

ABSTRAK

Perkembangan pesat teknologi informasi sekarang ini sangat mempengaruhi kehidupan masyarakat, terutama kebutuhan akan informasi dan komunikasi. Keamanan data informasi merupakan faktor utama dan terdepan yang menentukan apakah data informasi tersebut aman dan berada di tangan yang semestinya. Tingkat keamanan data informasi yang akan digunakan bermacam – macam bergantung pada kegunaan data informasi tersebut.

Salah satu teknik pengamanan data informasi di dunia internet adalah penggunaan teknik algoritma kriptografi. Suatu algoritma kriptografi berisi fungsi-fungsi matematika yang digunakan untuk melakukan proses enkripsi dan dekripsi. Algoritma kriptografi yang digunakan merupakan jenis algoritma kriptografi simetrik yang menggunakan kunci rahasia yang sama untuk proses enkripsi dan dekripsinya.

Tugas akhir ini menggunakan algoritma kriptografi Einstein sebagai salah satu cara untuk mengamankan data. Algoritma Einstein direalisasikan dengan menggunakan program Microsoft Visual Basic 6. Pada algoritma Einstein, terdapat proses acak (*random*) yang menggunakan metoda kongruensial linear (*linear congruential method*). Algoritma Einstein mempunyai kelebihan dalam melakukan proses enkripsi dan dekripsi pada hampir semua jenis *file* yang umum digunakan. Algoritma Einstein bisa diimplementasikan untuk semua ukuran *file*.

ABSTRACT

Information technology growth rapidly nowadays makes influence in social society, especially information and communication needs. Information data security is major and first thing factor to decide what if the information data is secure and in the proper hand. Information data security levels which will be used depend on the usage of the information data.

One of information data security technique in internet realm is cryptography algorithm technique usage. Cryptography algorithm contains the mathematics function used to conduct the process of encrypts and decrypts. Cryptography algorithm used represents the symmetrical algorithm type using same key of encrypt and decrypts process.

This Final Assignment is using Einstein cryptography algorithm as one of securing data technique. Realization Einstein algorithm makes use of Microsoft Visual Basic 6 program. Einstein algorithm make use random process using linear congruencies method. Einstein Algorithm has the excess in conducting process encrypts and decrypts at almost file type which is often used. Einstein Algorithm can be implemented for all size file.

DAFTAR ISI

LEMBAR PENGESAHAN	
SURAT PERNYATAAN	
ABSTRAK	i
<i>ABSTRAC</i>	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR TABEL	viii
DAFTAR GAMBAR	ix
Bab I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Identifikasi Masalah	1
I.3 Tujuan	2
I.4 Pembatasan Masalah	3
I.5 Sistematika Pembahasan	3
Bab II TEORI PENUNJANG	4
II.1 Kriptologi, Kriptanalisis, Kriptografi, dan Sistem Kripto	4
II.1.1 Tujuan Kriptografi	5
II.1.1.1 Kebutuhan Autentikasi	5
II.1.2 Dimensi Kriptografi	12
II.1.3 Ancaman Serangan	12
II.1.3.1 Penyusupan Pihak ke 3	12
II.1.3.2 Serangan Acak	13
II.1.3.3 <i>Eavesdropping</i>	13
II.1.3.4 <i>Chosen ciphertext attack</i>	13
II.1.3.5 <i>Adaptive chosen ciphertext attack</i>	14
II.1.3.6 Kriptanalisis	14
II.1.3.7 <i>Differential Cryptanalysis</i>	15
II.1.3.8 <i>Linear Cryptanalysis</i>	15
II.1.4 Enkripsi dan Dekripsi	16

II.1.5 Algoritma dan Pengaturan Kunci	17
II.1.5.1 Algoritma Simetrik	18
II.1.5.2 Algoritma Asimetrik	20
II.1.6 Pemeriksaan kunci	21
II.1.6.1 Infrastruktur Kunci Publik	22
II.1.6.2 Jaringan Kepercayaan	22
II.1.6.3 Otoritas Sertifikasi Robot	23
II.1.7 Angka Acak	23
II.1.7.1 Fungsi Angka Acak	23
II.1.7.2 Pembuatan Angka Acak	24
II.2 Teori Matematika	24
II.2.1 Bilangan Prima	24
II.2.2 Operasi Modulus	25
II.2.3 Operasi XOR	26
II.2.4 Angka <i>Pseudorandom</i> dengan metoda kongruensial linear	26
II.3 Algoritma Einstein	27
II.3.1 Algoritma Enkripsi Einstein	28
II.3.2 Algoritma Dekripsi Einstein	29
II.3.3 Proses Acak	29
Bab III IMPLEMENTASI ALGORITMA DAN REALISASI	
PERANGKAT LUNAK	31
III.1 Perangkat Lunak Pengamanan Data Algoritma Einstein	31
III.2 Program Utama	33
III.2.1 Program Enkripsi	33
III.2.2 Program Pemeriksaan Kunci Untuk Enkripsi	34
III.2.3 Program Dekripsi	35
III.2.4 Program Pemeriksaan Kunci Untuk Dekripsi	37
III.2.5 Program Acak	37
Bab IV HASIL PENGAMATAN	39
IV.1 Perangkat Lunak Pengamanan Data	39
IV.2 Hasil Pengamatan	39
IV.3 Analisa Hasil Pengamatan	41

Bab V KESIMPULAN DAN SARAN	42
V.1 Kesimpulan	42
V.2 Saran	42
DAFTAR PUSTAKA	43
LAMPIRAN A <i>LISTING</i> PROGRAM	
LAMPIRAN B GAMBAR dan TAMPILAN PROGRAM	

DAFTAR TABEL

Tabel IV.1 Hasil Pengamatan

40

DAFTAR GAMBAR

Gambar II.1 Kegunaan dasar enkripsi pesan	8
Gambar II.2 Kegunaan dasar autentikasi pesan	10
Gambar II.3 Kegunaan dasar fungsi <i>hash</i>	11
Gambar II.4 Diagram blok proses enkripsi dan dekripsi	16
Gambar II.5 Contoh penggunaan <i>stream cipher</i> pada algoritma RC4	18
Gambar II.6 Proses enkripsi <i>block cipher</i>	19
Gambar II.7 Proses dekripsi <i>block cipher</i>	19
Gambar II.8 Algoritma simetrik	20
Gambar II.9 Algoritma asimetrik	21
Gambar II.10 Gerbang logika XOR	26
Gambar III.1 Diagram alir perangkat lunak algoritma Einstein	32
Gambar III.2 Diagram alir proses enkripsi	34
Gambar III.3 Diagram alir pemeriksaan kunci untuk enkripsi	35
Gambar III.4 Diagram alir program dekripsi	36
Gambar III.5 Diagram alir pemeriksaan kunci untuk dekripsi	37