



**PENERAPAN METODE ENKRIPSI IDEA, FUNGSI
HASH MD5 DAN METODE KOMPRESI HUFFMAN
UNTUK KEAMANAN DAN EFISIENSI RUANG
DOKUMEN**

PESTA FERDINAN SITOANG
41506110049

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2010



**PENERAPAN METODE ENKRIPSI IDEA, FUNGSI
HASH MD5 DAN METODE KOMPRESI HUFFMAN
UNTUK KEAMANAN DAN EFISIENSI RUANG
DOKUMEN**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
PESTA FERDINAN SITOANG
41506110049

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2010

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41506110049
Nama : PESTA FERDINAN SITOANG
Judul Skripsi : PENERAPAN METODE ENKRIPSI IDEA, FUNGSI
HASH MD5 DAN METODE KOMPRESI HUFFMAN
UNTUK KEAMANAN DAN EFISIENSI RUANG
DOKUMEN

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, 22 Februari 2010

(Pesta Ferdinan Sitohang)

LEMBAR PENGESAHAN

NIM : 41506110049
Nama : PESTA FERDINAN SITOANG
Judul Skripsi : PENERAPAN METODE ENKRIPSI IDEA, FUNGSI
HASH MD5 DAN METODE KOMPRESI HUFFMAN
UNTUK KEAMANAN DAN EFISIENSI RUANG
DOKUMEN

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

JAKARTA, 22 Februari 2010

Raka Yusuf, ST., MTI
Pembimbing

Devi Fitriana, S.Kom., MTI

Koord. Tugas Akhir Teknik Informatika

Abdusy Syarif, ST., MT

Kaprodi Teknik Informatika

KATA PENGANTAR

Puji dan syukur Penulis panjatkan kepada Tuhan Yang Maha Kuasa atas berkat dan rahmatNya Penulis telah diberi kesehatan dan kesempatan sehingga dapat menyelesaikan dokumen ini. Penulis mengucapkan terimakasih yang sebesar-besarnya kepada seluruh pihak yang telah mendukung di dalam pelaksanaan TA ini. Penulis mohon maaf apabila di sini Penulis tidak dapat menyebut semua nama yang telah membantu dalam penyelesaian TA ini, namun bukan berarti mengurangi rasa hormat dan terimakasih Penulis kepada mereka. Secara khusus Penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Ayah dan Ibu atas segala cinta, pengorbanan, dukungan, perhatian, kepercayaan, serta doa yang menyertai Penulis selama ini.
2. Bapak Raka Yusuf selaku Pembimbing yang telah membimbing, mengevaluasi, memberikan masukan dan saran untuk memperbaiki segala kekurangan isi dokumen.
3. Dosen penguji Tugas Akhir yang telah menguji, mengevaluasi dan memberikan saran perbaikan laporan TA pada saat Sidang TA.
4. Semua staf akademik dan non akademik Program Studi Teknik Informatika yang telah memberikan banyak ilmu selama masa perkuliahan, dan telah membantu selama masa perkuliahan dan masa pengerjaan TA.
5. Marolop Sitohang, Febrin Sitohang, Saut Sitohang, dan Verawati Grace br. Sitohang yang selalu memberri semangat dan mendukung di dalam doa.

6. Rosinta Eveline Rosalina Tampubolon yang senantiasa menemani, memberi dukungan, semangat dan pengorbanan untuk menyelesaikan tugas akhir Penulis.
7. Rekan-rekan lainnya yang senantiasa memberikan semangat buat Penulis.

Jakarta, 22 Februari 2010

NIM 41506110049, Pesta Ferdinan Sitohang

DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	I
LEMBAR PENGESAHAN	II
KATA PENGANTAR	III
ABSTRACT	V
ABSTRAK	VI
DAFTAR TABEL	X
DAFTAR GAMBAR	XI
DAFTAR LAMPIRAN	XIII
BAB I	1
PENDAHULUAN	1
1.1. LATAR BELAKANG	1
1.2. TUJUAN PEMBAHASAN	2
1.3. BATASAN MASALAH	3
1.4. METODOLOGI	3
1.5. SISTEMATIKA PEMBAHASAN	4
BAB II LANDASAN TEORI	5
2.1. KRIPTOGRAFI	5
2.1.1. Pengenalan	5
2.1.2. Sejarah Kriptografi	7
2.1.3. Kriptografi Modern	8
2.1.3.1. Teori keamanan Shannon	9
2.1.3.2. Kriptografi Standar	10
2.1.3.3. Public Key	11
2.2. INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)	12
2.2.1. Operasi	12
2.2.2. Blok dasar	17
2.2.2.1. Bitwise eXclusive OR (XOR)	17
2.2.2.2. Tambah Modulo 2^{16}	18
2.2.2.3. Perkalian modulo $2^{16}+1$	18
2.2.2.4. Blok-blok pembalikan	20
2.2.3. Arsitektur Dasar IDEA	20
2.2.3.1. Putaran IDEA	21
2.2.3.2. Unit kontrol	21
2.2.3.3. Penjadwalan kunci	22
2.3. FUNGSI HASH MD5	24
2.3.1. Sejarah dan Pemecahan Tulisan-Tulisan Rahasia	24

2.3.2. Kerentanan terhadap serangan	25
2.3.3. Pengujian Integritas	26
2.3.4. Algoritma	26
2.3.5. Hash-hash MD5	28
2.4. KOMPRESI	29
2.4.1. Lossless dan Lossy	30
2.4.2. Aplikasi	32
2.4.3. Teori	33
2.5. KODE HUFFMAN	34
2.5.1. Deskripsi Permasalahan	35
2.5.2. Teknik Dasar	38
2.5.3. Tipe-tipe Kode Huffman	41
2.6. DIAGRAM ALIRAN DATA	44
2.6.1. Mengembangkan diagram aliran-data	46
2.6.1.1. Pendekatan Top-Down (Atas-Bawah)	46
2.6.1.2. Pendekatan Berdasarkan Pembagi-bagian	47
2.6.1.3. Level Diagram Aliran Data	48
2.6.1.3.1. Diagram Level Konteks	48
2.6.1.3.2. Diagram Level 1	49
2.6.1.3.3. Diagram Level 2 (Level diagram yang lebih rendah)	50
BAB III ANALISIS DAN PERANCANGAN	52
3.1. ANALISIS MASALAH	52
3.2. ALTERNATIF SOLUSI	53
3.3. DESKRIPSI SISTEM	54
3.4. PERANCANGAN	55
3.4.1. Diagram Aliran Data	55
3.4.1.1. Diagram Konteks	55
3.4.1.2. DAD Level 1	56
3.4.1.3. DAD Level 2 Proses Hash	57
3.4.1.4. DAD Level 2 Proses Kompresi	58
3.4.1.5. DAD Level 2 Proses Enkripsi	59
3.4.1.6. DAD Level 2 Dekripsi, Dekompresi	60
3.4.2. Flowchart	61
3.4.2.1. File Masukan	62
3.4.2.2. Membentuk Nilai Hash MD5	62
3.4.2.2.1. Penambahan Bit-bit Penyangga	62
3.4.2.2.2. Penambahan Panjang Pesan	63
3.4.2.2.3. Inisialisasi Penyangga MD	64
3.4.2.2.4. Proses Blok-blok Pesan	65
3.4.2.3. Keluaran	69
3.4.2.4. Mengkompres File	69
3.4.2.4.1. Pembentukan Pohon Biner HUFFMAN	69
3.4.2.4.2. Proses Encoding	70
3.4.2.4.3. Keluaran	73
3.4.2.4.4. Proses Decoding	73
3.4.2.5. Proses Enkripsi International Data Encryption Algorithm	73
3.4.2.6. Proses Penghilangan Enkripsi (Dekripsi)	75

3.4.2.7. Proses Perbandingan Nilai Hash MD5	75
3.4.3. Perancangan Antarmuka	76
3.4.3.1. Menu Awal	76
3.4.3.2. Menu Layar Dua	76
3.4.3.3. Menu Layar Tiga	77
BAB IV IMPLEMENTASI DAN PENGUJIAN	78
4.1. IMPLEMENTASI	78
4.1.1. MD5	78
4.1.2. Metode kompresi HUFFMAN	84
4.1.3. Enkripsi IDEA	96
4.1.4. Antarmuka	99
4.2. PENGUJIAN	101
4.2.1. Lingkungan pengujian	101
4.2.2. Pengujian Black Box	102
4.2.2.1. Skenario Pengujian	102
4.2.2.2. Hasil Pengujian	103
4.2.2.3. Analisis Hasil Pengujian	104
4.2.2.4. Pengujian Metode	105
4.2.2.4.1. Pengujian MD5	106
4.2.2.4.2. Pengujian Huffman	107
4.2.2.4.3. Pengujian Enkripsi IDEA	111
4.2.3. Pengujian White Box	113
BAB V KESIMPULAN DAN SARAN	116
5.1. KESIMPULAN	116
5.2. SARAN	116
DAFTAR PUSTAKA	XIV
LAMPIRAN	ERROR! BOOKMARK NOT DEFINED.

DAFTAR TABEL

	Halaman
Tabel 2-1. Sub kunci enkripsi IDEA $K_i^{(t)}$.	16
Tabel 2-2. Sub kunci $K_i^{(t)}$ dekripsi.	16
Tabel 2-3. Permasalahan formal.	36
Tabel 4-1. Skenario Pengujian.	102
Tabel 4-2. Hasil Pengujian.	103
Tabel 4-3. Tabel Kode Huffman.	108
Tabel 4-4. Tabel Pengujian Metode Kompresi Terhadap Beberapa Jenis File.	111
Tabel 4-5. Pengujian Untuk Membentuk Kunci Enkripsi.	113

DAFTAR GAMBAR

	Halaman
Gambar 2.1. Model Enkripsi Shannon.	9
Gambar 2.2. Arsitektur DES.	10
Gambar 2.3. Enkripsi asimetris.	12
Gambar 2.4. Proses Putaran Enkripsi IDEA.	14
Gambar 2.5. Jalur Perhitungan IDEA.	14
Gambar 2.6. Transformasi Keluaran IDEA.	15
Gambar 2.7. Bitwise eXclusive OR.	17
Gambar 2.8. Tambahan Modulo 2^{16} .	18
Gambar 2.9. Blok perkalian modulo $2^{16}+1$.	18
Gambar 2.10. Penjadwalan kunci.	23
Gambar 2.11. Arsitektur Dasar IDEA.	23
Gambar 2.12. Satu Operasi MD5.	28
Gambar 2.13. Diagram Level Konteks.	48
Gambar 2.14. Diagram aliran data level 1 (DAD Level 1).	50
Gambar 2.15. DAD level 2 menunjukkan anak proses dalam sistem yang sama.	51
Gambar 3.1. Diagram Konteks.	56
Gambar 3.2. DAD Level 1.	57
Gambar 3.3. DAD Level 2 Proses Hash.	58
Gambar 3.4. DAD Level 2 Proses Kompresi.	59
Gambar 3.5. DAD Level 2 Proses Enkripsi.	60
Gambar 3.6. Flowchart Sistem Pemampatan dan Keamanan.	61
Gambar 3.7. Pesan dengan panjang bit kongruen 448, modulus 512.	63
Gambar 3.8. Pesan dengan panjang kelipatan 512.	64
Gambar 3.9. Proses MD5.	65
Gambar 3.10. Menu awal.	76
Gambar 3.11. Menu Layar dua.	77
Gambar 3.12. Menu layar tiga.	77
Gambar 4.1. Tampilan Menu Awal.	99
Gambar 4.2. Menu Awal dan Pesan Kesalahan.	99
Gambar 4.3. File Masukan dan Password.	100
Gambar 4.4. Tampilan akhir.	100
Gambar 4.5. Pengujian MD5 Aplikasi Yang Dibangun.	106
Gambar 4.6. Pengujian MD5 dengan WinMD5.	107
Gambar 4.7. File test 'yap.txt'.	109
Gambar 4.8. Besar File Test 'yap.txt'.	109
Gambar 4.9. File test 'yap.txt'.	109
Gambar 4.10. Perintah melakukan kompresi file 'yap.txt'.	110
Gambar 4.11. Besar File kompresi 'hh.jz'.	110
Gambar 4.12. Satu Siklus Penuh Hash, Kompresi dan Enkripsi.	111
Gambar 4.13. Dekripsi dengan password yang salah.	112
Gambar 4.14. Enkripsi dengan password yang benar.	113

DAFTAR KODE

	Halaman
Kode 3.1. Pseudocode MD5-1.	66
Kode 3.2. Pseudocode MD5-2	67
Kode 3.3. Pseudocode MD5-3.	67
Kode 3.4. Pseudocode MD5-4	68
Kode 3.5. Pseudocode MD5-5.	68
Kode 3.6. Pembentukan pohon HUFFMAN.	70
Kode 3.7. Fungsi pembentukan kode baru.	72
Kode 3.8. Fungsi pemberian kode baru.	72
Kode 3.9. Operasi perkalian modulo $2^{16}+1$.	75
Kode 4.1. Inisialisasi MD5.	79
Kode 4.2. Fungsi final MD5 bagian penambahan bit-bit penyangga.	79
Kode 4.3. Fungsi final MD5 bagian penambahan panjang pesan.	80
Kode 4.4. Pendefinisian empat transformasi putaran.	81
Kode 4.5. Putaran pertama transformasi.	81
Kode 4.6. Putaran kedua transformasi.	82
Kode 4.7. Putaran ketiga transformasi.	82
Kode 4.8. Putaran keempat transformasi.	83
Kode 4.9. Pembentukan Pohon HUFFMAN.	84
Kode 4.10. Pembentukan Kode Baru.	85
Kode 4.11. Pembentukan Kode Baru -2.	86
Kode 4.12. Pembentukan Kode Baru -3.	87
Kode 4.13. Pemberian Kode Baru.	88
Kode 4.14. Fungsi Encode File.	89
Kode 4.15. Fungsi Encode File-2.	90
Kode 4.16. Fungsi Encode File-3.	91
Kode 4.17. Fungsi Decode File.	92
Kode 4.18. Fungsi Decode File-2.	92
Kode 4.19. Fungsi Decode File-3.	93
Kode 4.20. Fungsi Decode File-4.	93
Kode 4.21. Fungsi Decode File-5.	94
Kode 4.22. Fungsi Decode File-6.	95
Kode 4.23. Fungsi enkripsi IDEA .	96
Kode 4.24. Fungsi enkripsi IDEA-2 .	97
Kode 4.25. Fungsi Inverse.	98

DAFTAR LAMPIRAN

Halaman

Lampiran A Kode Program MD5, HUFFMAN dan IDEA. **Error! Bookmark not defined.**