dengan <i>plaintext</i> “percobaan 2”, kunci “coba”	46
Gambar 4.7	Tampilan program dekripsi dari algoritma <i>XTEA plaintext</i> “percobaan 2” dengan kunci “coba”	47
Gambar 4.8	Isi dari <i>coba2dekrip.txt</i>	48
Gambar 4.9	Tampilan program enkripsi algoritma <i>XTEA</i> dengan <i>plaintext</i> <i>file original_text.txt</i> , kata kunci “kunci”	50
Gambar 4.10	Tampilan program dekripsi dari <i>file original_text_enkrip.txt</i> dengan menggunakan kunci “kunci”, disimpan dalam <i>file</i> <i>original_text_dekrip.txt</i>	52
Gambar 4.11	Isi dari <i>original_text_dekrip.txt</i>	53
Gambar 4.12	Tidak valid karena kesalahan public key	64

DAFTAR TABEL

Tabel 2.1	Nilai <i>Extended Euclidean</i>	18
Tabel 4.1	Enkripsi dan dekripsi menggunakan kunci yang sama, <i>plaintext</i> yang berbeda-beda	39
Tabel 4.2	Enkripsi dan dekripsi menggunakan kunci yang sama, <i>plaintext</i> yang berbeda-beda	45
Tabel 4.3	Hasil Pengamatan Proses Enkripsi XTEA	54
Tabel 4.4	Hasil Pengamatan Proses Dekripsi XTEA	55
Tabel 4.5	Hasil pengamatan Enkripsi file menggunakan kunci yang berbeda, <i>plaintext</i> yang sama	56
Tabel 4.6	Hasil pengamatan Enkripsi file menggunakan kunci yang berbeda, <i>plaintext</i> yang sama	56
Tabel 4.7.	Hasil pengamatan Enkripsi file menggunakan kunci kedua yang berbeda, <i>plaintext</i> yang sama.....	57
Tabel 4.8.	Hasil pengamatan Enkripsi file menggunakan kunci kedua yang berbeda, <i>plaintext</i> yang sama.....	58