PENERAPAN ALGORITMA RIJNDAEL DALAM ENKRIPSI FILE SECARA SIMETRIK MENGGUNAKAN BAHASA C#

SURACHMAN
41505120003

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2011

PENERAPAN ALGORITMA RIJNDAEL DALAM ENKRIPSI FILE SECARA SIMETRIK MENGGUNAKAN BAHASA C#

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

SURACHMAN
41505120003

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2011

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41505120003

Nama : SURACHMAN

Judul Skripsi : PENERAPAN ALGORITMA RIJNDAEL DALAM ENKRIPSI FILE SECARA SIMETRIK MENGGUNAKAN BAHASA C#

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 10 Juni 2011.

(SURACHMAN)

LEMBAR PERSETUJUAN

NIM	:	41505120003
Nama	:	SURACHMAN
Judul Skripsi	:	PENERAPAN ALGORITMA RIJNDAEL DALAM ENKRIPSI FILE SECARA SIMETRIK MENGGUNAKAN BAHASA C#.

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI
JAKARTA, 10 JUNI 2011

Abdusy Syarif, ST., MT
Pembimbing

Ida Nurhaida ST., MT
Koord. Tugas Akhir Teknik Informatika

Devi Fitrianah, S.Kom., MTI
KaProdi Teknik Informatika

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Allah SWT yang telah memberikan taufik dan hidayah-Nya kepada penulis sehingga penulis akhirnya dapat menyelesaikan tugas akhir ini dengan judul "PENERAPAN ALGORITMA RIJNDAEL DALAM ENKRIPSI FILE SECARA SIMETRIK MENGGUNAKAN BAHASA C#".

Tugas akhir ini merupakan salah satu syarat untuk menempuh ujian akhir pada program Strata Satu (S-1) Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana Jakarta.

Dalam penulisan ini penulis banyak mendapat bantuan, saran baik bimbingan dan dorongan dari berbagai pihak sehingga kesulitan yang penulis hadapi dalam penulisan ini dapat terlewati dengan baik, dan akhirnya tugas akhir ini dapat diselesaikan sebagaimana mestinya. Untuk itu penulis mengucapkan terima kasih yang sebesar-besarnya kapada banyak pihak yang telah memberikan bantuan baik pikiran, tenaga maupun waktu sehingga tugas akhir ini dapat diselesaikan. Dalam kesempatan ini penulis mengucapkan banyak terima kasih kepada :

1. Bapak Abdusy Syarif, ST. MT. selaku pembimbing tugas akhir, Terima kasih atas bantuan dan bimbingan serta waktunya dalam menyelesaikan tugas akhir ini.
2. Para Dosen dan staff administrasi Universitas Mercu Buana.
3. Kepada keluargaku, Bapak,Ibu dan Istri tercinta serta anak-anaku yang telah memberikan curahan kasih sayang, pengertian dan selalu memotivasi sehingga penulis dapat menyelesaikan tugas akhir ini.
4. Finance & Accounting Comtextile (HK) Ltd Jakarta, Terima kasih atas pengertian dan dukungannya sehingga penulis bisa memiliki waktu untuk menyusun tugas akhir ini.
5. Angkatan VIII IT PKSM Universitas Mercu Buana, terima kasih atas kebersamaan serta kekompakannya selama ini.

Serta pihak-pihak lain yang tidak dapat penulis sebutkan namanya satu persatu.

Semoga Allah SWT memberikan balasan atas segala bantuan yang telah diberikan kepada penulis.

Akhir kata, dengan segala kerendahan hati penulis berharap semoga tulisan ini dapat bermanfaat bagi penulis khususnya dan para pembaca pada umumnya.

Jakarta, Juni 2011.

DAFTAR ISI

LEMBAR PERNYATAAN i
LEMBAR PERSETUJUAN ii
KATA PENGANTAR iii
ABSTRACTION v
ABSTRAKSI vi
DAFTAR ISI vii
DAFTAR GAMBAR x
DAFTAR TABEL xi
DAFTAR SIMBOL xii
BAB I PENDAHULUAN
1.1. Latar Belakang 1
1.2. Rumusan Masalah 3
1.3. Tujuan Penulisan 3
1.4. Batasan Masalah 3
1.5. Metodologi 4
1.6. Sistematika Pembahasan 5

BAB II LANDASAN TEORI
2.1. Enkripsi dan Dekripsi 6
2.2. Algoritma dan Kunci 7
2.2.1. Algoritma Kriptografi Simetrik 8
2.2.2. Algoritma Kriptografi Asimetrik 8
2.3. Enrkripsi File 8
2.4. Algoritma Rijndael 9
2.4.1. Proses Enkripsi Algoritma Rijndael 11
2.4.2. Proses Dekripsi Algoritma Rijndael 17
2.5. Konsep Object Oriented Programming 18
2.6. Unified Modelling Language (UML) 21
2.6.1. Use Case Diagram 22
2.6.2. Class Diagram 22
2.6.3. State Mechine Diagram 23
2.6.4. Sequence Diagram 24
2.6.5. Activity Diagram 25
2.6.6. Componen Diagram 26
2.6.7. Deployment Diagram 27

2.6.8. Class Responsibility Colaboration 27
2.7. Bagan Alir Siste 28
2.8. Daur Hidup Pengembangan Sistem 29
2.9. Bahasa Pemrograman Visual C# 32
2.9.1. Struktur Penulisan Kode C# 35
2.9.2. Aksesories penulisan kode C# 37
2.9.3 Kompilasi (Compile) Aplikasi 38

BAB III ANALISA DAN PERANCANGAN
3.1. Analisa Masalah 41
3.1.1. Analisa Struktur File 45
3.1.2. Analisa Proses Enkripsi Rijndael 47
3.1.2.1. Analisa Pembentukan ExpandKey pada Proses Enkripsi 49
3.1.2.2. Analisa SubByte pada Proses Enkripsi 51
3.1.2.3. Analisa ShiftRow pada Proses Enkripsi 51
3.1.2.4. Analisa MixColumn pada Proses Enkripsi 53
3.1.2.5. Analisa AddRoundKey pada Proses Enkripsi 54
3.1.3. Analisia Proses Dekripsi Rijndael 54
3.1.3.1. Analisa Pembentukan ExpandKey pada Proses Dekripsi 55
3.1.3.2. Analisa AddRoundKey pada Proses Dekripsi 56
3.1.3.3. Analisa Invers ShiftRow pada Proses Dekripsi 56
3.1.3.4. Analisa Invers SubByte pada Proses Dekripsi 57
3.1.3.5. Analisa Invers AddRoundKey pada Proses Dekripsi 58
3.1.4. Analisa Penerapan Enkripsi dan Dekripsi 58
3.1.5. Analsia Dampak Sistem 61
3.2. Analisa Kebutuhan Pembangunan Aplikasi 62
3.2.1 Deskripsi Umum Sistem 62
3.2.2 Analisis Spesifikasi dan Kebutuhan Aplikasi 63
3.2.3 Batasan Rancangan Sistem 64
3.2.4 Use Case 64
3.2.5 Aktivity Diagram 67

3.3. Perancangan Kelas 69
3.4 Perancangan Antarmuka Perangkat Lunak 70

BAB IV IMPLEMENTASI DAN PENGUJIAN
4.1. Lingkungan Implementasi 73
4.1.1. Lingkungan Perangkat Keras 73
4.1.2. Lingkungan Perangkat Lunak 73
4.1.3. Batasan Implementasi 73
4.1.4. Implementasi Kelas 74
4.1.5. Implementasi Operasi pada Kelas 75
4.1.6. Implementasi Antar Muka 79
4.2. Pengujian Aplikasi 81
4.2.1. Pengujian Proses Enkripsi dan Dekripsi 81
4.2.2 Pengujian performansi aplikasi 85
4.2.3 Analisa Hasil Pengujian 87

BAB V KESIMPULAN DAN SARAN
5.1. Kesimpulan 88
5.2. Saran 89
DAFTAR PUSTAKA 90
LAMPIRAN 91

DAFTAR GAMBAR

			Halaman
1.	Gambar 2.1.	Proses enkripsi dan dekripsi pada plaintext dan Ciphertext	6
2.	Gambar 2.2.	Proses dekripsi dan enkripsi dengan kunci	7
3.	Gambar 2.3.	Notasi Prosedur Algoritma Enripsi Rijndael	10
4.	Gambar 2.4	Ilustrasi array *state*	10
5.	Gambar 2.5	Illustrasi pengisian array state	11
6.	Gambar 2.6.	Diagram Proses Enkripsi Rijndael	12
7.	Gambar 2.7.	Ilustrasi Transformasi SubBytes() Rijndael	12
8.	Gambar 2.8.	Hasil Transformasi Subbytes() Rijndael	13
9.	Gambar 2.9.	Ilustrasi Transformasi ShiftRow() Rijndael	13
10.	Gambar 2.10.	Ilustrasi Perkalian Matriks MixColumn() Rijndael	14
11.	Gambar 2.11.	Ilustrasi Transformasi MixColumn() Rijndael	15
12.	Gambar 2.12.	Hasil Transformasi MixColumn() Rijndael	15
13.	Gambar 2.13.	Ilustrasi Transformasi AddRoundKey() Rijndael	15
14.	Gambar 2.14.	Hasil Transformasi AddRoundKey() Rijndael	16
15.	Gambar 2.15.	Diagram Proses Dekripsi Rijndael	16
16.	Gambar 2.17.	*Use Case* Model	22
17.	Gambar 2.18.	Notasi *Sequence diagram*	25
18.	Gambar 2.19.	Notasi C*omponent Diagram*	26
19.	Gambar 2.20.	Notasi *deployment diagram*	27
20.	Gambar 2.21.	Notasi CRC	28
21.	Gambar 2.22.	Tahapan siklus secara umum	30
22.	Gambar 2.23.	Model Waterfall	31
23.	Gambar 2.24.	Tampilan com*mand-line compiler* dari *Visual Studio .NET*	39
24.	Gambar 2.25.	Tampilan awal Microsoft Visual Studio 2010	40
25.	Gambar 2.26.	Tampilan ketika memulai proyek baru dalam Microsoft Visual Studio 2010	40
26.	Gambar 3.1.	Fungsi pilihan keamanan pada *Microsoft Word.*	42
27.	Gambar 3.2.	Pencarian Google untuk menembus dokumen *word*	42
28.	Gambar 3.3.	Program *Password Recovery Word 2007*	43
29.	Gambar 3.4.	Contoh dokumen *microsoft word*	43
30.	Gambar 3.5.	Dokumen *microsoft word* dibuka dengan notepad	44
31.	Gambar 3.6.	Dokument *word* yang diberi password dan dibuka dengan notepad	44
32.	Gambar 3.7.	Alur enkripsi Rijndael (A) & Alur dekripsi Rijndael (B)	48
33.	Gambar 3.8.	Use Case Diagram	65
34.	Gambar 3.9.	Aktivity Diagram enkripsi	67
35.	Gambar 3.10.	Aktivity Diagram dekripsi	68
36.	Gambar 3.11.	Diagram kelas perancangan	69
37.	Gambar 3.12.	Form input kunci enkripsi/dekripsi	70
38.	Gambar 3.13.	Rancangan antarmuka Pendaftaran Folder	70
39.	Gambar 3.14.	Rancangan antarmuka Proses Enkripsi/Dekripsi	71
40.	Gambar 4.1.	Tampilan awal saat program dijalanan	79
41.	Gambar 4.2.	Tampilan pemberitahuan inisialisasi folder	79

42. Gambar 4.3. Tampilan penambahan folder 80
43. Gambar 4.4. Tampilan proses siap dilakukan 80
44. Gambar 4.5. File Test1.txt asli 83
45. Gambar 4.6. File Test1.txt dibuka dengan hex editor 83
46. Gambar 4.7. File Test1.txt.enk terenkripsi dibuka dengan hex editor 84
47. Gambar 4.8. Proses Enkripsi File 85
48. Gambar 4.9. Proses Dekripsi File 85

DAFTAR TABEL

			Halaman
1.	Tabel 2.1.	Tabel S-box yang digunakan dalam transformasi SubByte() Rijndael pada proses enkripsi	13
2.	Tabel 2.2	Tabel S-box yang digunakan dalam transformasi InvSubByte() Rijndael pada proses dekripsi	18
3.	Tabel 2.3	Notasi Kelas	23
4.	Tabel 2.4	Notasi-notasi pada *state machine diagram*	23
5.	Tabel 2.5.	Notasi-notasi pada *activity diagram*	25
6.	Tabel 2.6.	Simbol Bagan Alir Sistem	29
7.	Tabel 2.7.	Daftar karakter khusus pada bahasa C#	38
8.	Tabel 3.1.	Konversi plain teks dalam bit dan hexadesimal	46
9.	Tabel 3.2	File PDF dalam plain text, bit dan hexadesimal	46
10.	Tabel 3.3	Kunci rounde ke-1 sampai ke-10 proses enkripsi	51
11.	Tabel 3.4	Referensi tabel subbyte proses enkripsi	52
12.	Tabel 3.5	Kunci rounde ke-1 sampai ke-10 proses enkripsi	55
13.	Tabel 3.6	Referensi Tabel Subbyte Proses Dekripsi	57
14.	Tabel 4.1	Daftar Implementasi Kelas	74
15.	Tabel 4.2	Implementasi operasi pada kelas FormPassword	75
16.	Tabel 4.3	Implementasi operasi pada kelas FormProses	75
17.	Tabel 4.4	Implementasi operasi pada kelas KryptoManager	77
18.	Tabel 4.5	Implementasi operasi pada kelas InisialisasiFile	78
19.	Tabel 4.6	Implementasi operasi pada kelas ListFileSelection	78
20.	Tabel 4.7	Daftar Pengujian Aplikasi	81
21.	Tabel 4.8	Hasi enkripsi dan dekripsi file sederhana	81
22.	Tabel 4.9	Pengujian lanjutan terhadap aplikasi	84
23.	Tabel 4.10	Pengujian performansi dari aplikasi	86