



**Aplikasi Kriptografi Dengan Algoritma (*Advanced Encryption Standard*) AES
Menggunakan Microsoft Visual C Sharp Berbasis Desktop**



PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCUBUANA
JAKARTA
2016



**Aplikasi Kriptografi Dengan Algoritma (*Advanced Encryption Standard*) AES
Menggunakan Microsoft Visual C Sharp Berbasis Desktop**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
MERCU BUANA

RIZKI ANGGA PRABOWO

41512010052

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2016

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41512010052
Nama : Rizki Angga Prabowo
Judul Tugas Akhir : Aplikasi Kriptografi Dengan Algoritma (*Advanced Encryption Standard*) AES Menggunakan Microsoft Visual C Sharp Berbasis Desktop.

Menyatakan bahwa Tugas Akhir dengan judul yang tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

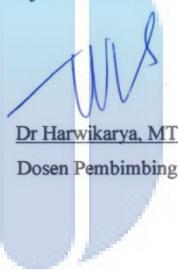
Jakarta, Juni 2016



LEMBAR PENGESAHAN

Nama : Rizki Angga Prabowo
NIM : 41512010052
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul : Aplikasi Kriptografi Dengan Algoritma (*Advanced Encryption Standard*) AES Menggunakan Microsoft Visual C Sharp Berbasis Desktop

Jakarta, Juni 2016
Disetujui dan diterima oleh,


Dr Harwikarya, MT
Dosen Pembimbing


UNIVERSITAS
MERCU BUANA
Dr. Yaya Sudarya Triana, M.Kom
Kaprodi Informatika
Desi Ramayanti, S.Kom, MT
Koordinator Tugas Akhir

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas karunia yang telah diberikan kepada penulis sehingga penulis dapat menyelesaikan Laporan Tugas Akhir tepat pada waktunya, dimana Laporan Tugas Akhir tersebut merupakan salah satu persyaratan untuk menyelesaikan Program Sarjana pada Jurusan Informatika Universitas Mecu Buana Jakarta.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Penulis juga menyadari Laporan Tugas Akhir ini takkan dapat selesai tepat pada waktunya tanpa bantuan, bimbingan, dan motivasi dari berbagai pihak. Maka dari itu, dengan segala kerendahan hati, Penulis ingin menyampaikan ucapan terimakasih kepada:

1. Bapak Dr Harwikarya, MT, selaku Pembimbing Tugas Akhir yang telah membimbing penulis dengan semua nasihat, semangat dan ilmunya dalam menyusun laporan tugas akhir ini.
2. Bapak Yaya Sudarya, M.Kom selaku Kaprodi Informatika Universitas Mercu Buana.
3. Ibu Desi Ramayanti, S.Kom, MT selaku Koordinator Tugas Akhir Informatika Universitas Mercu Buana.
4. Bapak Sabar Rudiarto, M.Kom selaku dosen Pembimbing Akademik Informatika Universitas Mecu Buana.
5. Kedua orang tua penulis yang begitu banyak memberikan dukungan baik, Do'a maupun semangat serta motivasi yang tak pernah hentinya.
6. Rekan seperjuangan, Keluarga Besar Informatika. Khususnya kawan-kawan Informatika angkatan 2012 yang selalu memberi motivasi dan semangat serta inspirasi kepada penulis.
7. Berserta semua pihak yang telah memotivasi dan ikut memberikan bantuannya kepada penulis yang namanya tidak dapat saya sebutkan satu per satu.

Semoga Tuhan Yang Maha Esa membala kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua. Amin

Jakarta, Mei 2016

Rizki Angga Prabowo



DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PERNYATAAN	ii
LEMBAR PERSETUJUAN.....	iii
KATA PENGANTAR	iv
ABSTRACT.....	vi
ABSTRAK	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xii
DAFTAR TABEL.....	xv
DAFTAR LAMPIRAN.....	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan dan Manfaat.....	2
1.5 Metode Penelitian.....	3
1.5.1 Metode Pengumpulan Data	3
1.5.2 Metode Perancangan Aplikasi.....	3
1.6 Jadwal Pelaksanaan	4
1.7 Sistematika Penulisan	5
BAB II LANDASAN TEORI	5
2.1 Kriptografi	5
2.2 Sejarah Kriptografi	6
2.3 Algoritma Kriptografi.....	9

2.4	Sejarah (<i>Advanced Encryption Standard</i>) AES.....	11
2.5	Panjang Kunci dan Ukuran Blok AES	11
2.6	Algoritma <i>Advanced Encryption Standard (AES)</i>	12
2.6.1	<i>Key Expansion</i>	15
2.6.2	Transformasi <i>AddRoundKey</i>	16
2.6.3	Transformasi <i>SubBytes()</i>	17
2.6.4	Transformasi <i>ShiftRows()</i>	18
2.6.5	Transformasi <i>MixColumns</i>	19
2.7	Microsoft Visual C Sharp.....	20
2.7.1	Visual C Sharp (C#)	20
2.8	Metode <i>Waterfall</i>	21
2.9	Bagan Alir Sistem (<i>flowchart</i>).....	22
BAB III ANALISA DAN PERANCANGAN		24
3.1	Analisa Sistem.....	24
3.2	Penyelesaian Masalah.....	24
3.3	Kebutuhan Sistem.....	25
3.4	Analisa Kebutuhan Sistem	25
3.5	Rancangan Sistem	25
3.6	Rancangan Layar	26
3.6.1	Rancangan Layar Menu Home	26
3.6.2	Rancangan Layar <i>Form Encryption File</i>	27

3.6.3 Rancangan Layar <i>Form Decryption File</i>	28
3.6.4 Rancangan Layar <i>Form About</i>	28
3.6.5 Rancangan Layar <i>Form Help</i>	29
3.7 Bagan Alir (<i>Flowchart</i>)	30
3.7.1 Flowchart <i>Form Home</i>	30
3.7.2 Flowchart <i>Form Encryption</i>	31
3.7.3 Flowchart <i>Form Decryption</i>	32
3.7.4 Flowchart <i>Form About</i>	33
3.7.5 Flowchart <i>Form Help</i>	33
3.8 Pseudocode	34
3.8.1 Proses pada <i>Form Home</i>	34
3.8.2 Proses pada <i>Form Encryption</i>	35
3.8.3 Proses pada <i>Form Decryption</i>	36
3.8.4 Proses pada <i>Form About</i>	36
3.8.5 Proses Pada <i>Form Help</i>	37
3.8.5 Proses <i>Encryption Advanced Encryption Standard (AES)</i>	37
3.8.7 Proses <i>Decryption Pada Advanced Encryption Standard (AES)</i> ...	38
BAB IV IMPLEMENTASI DAN PENGUJIAN	41
4.1 Implementasi Program.....	41
4.2 Implementasi Antar Muka	41
4.2.1 Tampilan Layar <i>Form Home</i>	42

4.2.2	Tampilan Layar <i>Form Encryption</i>	42
4.2.3	Tampilan Layar <i>Form Decryption</i>	46
4.2.4	Tampilan Layar <i>Form About</i>	49
4.2.5	Tampilan Layar <i>Form Help</i>	49
4.3	Pengujian Program	50
4.3.1	Proses Enkripsi dan Dekripsi <i>File Txt, Docx, Pdf, Xlsx atau Pptx.</i>	50
4.4	Tabel Pengujian	58
4.4.1	Pengujian <i>Black Box</i> Pada <i>Form Home</i>	58
4.4.2	Pengujian Black Box Pada Form Encryption.....	58
4.4.3	Pengujian Black Box Pada Form Decryption.....	59
4.4.4	Pengujian <i>Black Box</i> Pada <i>Form About</i>	59
4.4.5	Pengujian <i>Black Box</i> Pada <i>Form Help</i>	59
4.4.6	Pengujian Proses Enkripsi	60
4.4.7	Pengujian Proses Dekripsi	60
4.5	Evaluasi Program	61
BAB V KESIMPULAN DAN SARAN.....		63
5.1	Kesimpulan.....	63
5.2	SARAN.....	63
DAFTAR PUSTAKA		64

DAFTAR GAMBAR

Gambar 2.1 Proses Kriptografi Secara Umum.....	5
Gambar 2.2 Tulisan yang menggunakan Hieroglyph	6
Gambar 2.3 Scytale	7
Gambar 2.4 Mesin Enigma	8
Gambar 2.5 Blok Diagram Proses Enkripsi	13
Gambar 2.6 Blok Diagram Dekripsi AES-128	14
Gambar 2.7 Ilustrasi Prosedur rijndael key schedule.....	15
Gambar 2.8 Lanjutan Ilustrasi Prosedur <i>rijndael key schedule</i>	16
Gambar 2.9 S-box	17
Gambar 2.10 S-box invers	18
Gambar 2.11 Operasi <i>ShiftRows</i> Pada Blok 128-bit	18
Gambar 2.12 Ilustrasi Transformasi <i>Mixcolumns</i>	20
Gambar 2.13 Metode <i>Waterfall</i>	22
Gambar 2.14 Daftar simbol flowchart.....	23
Gambar 3.1 Arsitektur Kerja Aplikasi	26
MERCU BUANA	
Gambar 3.2 Rancangan Layar <i>Form Menu Home</i>	27
Gambar 3.3 Rancangan Layar <i>Form Encryption File</i>	27
Gambar 3.4 Rancangan Layar <i>Form Decryption File</i>	28
Gambar 3.5 Rancangan Layar <i>Form About</i>	29
Gambar 3.6 Rancangan Layar <i>Form Help</i>	29
Gambar 3.7 Flowchart <i>Form Home</i>	30
Gambar 3.8 Flowchart <i>Encryption</i>	31
Gambar 3.9 Flowchart <i>Form Decryption</i>	32

Gambar 3.10 Flowchart <i>Form About</i>	33
Gambar 3.11 Flowchart <i>Form Help</i>	34
Gambar 4.1 Tampilan Layar <i>Form Home</i>	42
Gambar 4.2 Tampilan <i>Form Encryption</i>	43
Gambar 4.3 Tampilan Layar <i>Choose File Encryption</i>	43
Gambar 4.4 Tampilan Layar <i>Alert Message Pilih File Encryption</i>	44
Gambar 4.5 Tampilan <i>Alert Message Masukkan Password</i>	44
Gambar 4.6 Tampilan <i>Alert Message Salah Input Confirm Password</i>	45
Gambar 4.7 Tampilan Layar Enkripsi Berhasil	45
Gambar 4.8 Tampilan <i>Form Decryption</i>	46
Gambar 4.9 Tampilan Layar <i>Alert Message Pilih File Decryption</i>	46
Gambar 4.10 Tampilan <i>Choose File Decryption</i>	47
Gambar 4.11 Tampilan <i>Alert Message Masukkan Password</i>	47
Gambar 4.12 Tampilan Layar <i>Alert Message Salah Confirm Password</i> ..	48
Gambar 4.13 Tampilan Layar Proses Dekripsi Berhasil.....	48
Gambar 4.14 Tampilan Layar <i>Form About</i>	49
Gambar 4.15 Tampilan Layar <i>Form Help</i>	49
Gambar 4.16 Tampilan Isi <i>File Docx</i>	50
Gambar 4.17 Tampilan Isi <i>File Txt</i>	51
Gambar 4.18 Tampilan Isi <i>File PDF</i>	51
Gambar 4.19 Tampilan Isi <i>File Xlsx</i>	52
Gambar 4.20 Tampilan Isi <i>File Pptx</i>	52
Gambar 4.21 Tampilan Hasil Enkripsi <i>File Docx</i>	53
Gambar 4.22 Tampilan Hasil Enkripsi <i>File Txt</i>	53

Gambar 4.23 Tampilan Hasil Enkripsi <i>File Pdf</i>	54
Gambar 4.24 Tampilan Hasil Enkripsi <i>File Xlsx</i>	54
Gambar 4.25 Tampilan Hasil Enkripsi <i>File Pptx</i>	55
Gambar 4.26 Tampilan Hasil Dekripsi <i>File Docx</i>	55
Gambar 4.27 Tampilan Hasil Dekripsi <i>File Txt</i>	56
Gambar 4.28 Tampilan Hasil Dekripsi <i>File Pdf</i>	56
Gambar 4.29 Tampilan Hasil Dekripsi <i>File Xlsx</i>	57
Gambar 4.30 Tampilan Hasil Dekripsi <i>File Pptx</i>	57



DAFTAR TABEL

Tabel 1.1 Tabel Kegiatan Pelaksaan Pembuatan Aplikasi.....	4
Tabel 2.1 Tabel Panjang Kunci dan Ukuran Blok <i>Rijndael</i>	11
Tabel 4.1 Pengujian <i>Black Box</i> Pada <i>Form Home</i>	58
Tabel 4.2 Pengujian <i>Black Box</i> Pada <i>Form Ecryption</i>	58
Tabel 4.3 Pengujian <i>Black Box</i> Pada <i>Form Decryption</i>	59
Tabel 4.4 Pengujian <i>Black Box</i> Pada <i>Form About</i>	59
Tabel 4.5 Pengujian <i>Black Box</i> Pada <i>Form Help</i>	59
Tabel 4.6 Hasil Pengujian Proses Enkripsi	60
Tabel 4.7 Hasil Pengujian Proses Dekripsi	60
Tabel 4.7 Hasil Pengujian Proses Dekripsi	61



DAFTAR LAMPIRAN

Lampiran 1 : Daftar Absensi Bimbingan Tugas Akhir.....

