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,

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

Ketua Program Studi
Sistem Komputer,

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

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

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 expirement 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.

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 penulisak 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 HOTY 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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL