

**SISTEM KEAMANAN DATA DENGAN ALGORITMA  
KRIPTOGRAFI RIJNDAEL DAN ALGORITMA  
STEGANOGRAFI LSB**

**SKRIPSI**

**DEDE PURNAMA**

**041401033**



**PROGRAM STUDI S-1 ILMU KOMPUTER  
DEPARTEMEN ILMU KOMPUTER  
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS SUMATERA UTARA**

**MEDAN**

**2008**

## PERSETUJUAN

Judul : SISTEM KEAMANAN DATA DENGAN  
ALGORITMA KRIPTOGRAFI RIJNDAEL DAN  
ALGORITMA STEGANOGRAFI LSB

Kategori : SKRIPSI  
Nama : DEDE PURNAMA  
Nomor Induk Mahasiswa : 041401033  
Program Studi : SARJANA (S1) ILMU KOMPUTER  
Departemen : ILMU KOMPUTER  
Fakultas : MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
(FMIPA) UNIVERSITAS SUMATERA UTARA

Diluluskan di  
Medan, 9 September 2008

Komisi Pembimbing

Pembimbing 2

Pembimbing 1

Drs. James P. Marbun, M.Kom.  
Zarlis  
NIP 131 639 804

Prof. Dr. Muhammad  
NIP 131 570 434

Diketahui/Disetujui oleh  
Departemen Ilmu Komputer FMIPA USU  
Ketua,

Prof. Dr. Muhammad Zarlis  
NIP 131 570 434

## **PERNYATAAN**

**SISTEM KEAMANAN DATA DENGAN ALGORITMA KRIPTOGRAFI  
RIJNDAEL DAN ALORITMA STEGANOGRAFI LSB**

## **SKRIPSI**

Saya mengakui bahwa skripsi ini adalah hasil kerja saya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, 9 September 2008

DEDE PURNAMA  
041401033

## **PENGHARGAAN**

Puji dan syukur penulis panjatkan kepada Allah SWT karena dengan limpahan karuniaNya skripsi ini berhasil diselesaikan dalam waktu yang ditetapkan.

Ucapan terima kasih penulis sampaikan kepada Prof. Dr. Muhammad Zarlis dan Drs. James Peter Marbun M.Kom. selaku pembimbing pada skripsi ini yang telah memberikan panduan dan arahan serta kepercayaan kepada penulis untuk menyempurnakan kajian ini. Panduan ringkas, padat dan profesional telah diberikan kepada penulis agar penulis dapat menyelesaikan tugas ini. Ucapan terima kasih juga ditujukan kepada Ketua dan Sekretaris Departemen Ilmu Komputer yaitu Prof. Dr. Muhammad Zarlis dan Syahriol Sitorus S.Si, M.IT. Dekan dan Pembantu Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sumatera Utara. Semua dosen dan pegawai pada Departemen Ilmu Komputer FMIPA USU.

Ucapan terima kasih penulis ucapkan juga kepada orangtua, suami, adik-adik dan kakak penulis serta sahabat-sahabat penulis yang telah memberikan semangat dan dorongan serta berlapang hati untuk membantu penulis dalam pembuatan skripsi ini.

Akhirnya penulis berharap bahwa skripsi ini bermanfaat terutama kepada penulis maupun para pembaca serta semua pihak yang berhubungan dengannya. Penulis menyadari sepenuhnya bahwa kajian ini sangat jauh dari sempurna. Oleh karena itu kritik dan saran yang membangun sangat diharapkan demi perbaikan skripsi ini.

## **ABSTRAK**

Dalam komunikasi data, memungkinkan pengiriman data jarak jauh yang relatif cepat dan murah. Di pihak lain pengiriman data jarak jauh misalnya melalui internet dengan jumlah pemakai yang banyak, memungkinkan pihak lain menyadap dan mengubah data. Dalam penelitian ini penulis menggunakan algoritma kriptografi Rijndael sehingga data dapat terjaga kerahasiaannya dengan cara menyandikan pesan tersebut ke dalam kode-kode tertentu. Setelah data disandikan selanjutnya data tersebut disembunyikan dengan menggunakan algoritma steganografi LSB, sehingga menurut penulis jika kedua algoritma ini digunakan dalam sebuah sistem keamanan data akan relatif sulit dipecahkan oleh kriptanalis. Walaupun dalam penerapannya, waktu yang dibutuhkan pada saat pemrosesan lebih lama dibandingkan dengan hanya menggunakan salah satu algoritma tersebut, namun manfaat penggunaan sistem ini adalah ciphertext yang disembunyikan akan menyulitkan kriptanalis dalam menganalisa ciphertext.

# **THE SECURITY SYSTEM OF DATA BY USING RIJNDAEL CRYPTOGRAPHY ALGORITHM AND LSB STEGANOGRAPHY ALGORITHM**

## **ABSTRACT**

In data communication, it is possible to send data in far distance that is relatively faster and cheaper. The other side, sending the data in far distance, for example by using internet with many users, will make cryptanalyst could steals or changes the data. In this research, the writer uses Rijndael cryptography algorithm in order to make the data more safe by coding the message to the exact code. After the coding, the data will be hidden by using LSB steganography algorithm, so in the writer opinion, if both of algorithms are used in security system of data, it will be difficult for cryptanalyst to cryptanalyze. Although in the implementation, the time to process that two algorithms is slower than the time to process one of the algorithm, but the useful by using this system is that the ciphertext that being hidden will make difficult for cryptanalyst to analyse the ciphertext.

## DAFTAR ISI

Halaman	
Persetujuan	ii
Pernyataan	iii
Penghargaan	iv
Abstrak	v
Abstract	vi
Daftar Isi	vii
Daftar Tabel	ix
Daftar Gambar	x
BAB 1	PENDAHULUAN
1	
1.1	Latar Belakang 1
1.2	Perumusan Masalah 2
1.3	Batasan Masalah 2
1.4	Tujuan Penelitian 2
1.5	Manfaat Penelitian 3
1.6	Metode Penelitian 3
1.7	Sistematika Penulisan 4
BAB 2	LANDASAN TEORI
5	
2.1	Kriptografi 5
2.1.1	Definisi Kriptografi 5
2.1.2	Macam-macam Algoritma Kriptografi 7
2.1.3	Keamanan Algoritma 8
2.1.4	Algoritma Rijndael 9
2.1.4.1	Algoritma Enkripsi Rijndael 14
2.2	Steganografi 19
2.2.1	Definisi Steganografi 20
2.2.2	Carrier File 20
2.2.3	Steganografi Gambar 23
2.2.3.1	Kategori Gambar 23
2.2.3.2	Resolusi Gambar

2.2.4	Algoritma LSB	25
BAB 3 ANALISIS PERMASALAHAN		27
3.1	Analisis Algoritma Rijndael	27
3.1.1	Proses Enkripsi Rijndael	27
3.1.2	Proses Dekripsi Rijndael	39
3.1.3	Analisis File	49
3.2	Analisis Algoritma LSB	51
3.3	Flowchart	55
3.3.1	Flowchart Enkripsi Rijndael	56
3.3.2	Flowchart Ekspansi Kunci Enkripsi	58
3.3.3	Flowchart ShiftRow Kunci	60
3.3.4	Flowchart Dekripsi Rijndael	61
3.3.5	Flowchart Ekspansi Kunci Dekripsi	63
3.3.6	Flowchart InvShiftRow	65
3.3.7	Flowchart sembunyikan Pesan	66
3.3.8	Flowchart Baca Pesan	68
BAB 4 PERANCANGAN DAN IMPLEMENTASI		
4.1	Perancangan	70
4.1.1	Perancangan Antarmuka	70
4.1.1.1	Tampilan Utama	71
4.1.1.2	Tampilan Menu Utama	71
4.1.1.3	Rancangan Tampilan Input Picture	72
4.1.1.4	Rancangan Tampilan Write Message	73
4.1.1.5	Rancangan Tampilan Finish	75
4.1.1.6	Rancangan Tampilan Decryption	78
4.1.1.7	Rancangan Tampilan About	79
4.2	Implementasi	79
4.3	Penerapan Program	90
BAB 5 PENUTUP		
5.1	Kesimpulan	92
5.2	Saran	93
DAFTAR PUSTAKA		94
LAMPIRAN A: LISTING PROGRAM		96
LAMPIRAN B: DAFTAR KODE ASCII		127



## DAFTAR GAMBAR

	Halaman
Gambar 2.1 Alir Proses Enkripsi	16
Gambar 2.2 Diagram Alir Proses Dekripsi	19
Gambar 3.1 Contoh gambar yang akan menyembunyikan informasi	53
Gambar 3.2 Flowchart Program Sistem Keamanan Data	55
Gambar 3.3 Flowchart Enkripsi Rijndael	56
Gambar 3.4 Flowchart Ekspansi Kunci Enkripsi Rijndael	58
Gambar 3.5 Flowchart ShiftRow Rijndael	60
Gambar 3.6 Flowchart Dekripsi Rijndael	61
Gambar 3.7 Flowchart Ekspansi Kunci Dekripsi Rijndael	63
Gambar 3.8 Flowchart InvShiftRow Rijndael	65
Gambar 3.9 Flowchart Tulis Pesan LSB	66
Gambar 3.10 Flowchart Baca Pesan	68
Gambar 4.1 Gambar RancanganTampilan Awal	71
Gambar 4.2 Gambar Rancangan Tampilan Menu Utama	72
Gambar 4.3 Gambar Rancangan Tampilan Input Picture 1	73
Gambar 4.4 Gambar Rancangan Tampilan write Message	74
Gambar 4.5 Gambar Rancangan Tampilan Finish	75
Gambar 4.6 Rancangan View Detail Proses Enkripsi	76
Gambar 4.7 Rancangan View Detail Proses Dekripsi	77
Gambar 4.8 Gambar Rancangan Tampilan Decryption	78
Gambar 4.9 Gambar Rancangan Tampilan About	79
Gambar 4.10 Tampilan Utama	80
Gambar 4.11 Tampilan Menu Utama	81
Gambar 4.12 Tampilan Input Picture 1	81
Gambar 4.13 Tampilan Input Picture	82
Gambar 4.14 Tampilan Information	82
Gambar 4.15 Tampilan Error	83
Gambar 4.16 Tampilan Write Message	84
Gambar 4.17 Tampilan Finish	85
Gambar 4.18 Tampilan Hasil Enkripsi	86
Gambar 4.19 Tampilan Decryption 1	87
Gambar 4.20 Tampilan Decryption 2	88
Gambar 4.21 Tampilan Finish Decryption	88
Gambar 4.22 Tampilan Hasil Dekripsi	89

Gambar 4.23 Tampilan About	89
Gambar 4.22 Contoh Gambar 1	90
Gambar 4.23 Contoh GAmbar 2	90

## **DAFTAR TABEL**

	Halaman
Tabel 2.1 Perbandingan Algoritma	11
Tabel 2.2 Perbandingan Beberapa Cipher	12
Tabel 2.3 Perbandingan jumlah Round dan Key	13
Tabel 2.4 S-Box dalam Rijndael	15
Tabel 2.5 Invers S-Box Dalam Rijndael	18
Tabel 3.1 Round Constanta (Rcon)	28
Tabel 3.2 RoundKey Enkripsi	29
Tabel 3.3 Roundkey Dekripsi	40
Tabel 4.1 Laporan Hasil Pengujian	91