



### **Hak cipta dan penggunaan kembali:**

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

### **Copyright and reuse:**

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

# **Implementasi Digital Signature Untuk Aplikasi Kriptografi Pengaman Berkas Digital**



SKRIPSI

Diajukan Sebagai Salah Satu Syarat Memperoleh  
Gelar Sarjana Komputer (S.Kom.)

Kevin Malviyanto

09110210013

**JURUSAN SISTEM KOMPUTER  
FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI  
UNIVERSITAS MULTIMEDIA NUSANTARA  
TANGERANG  
2015**

**HALAMAN PENGESAHAN SKRIPSI**

**IMPLEMENTASI DIGITAL SIGNATURE UNTUK APLIKASI  
KRIPTOGRAFI BERKAS PENGAMAN DIGITAL**

Oleh  
Nama : Kevin Malviyanto  
NIM : 09110210013  
Program Studi : Sistem Komputer  
Fakultas : Teknologi Informasi dan Komunikasi

Gading Serpong, 26 Januari 2015

Mengetahui,

Dosen Pembimbing,

Ketua Program Studi  
Sistem Komputer,

Hargyo Tri Nugroho, S.Kom., M.Sc.

Kanisius Karyono, S.T., M.T.

UMMN

## PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya

Nama : Kevin Malviyanto

NIM : 09110210013

Program Studi : Sistem Komputer

Fakultas : Teknologi Informasi dan Komunikasi

menyatakan bahwa skripsi yang berjudul “Implementasi Digital Signature Untuk Aplikasi Kriptografi Pengaman Berkas Digital” adalah karya pribadi saya, bukan karya ilmiah yang ditulis oleh orang atau lembaga lain. Semua karya ilmiah orang atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumbernya serta dicantumkan dalam daftar pustaka.

Jakarta,

Kevin Malviyanto

UMMN

# IMPLEMENTASI DIGITAL SIGNATURE UNTUK APLIKASI KRIPTOGRAFI BERKAS PENGAMAN DIGITAL

## ABSTRAKSI

Seiring berkembangnya teknologi informasi, tidak lepas dari permasalahan keamanannya. Oleh karena itu, dikembangkan metode - metode kriptografi file yang digunakan sebelum file dikirimkan atau diberikan kepada orang yang dituju. Metode – metode kriptografi file yang dipakai dalam penelitian ini adalah SHA256, RSA, dan *twofish*. Penelitian ini membandingkan *throughput* dan konsumsi memori dari masing – masing metode. Pengujian dilakukan dengan menggunakan ukuran file yang berbeda – beda. Berdasarkan hasil penelitian didapatkan nilai dari *throughput* dari SHA256 lebih besar dibanding dengan nilai *throughput* RSA dan *twofish* namun *throughput* dari ketiga algoritma tidak optimal. *Throughput* ketiga algoritma tidak optimal karena adanya kemungkinan *memory fragmentation* yang besar.

Kata kunci : SHA256, RSA, *Twofish*, *Throughput*, *Memory fragmentation*.

# **IMPLEMENTATION OF DIGITAL SIGNATURE FOR CRYPTOGRAPHY DIGITAL FILE SECURITY APPLICATION**

## **ABSTRACT**

As the development of information technology, security issues can not be negligible. Therefore, cryptography methods have been developed and used before the file is sent or given to the intended person. Cryptography methods used in this research are SHA256, RSA, and Twofish. This research compares the throughput and memory consumption of each method. The testing is carried out by using different file sizes. Based on the experiment result, the throughput of the SHA256 value is greater than the value of throughput RSA and Twofish but the throughput value of the three algorithms are not optimal. Throughput of three algorithms are not optimal, because there are possibilities of huge memory fragmentation.

Keywords : SHA256, RSA, Twofish, Throughput, Memory fragmentation.

# UMN

## KATA PENGANTAR

Sungguh besar nikmat dan karunia yang diberikan oleh Tuhan Yang Maha Esa sehingga penulis dapat menyelesaikan penelitian yang berjudul “Implementasi Digital Signature Untuk Aplikasi Kriptografi Pengaman Berkas Digital” ini. Puji dan syukur kepada Tuhan Yang Maha Esa seakan tidak cukup untuk menggambarkan rasa terima kasih yang penulis rasakan dalam melakukan penelitian ini.

Penelitian ini dilakukan sebagai salah satu syarat memperoleh gelar Sarjana Komputer (S. Kom.) pada program Strata 1 (S-1) di Universitas Multimedia Nusantara.

Dalam proses penelitian ini tentunya penulis mendapatkan berbagai dukungan dan motivasi dari berbagai pihak. Untuk itu rasa terima kasih yang dalam penulis tujukan kepada

1. Orang tua dan keluarga yang tidak pernah berhenti untuk mendukung penulis dalam berbagai kondisi.
2. Hira Meidia, Ph.D., selaku Wakil Rektor Bidang Akademik dan Kemahasiswaan.
3. Hargyo Tri Nugroho Ignatius, S.Kom., M.Sc., selaku Dosen Pembimbing yang telah membimbing, memberikan masukan, dan nasihat dalam penelitian dan penulisan skripsi ini.
4. Kanisius Karyono, S.T., M.T., selaku Ketua Program Studi Sistem Komputer.
5. Teman – teman SK angkatan 2009 yang telah bersama – sama menjalani pendidikan di Universitas Multimedia Nusantara.

6. Teman – teman IT angkatan 2009 yang telah bersama – sama menjalani pendidikan di Universitas Multimedia Nusantara.
7. Teman – Teman dari HOTHY yang selalu mengingatkan dan menyemangati penulis.
8. Dosen-dosen yang telah berbagi ilmu dan pengalaman selama delapan semester yang telah dilalui.
9. Pihak-pihak lainnya yang tidak dapat penulis sebutkan satu per satu.

Akhir kata, dengan segala kerendahan hati penulis sadar masih terdapat banyak kekurangan. Penulis sangat mengharapkan adanya saran dan kritik membangun dari pembaca. Dan semoga skripsi ini bermanfaat bagi para pembaca, terutama para mahasiswa UMN dalam mengembangkan teknologi informasi dan komunikasi.

Jakarta, 26 Januari 2015

UMN



## DAFTAR ISI

HALAMAN PENGESAHAN SKRIPSI .....	i
PERNYATAAN TIDAK MELAKUKAN PLAGIAT .....	ii
ABSTRAKSI .....	iii
<i>ABSTRACT</i> .....	iv
KATA PENGANTAR.....	v
DAFTAR ISI .....	vii
DAFTAR GAMBAR .....	ix
DAFTAR TABEL.....	x
BAB I PENDAHULUAN .....	1
1.1. Latar Belakang.....	1
1.2. Perumusan Masalah .....	3
1.3. Pembatasan Masalah .....	3
1.4. Tujuan Penelitian.....	4
1.5. Manfaat Penelitian.....	4
1.6. Sistematika Penulisan.....	5
BAB II LANDASAN TEORI .....	7
2.1. Digital Signature .....	7
2.2. Rivest-Shamir-Adleman (RSA) .....	10
2.3. Secure Hashing Algorithm – 2 (SHA-2) .....	13
2.4. Symmetric Cryptography Twofish .....	16
BAB III METODOLOGI PENELITIAN.....	18
3.1. Metode Penelitian.....	18
3.2. Perancangan Sistem.....	20
3.2.1. Diagram Alir.....	20
3.3. Desain Antarmuka .....	48
3.3.1. Halaman Pembuka .....	48
3.3.2. Halaman Menu Utama .....	49
3.3.3. Halaman Penjelasan Tentang Aplikasi .....	52
3.3. Skenario Pengujian.....	53
BAB IV IMPLEMENTASI DAN EVALUASI.....	54
4.1. Spesifikasi Perangkat.....	54
4.2. Implementasi Sistem.....	54
4.2.1. Halaman Utama .....	55
4.2.2. Halaman Menu Enkripsi .....	57
4.2.3. Halaman Menu Dekripsi .....	61
4.2.4. Hasil About .....	67
4.3. Pengujian .....	68
4.3.1. Variable Pengujian .....	68
4.3.2. Hasil Pengujian .....	69
4.4. Analisa .....	75
BAB V KESIMPULAN DAN SARAN.....	80
5.1 Kesimpulan .....	80
5.2 Saran.....	81

DAFTAR PUSTAKA ..... 82

Lampiran A – Hasil *Throughput* SHA256 Proses Enkripsi

Lampiran B – Hasil *Throughput* RSA Proses Enkripsi

Lampiran C – Hasil *Throughput Twofish* Proses Enkripsi

Lampiran D – Hasil *Throughput Twofish* Proses Dekripsi

Lampiran E – Hasil *Throughput* RSA Proses Dekripsi

Riwayat Hidup

Formulir Konsultasi Skripsi



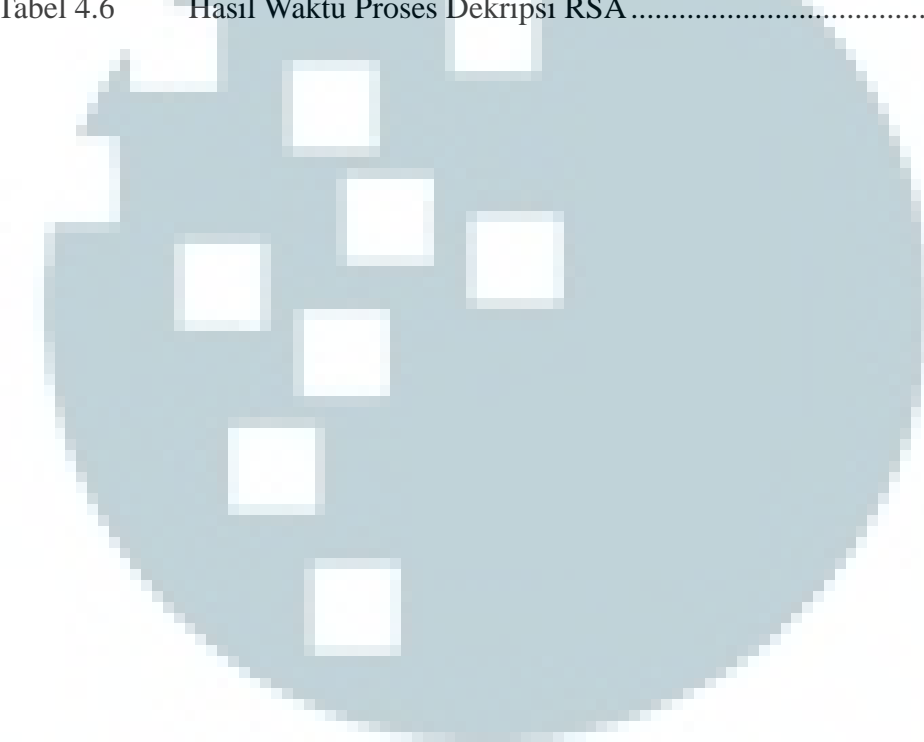
UMMN

## DAFTAR GAMBAR

Gambar 2.1	<i>Pseudocode RSA</i> .....	11
Gambar 2.2	<i>Six logical function 32-bit word</i> .....	13
Gambar 2.3	Algoritma <i>Twofish</i> .....	16
Gambar 3.1	Diagram Alir Menu Utama.....	20
Gambar 3.2	Diagram Alir Menu Enkripsi.....	22
Gambar 3.3	Diagram Alir Proses Pembangkit Kunci RSA ( <i>Generate Key Pairs RSA</i> ) Dan Diagram Alir Proses Enkripsi Algoritma RSA .....	24
Gambar 3.4	Diagram Alir Proses Enkripsi .....	26
Gambar 3.5	Diagram Alir Proses <i>Hashing</i> SHA256 .....	28
Gambar 3.6	Diagram Alir Inisialisasi Kunci Algoritma <i>Twofish</i> .....	30
Gambar 3.7	Diagram Alir Proses Enkripsi Berkas Algoritma <i>Twofish</i> .....	32
Gambar 3.8	Diagram Alir Proses Enkripsi <i>Twofish</i> .....	35
Gambar 3.9	Diagram Alir Menu Dekripsi .....	36
Gambar 3.10	Diagram Alir <i>Sub</i> Proses Dekripsi Dan Menu Verifikasi.....	38
Gambar 3.11	Diagram Alir <i>Sub</i> Proses Dekripsi Berkas Algoritma <i>Twofish</i> .....	40
Gambar 3.12	Diagram Alir Proses Dekripsi Algoritma <i>Twofish</i> .....	42
Gambar 3.13	Diagram Alir Proses Pengambilan Kunci Publik RSA Dan Proses Dekripsi Algoritma RSA .....	44
Gambar 3.14	Diagram Alir <i>Sub</i> Proses Verifikasi.....	45
Gambar 4.1	Halaman Utama.....	55
Gambar 4.2	Halaman Menu Enkripsi .....	56
Gambar 4.3	Hasil Pencatatan Proses <i>Generate Key</i> RSA.....	57
Gambar 4.4	Hasil Pencatatan Proses Enkripsi RSA .....	57
Gambar 4.5	Hasil Pencatatan Proses Enkripsi <i>Twofish</i> .....	58
Gambar 4.6	Persiapan Proses Enkripsi .....	59
Gambar 4.7	Proses Enkripsi Berhasil .....	60
Gambar 4.8	Halaman Menu Dekripsi Dan Verifikasi .....	61
Gambar 4.9	Hasil Pencatatan Proses Dekripsi <i>Twofish</i> .....	62
Gambar 4.10	Hasil Pencatatan Proses Dekripsi RSA .....	63
Gambar 4.11	Proses Dekripsi Berhasil .....	64
Gambar 4.12	Hasil Verifikasi Sama .....	66
Gambar 4.13	Hasil Verifikasi Tidak Sama .....	66
Gambar 4.14	Halaman <i>About</i> .....	67
Gambar 4.15	Perbandingan Waktu Proses <i>Hashing</i> Dan Enkripsi Ketiga Algoritma.....	75
Gambar 4.16	Hasil Pengujian Memori .....	78
Gambar 4.17	Konsumsi Memori <i>Classes With Source Code</i> .....	79

## DAFTAR TABEL

Tabel 4.1	Hasil Waktu Proses <i>Hashing</i> Algoritma SHA256.....	69
Tabel 4.2	Hasil Rata –Rata Waktu Proses <i>Hashing</i> SHA256 .....	70
Tabel 4.3	Hasil Waktu Proses Enkripsi Algoritma RSA .....	71
Tabel 4.4	Hasil Waktu Proses Enkripsi Algoritma <i>Twofish</i> .....	72
Tabel 4.5	Hasil Waktu Proses Dekripsi Algoritma <i>Twofish</i> .....	73
Tabel 4.6	Hasil Waktu Proses Dekripsi RSA.....	74



U M N