



**PERANCANGAN APLIKASI KRIPTOGRAFI
MENGUNAKAN METODE MESSAGE DIGEST5 (MD5)**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana
Komputer

Oleh :

SARYANI
41508110023

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



**PERANCANGAN APLIKASI KRIPTOGRAFI
MENGUNAKAN METODE MESSAGE DIGEST5 (MD5)**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana
Komputer

Oleh :

SARYANI
41508110023

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

LEMBAR PENGESAHAN

NIM : 41508110023
Nama : SARYANI
Judul Skripsi : PERANCANGAN APLIKASI KRIPTOGRAFI
MENGUNAKAN METODE MESSAGE DIGEST 5
(MD5)

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

JAKARTA, Maret 2011

Ari Sukmawibowo B.Eng, M.IT

Pembimbing

Ida Nurhaida, ST., MT

Koord. Tugas akhir Teknik Informatika

Devi Fitrianah, S.Kom., MTI

Kaprodi Teknik Informaka

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41508110023
Nama : SARYANI
Judul Skripsi : PERANCANGAN APLIKASI KRIPTOGRAFI
MENGUNAKAN METODE MESSAGE DIGEST 5
(MD5)

Menyatakan Bahwa skripsi tersebut diatas adalah hasil karya 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, Maret 2011

(SARYANI)

KATA PENGANTAR

Puji Syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, Sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

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

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan tugas akhir ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan trima kasih kepada:

1. Bapak, ibu dan seluruh keluarga tercinta yang telah mendukung penulis baik spirit maupun materi.
2. Bapak Ari Sukmawibowo B.Eng, M.IT, selaku pembimbing tugas akhir pada jurusan teknik informatika Universitas Mercu Buana.
3. Teman-temanku tercinta yang selalu memberikan spirit maupun materi untuk terus menyelesaikan tugas akhir ini.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Jakarta, Maret 2011

Penulis

DAFTAR ISI

	Hal
HALAMAN PERNYATAAN	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
ABSTRACTION.....	iv
ABSTRAKSI	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR	x
DAFTAR TABEL	xii

BAB I PENDAHULUAN

1.1. Latar Belakang	1
1.2. Ruang Lingkup.....	2
1.3 Perumusan Masalah	3
1.3. Batasan Masalah.....	3
1.4. Tujuan Perancangan	3
1.5. Metode Penelitian.....	4
1.6. Sistematika Penulisan	4

BAB II LANDASAN TEORI

2.1. Sistem Perangkat Lunak.....	6
2.2. Rekayasa Perangkat Lunak	6
2.3. Proses Perangkat Lunak	7
2.4. Prinsip Dasar Kriptografi	9
2.5. Tujuan Kriptografi	11
2.6. Fungsi Hash Satu Arah	11
2.7. Message Digest5 (MD5)	12
2.7.1 Prinsip Dasar Message Digest5 (MD5)	13

2.7.2	Algoritma Message Digest5 (MD5)	14
2.7.3	Hash-Hash Message Digest5 (MD5)	16
2.8.	Jenis Metode Enkripsi Yang Lain	16
2.8.1	Metode Data Encryption Standard (DES)	16
2.8.2	Metode Anvanced Encryption Standard (AES)	17
2.9	Visual C++ 2005	17
2.9.1	Fungsi Dasar	18
2.9.1.1	Fungsi Main	18
2.9.1.2	File Header	18
2.9.1.3	Fungsi printf() atau cout <<	18
2.9.1.4	Fungsi scanf() atau cin >>	19
2.9.1.5	Komentar Dalam Program	19
2.9.2	Pemrograman Berorientasi Objek Dalam Visual C++	19
2.9.2.1	Enkapsulation	19
2.9.2.2	Inheritance	20
2.9.2.3	Polimorfisme	20
2.9.2.4	Struktur dan Kelas	21
2.10	Pengujian	22

BAB III ANALISA DAN PERANCANGAN

3.1	Analisa Masalah	23
3.2	Strategi Pemecahan Masalah	23
3.3	Pembahasan Algoritma	24
3.3.1	Gambaran Umum Algoritma Message Digest5 (MD5)	24
3.3.2	Algoritma Enkripsi	26
3.4	Perancangan Aplikasi	32
3.5	Rancangan Tampilan Layar	33
3.6	Pengukuran Tingkat Kecepatan Aplikasi Enkripsi MD5	35

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1	Implementasi Program	37
4.2	Fungsi – Fungsi Dalam Enkripsi MD5	43

4.3 Fungsi Browse File	43
4.4 Fungsi OnBnClickedBrowseButton()	44
4.5 Fungsi OnBnClickedEnkripButton()	45
4.5.1 Fungsi OnButtonClickedResetButton()	48
4.5.2 Fungsi OnFileOpen()	49
4.5.3 Fungsi OnFileExit()	49
4.5.4 Fungsi OnHelpAbout()	49
4.5.5 Fungsi OnBnClickedOkButton()	50
4.5.6 Fungsi - Fungsi Direktif Yang Dipakai	50
4.5.6.1 Fungsi Direktif F()	50
4.5.6.2 Fungsi Direktif G()	50
4.5.6.3 Fungsi Direktif H()	50
4.5.6.4 Fungsi Direktif I()	51
4.5.6.5 Fungsi Direktif ROTATE_LEFT().....	51
4.5.6.6 Fungsi Direktif FF()	51
4.5.6.7 Fungsi Direktif GG()	51
4.5.6.8 Fungsi Direktif HH()	52
4.5.6.9 Fungsi Direktif II()	52
4.5.7 Fungsi – Fungsi Utama Untuk Operasi MD5	52
4.5.7.1 Fungsi MD5Init().....	52
4.5.7.2 Fungsi MD5Update()	53
4.5.7.3 Fungsi MD5Final()	54
4.5.7.4 Fungsi MD5Transform()	55
4.5.7.5 Fungsi MD5Encode()	57
4.5.7.6 Fungsi MD5Decode()	58
4.5.7.7 Fungsi MD5_memcpy()	59
4.5.7.8 Fungsi MD5_memset()	59
4.6 Pengujian	60
4.6.1 Pengujian GUI (Graphical User Interface)	60
4.6.2 Pengujian Berganda (Multiple Testing)	61
4.6.3 Pengujian Kecepatan	63
4.7 Analisa Hasil Pengujian	67

BAB V KESIMPULAN DAN SARAN

5.1. Kesimpulan 71

5.2. Saran 71

DAFTAR PUSTAKA 72

LAMPIRAN 73

DAFTAR GAMBAR

	Hal
Gambar 2.1 Model Waterfall	8
Gambar 2.2 Proses Enkripsi dan Dekripsi	10
Gambar 2.3. Enkripsi-Dekripsi Kunci Simetrik	10
Gambar 2.4 Enkripsi-Dekripsi Kunci Asimetrik	10
Gambar 2.5 Fungsi hash satu arah	12
Gambar 2.6 Algoritma MD5	14
Gambar 3.1 Flowchart Enkripsi Data Menggunakan MD5	27
Gambar 3.2 Rancangan Tampilan Awal	33
Gambar 3.3 Rancangan Tampilan Form Utama	34
Gambar 3.4 Rancangan Tampilan Menu File	35
Gambar 3.5 Rancangan Tampilan About MD5	35
Gambar 4.1 Tampilan menu awal program	38
Gambar 4.2 Tampilan program utama MD5 Enkripsi	39
Gambar 4.3 Tampilan About MD5 Enkripsi	39
Gambar 4.4 Tampilan kesalahan jika teks masih kosong	40
Gambar 4.5 Tampilan pesan jika proses enkripsi berhasil	41
Gambar 4.6 Tampilan hasil enkripsi berhasil (metode mengetikkan teks langsung)	42
Gambar 4.7 Tampilan hasil enkripsi berhasil (metode membuka dari file teks)	42
Gambar 4.8 Tampilan hasil pengujian GUI	61
Gambar 4.9 Tampilan hasil pengujian berganda pola a (pertama)	62
Gambar 4.10 Tampilan hasil pengujian berganda pola b	63
Gambar 4.11 Tampilan hasil pengujian berganda pola a (kedua)	64
Gambar 4.12 Tampilan pengujian kecepatan pertama	65
Gambar 4.13 Tampilan pengujian hasil kecepatan pertama	65
Gambar 4.14 Tampilan pengujian kecepatan kedua	66
Gambar 4.15 Tampilan pengujian hasil kecepatan kedua	66

Gambar 4.16 Tampilan pengujian kecepatan ketiga	67
Gambar 4.17 Tampilan pengujian hasil kecepatan ketiga	67
Gambar 4.18 Tampilan pengujian kecepatan keempat	68
Gambar 4.19 Tampilan pengujian hasil kecepatan keempat	68
Gambar 4.20 Tampilan pengujian kecepatan kelima	69
Gambar 4.21 Tampilan pengujian hasil kecepatan kelima	69

DAFTAR TABEL

	Hal
Tabel 3.1 Tabel Operasi AND	25
Tabel 3.2 Tabel Operasi NOT	25
Tabel 3.3 Tabel Operasi OR	25
Tabel 3.4 Tabel Operasi XOR.....	25
Tabel 3.5 Tabel Operasi pergeseran bit ke kanan	26
Tabel 3.5 Tabel Operasi pergeseran bit ke kiri	26
Tabel 4.1 Tabel Hasil Enkripsi	48
Tabel 4.2 Tabel Analisis Hasil Pengujian	70