PENGUJIAN INTEGRITAS ISI FILE TEKS PADA OPERASI TANDA TANGAN DIGITAL DENGAN FUNGSI *HASH MD5* DAN KRIPTOGRAFI KUNCI-PUBLIK ALGORITMA *RSA*

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Infotmatika

Oleh:

Satriadinata
09021281621041

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN TUGAS AKHIR

Pengujian Integritas Isi File Teks pada Operasi Tanda Tangan Digital dengan Fungsi *hash MD5* dan Kriptografi Kunci-Publik Algoritma *RSA*

Oleh:

SATRIADINATA
NIM : 09021281621041

Palembang, Desember 2020

Pembimbing I.

Drs. Megah Mulya, M.T
NIP. 196602202006041001

Pembimbing II.

Muhammad Ali Buchari., M.T.
NIP. 198803302019031007

Mengetahui,
Ketua Jurusan Teknik Informatika,

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Jumat tanggal 20 November 2020 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama	:	Satriadinata
NIM	:	09021281621041
Judul	:	Pengujian Integritas Isi File Teks pada Operasi Tanda Tangan Digital dengan Fungsi *hash MD5* dan Kriptografi Kunci-Publik Algoritma *RSA*

1. Pembimbing I

   Drs. Megah Mulya, M.T .....
   NIP. 196602202006041001

2. Pembimbing II

   Muhammad Ali Buchari, M.T. .....
   NIP. 198803302019031007

3. Penguji I

   Alvi Syahrini Utami, M.Kom .....
   NIP. 197812222006042003

4. Penguji II

   Mastura Diana Marieska, S.T., M.T .....
   NIP. 19860321201803200l

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	:	Satriadinata
NIM	:	09021281621041
Program Studi	:	Teknik Informatika
Judul Skripsi	:	Pengujian Integritas Isi File Teks pada Operasi Tanda Tangan Digital dengan Fungsi *hash MD5* dan Kriptografi Kunci-Publik Algoritma *RSA*.

Hasil Pengecekan Software *iThenticate/Turnitin* : 18%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Desember 2020

Satriadinata
NIM. 09021281621041

MOTTO DAN PERSEMBAHAN

MOTTO:

“Balance in all things”
-Ember Spirit, Dota 2 –

"Jangan cari jawabannya tapi buatlah pilihan meskipun kau akan diumpat apa pun pilihanmu."

- Han ji Pyeong-

Kupersembahkan Karya Tulis ini kepada:

- **Keluargaku tercinta**
- **Orang-orang tersayangku**
- **Sahabat-sahabatku**
- **Fakultas Ilmu Komputer, Universitas Sriwijaya**

Text Files Integrity Test on Digital Signature Operation using MD5 Hash Function and RSA Public Key Cryptography Algorithm

By :
Satriadinata
09021281621041

ABSTRACT

Signatures have been used to prove the authentication of printed documents such as letters, certificates, diplomas, and so on for centuries. Signature is proof of authenticity of a document. This study aims to develop software and test the integrity of digitally signed messages using the MD5 hash function and RSA algorithm public key cryptography in a file with a .txt extension. This study used data in the form of text files consisting of 1000 words. The text file is given a digital signature with the developed software and then its integrity is tested by performing modification operations on the text file. In this research, a prototype software has been made to implement a document authentication scheme. From the results of experiments that have been carried out, it can be concluded that the MD5 hash function and the RSA algorithm public key cryptography can be implemented properly for digital signature operations.

Keywords: Digital Signature, MD5, RSA

Palembang, Desember 2020

Pembimbing I.

Drs. Megah Mulya, M.T
NIP. 196602202006041001

Pembimbing II.

Muhammad Ali Buchari, M.T.
NIP. 198803302019031007

Mengetahui,
Ketua Jurusan Teknik Informatika.

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Pengujian Integritas Isi File Teks pada Operasi Tanda Tangan Digital dengan Fungsi *hash MD5* dan Kriptografi Kunci-Publik Algoritma *RSA*

Oleh :
Satriadinata
NIM: 09021281621041

ABSTRAK

Tanda tangan telah digunakan untuk membuktikan otentikasi dokumen cetak seperti surat, piagam, ijazah, dan sebagainya selama berabad-abad lamanya. Tanda tangan merupakan bukti otentik sebuah dokumen. Penelitian ini bertujuan untuk mengmbangkan perangkat lunak dan menguji integritas pesan bertanda tangan digital dengan menggunakan fungsi hash MD5 dan Kriptografi kunci publik algoritma RSA pada file berekstensi .txt. Penelitian ini menggunakan data berupa file teks yang terdiri dari 1000 kata. File teks tersebut diberikan tanda tangan digital dengan perangkat lunak yang dikembangkan dan kemudian diuji integritasnya dengan melakukan operasi modifikasi terhadap file teks tersebut. Pada penelitian telah dibuat perangkat lunak prototype untuk menerapkan skema otentikasi dokumen. Dari hasil percobaan yang telah dilakukan, dapat disimpulkan jika fungsi hash MD5 dan kriptografi kunci publik algoritma RSA dapat diimplementasikan dengan baik untuk operasi tanda tangan digital.

Kata Kunci : Digital Signature, Tanda Tangan Digital, MD5, RSA

Palembang, Desember 2020

Pembimbing I.

Drs. Megah Mulya, M.T
NIP. 196602202006041001

Pembimbing II.

Muhammad Ali Buchari., M.T.
NIP. 198803302019031007

Mengetahui,
Ketua Jurusan Teknik Informatika.

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

KATA PENGANTAR

Puji syukur kepada Allah SWT atas berkat dan rahmat-Nya yang telah melimpahkan rahmat dan karunianya kepada Penulis sehingga mampu menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan Pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini, banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun tidak langsung. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih kepada:

1. Orang tuaku, Triono dan Tati Herlina, SS yang jasanya tiada tara dan tak akan dapat tergantikan. Adik perempuanku Siti Isyana Khairiya Dinata, serta seluruh keluarga besarku yang selalu mendoakan, menghibur, serta memberikan dukungan baik secara moril maupun materil.
2. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan ilmu, serta membimbing jalan penulis dalam menghadapi perkuliahan.
3. Pembimbing Tugas Akhir, Bapak Drs Megah Mulya, MT dan bapak Muhammad Ali Buchari, MT yang telah membimbing penulis dengan sabar dan semangat.

4. Penguji Tugas Akhir, Ibu Alvi Syahrini Utami, M.Kom dan ibu Mastura Diana Marieska, MT yang senantiasa memberikan masukan kepada penulis mengenai tugas akhir dan pengalaman kerja.
5. Pembimbing Akademik, Ibu Desty Rodiah, MT. yang telah banyak memberikan masukan kepada penulis mengenai perkuliahan.
6. Zahra Salsabila, Ade Fajri, Varian Dendisono, Zainudin yang telah menemani hari-hari perkuliahan dan perjuangan tugas akhir Bersama penulis.
7. Teman-teman perjuangan Tugas Akhir sekaligus nongkrongku Irfan, Adi ,Farid, Fadli, Luthfi, Ryadh, Daniel yang setia bersama penulis dalam perjuangan mengerjakan tugas akhir,

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan,oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat digunakan sebaik-baiknya serta bermanfaat bagi kita semua.

Palembang, Desember 2020

Penulis

Satriadinata

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini dibahas mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian serta batasan masalah. Bab ini akan memberikan penjelasan umum mengenai keseluruhan penelitian.

1.2 Latar Belakang

Tanda tangan telah digunakan untuk membuktikan otentikasi dokumen cetak seperti surat, piagam, ijazah, dan sebagainya selama berabad-abad lamanya. Tanda tangan merupakan bukti otentik sebuah dokumen. Surat yang tidak diberi tanda tangan umumnya diragukan kebenarannya. Berdasarkan artikel yang dikeluarkan oleh Kompas Jakarta, verifikasi pada dokumen digital akan sangat banyak terjadi di masyarakat. Salah satunya adalah tanda tangan digital. Tanda tangan dapat berguna sebagai bukti otentik bahwa kita telah membaca , memahami dan menyetujui isi sebuah dokumen (Munir, 2019).

Pada era digital seperti saat ini, kebanyakan pesan telah berbentuk data elektronis yang menyebabkan pemberian tanda tangan pada dokumen cetak tidak dapat dilakukan. Akan tetapi, fungsi tanda tangan pada dokumen cetak tetap dapat diterapkan untuk otentikasi pada pesan digital. Hal tersebut dapat dilakukan pada pesan yang ditransmisikan melalui saluran komunikasi maupun dokumen elektronik yang disimpan di dalam penyimpanan komputer. Suatu mekanisme

untuk menggantikan tanda tangan secara manual pada dokumen kertas ini disebut Tanda tangan digital (*digital signature*) (Sulaiman *et al.*, 2016).

Dokumen elektronik merupakan bagian dari layanan publik yang digunakan untuk mengganti dokumen kertas karena mereka memiliki karakteristik lebih fleksibel, pencarian lebih mudah, kemungkinan data yang hilang kecil, menghemat ruang, mengarsipkan secara digital, mentransfer dokumen lebih banyak dan mudah, serta meningkatkan keamanan dan mudah dalam pemulihan data. Namun, dokumen digital memerlukan penanda yang dapat menjamin keaslian seperti yang ada pada dokumen kertas. Tanda tangan digital adalah solusi yang dapat dilampirkan ke dokumen digital untuk menjaga keasliannya (Afrianto *et al.*, 2019).

Tanda tangan digital bukanlah tanda tangan yang digitalisasi dengan alat *scanner*, ataupun tanda tangan yang dibuat dengan menggunakan pena elektronik. Pada bidang kriptografi, tanda tangan digital adalah suatu nilai kriptografis yang bergantung pada isi pesan dan pengirim pesan. Pesan yang memiliki isi berbeda , meskipun dikirim dari pengirim yang sama akan menghasilkan tanda tangan digital yang berbeda. Tanda tangan yang mengacu kepada isi berkas dan pengirim berkas tentu berbeda dengan konsep tanda tangan pada dokumen kertas yang hanya bergantung pada pemberi tanda tangan dan selalu sama untuk semua dokumen. Walaupun memiliki konsep yang berbeda, tanda tangan digital memiliki tujuan yang sama seperti tanda tangan pada dokumen cetak, yaitu sebagai alat untuk otentikasi (Munir, 2019).

Banyaknya metode dalam menerapkan fungsi *hash* dan algoritma enkripsi, maka dipilihlah Algoritma MD5 untuk fungsi *hash* dan algoritma RSA untuk proses

enkripsi. MD5 merupakan salah satu jenis fungsi hash searah dimana hasil nya tidak dapat dikembalikan seperti semula. MD5 akan memberikan output berupa 128-bi*t message digest* dimana akan digunakan untuk proses otentikasi (Lekso Budi Handoko, Chaerul Umam, 2018).

Sedangkan algoritma RSA adalah salah satu algoritma kunci publik yang terpopuler. Salah satu kelebihan algoritma kunci publik adalah kombinasi kunci publik dan kunci privat tidak perlu diubah bahkan dalam jangka waktu yang panjang sekalipun. Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima *n* menjadi faktor primanya (Muchlis *et al.*, 2017).

Pada penelitian ini akan dilakukan operasi penyisipan tanda tangan digital dengan fungsi *hash* MD5 dan Kriptografi Kunci-Publik Algoritma RSA serta operasi pengujian integritas file teks yang telah diberikan tanda tangan digital dengan cara membandingkan nilai pesan setelah diberikan tanda tangan digital dan nilai pesan sebelum diberikan tanda tangan digital.

1.3 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah mengetahui bagaimana integritas isi file teks berformat .txt setelah diberikan tanda tangan digital dengan menggunakan fungsi h*ash* MD5 dan Kriptografi kunci publik Algoritma RSA.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengembangkan perangkat lunak yang mengimplementasikan fungsi *hash* MD5 dan Kriptografi Kunci-Publik Algoritma RSA pada operasi *digital signature* dan pengujian integritasnya.
2. Menguji integritas dengan membandingkan pesan sebelum dan sesudah disisipkannya tanda tangan digital menggunakan fungsi *Hash* MD5 dan Kriptografi kunci publik Algoritma RSA pada file berekstensi .txt.

1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Menghasilkan perangkat lunak yang dapat mengimplementasikan fungsi *hash* MD5 dan Kriptografi Kunci-Publik Algoritma RSA pada operasi *digital signature*.
2. Membuktikan keaslian isi file serta pengirim sehingga pengirim tidak dapat menyangkal jika telah mengirimkan sebuah dokumen. Hal tersebut membuktikan bahwa dokumen yang dikirim bersifat otentik dikirim dari pihak pengirim.

1.6 Batasan Masalah

Adapun batasan masalah yang diberikan pada penelitian ini adalah sebagai berikut:

1. Dokumen yang diberi tanda tangan digital hanya file teks berekstensi (*.txt*).

2. Pengamanan dokumen hanya meliputi otentikasi pengirim dan keutuhan file.

3. Tidak mencakup aspek keamanan pada jalur komunikasi pada proses transmisi dokumen.

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini mengikuti standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya yaitu sebagai berikut.:

BAB I. PENDAHULUAN

Pada bab ini akan diuraikan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, Batasan masalah/ruang lingkup, metodologi penelitian dan sistemarika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan membahas seluruh dasar-dasar teori yang digunakan mulai dari definisi sistem, informasi mengenai domain, dan semua yang digunakan pada tahapan analisis, perancangan, dan implementasi.

BAB III. METODELOGI PENELITIAN

Pada bab ini akan membahas mengenai tahap-tahap yang akan diterapkan pada penelitian. Setiap rencana dari tahapan penelitian dideskripsikan secara rinci berdasarkan kerangka kerja.

Dilanjutkan dengan perancangan manajemen proyek dalam pelaksanaan penelitian.

BAB IV PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini diuraikan tahapan yang dilakukan dalam proses pengembangan perangkat lunak untuk melakukan Pengujian Integritas Isi File Teks pada Operasi Tanda Tangan Digital dengan Fungsi *hash MD5* dan Kriptografi Kunci-Publik Algoritma *RSA*.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab ini menguraikan tentang hasil pengujian dan analisis hasil pengujian dari pengembangan perangkat lunak yang telah diuraikan pada bab IV.

BAB VI. KESIMPULAN DAN SARAN

Akan dipaparkan mengenai kesimpulan dan saran dari hasil dan analisis penelitian yang telah dilakukan pada bab V.

1.8 Kesimpulan

Dari pendahuluan ini, telah dijelaskan secara umum mengenai penelitian yang akan dilakukan, meliputi latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan.

DAFTAR PUSTAKA

Afrianto, I., Indonesia, U.K., Heryandi, A., Indonesia, U.K., Finandhita, A., Indonesia, U.K., Atin, S. & Indonesia, U.K. 2019. E-Document Autentification With Digital Signature For Smart City : Reference E-Document Autentification With Digital Signature For Smart City : Reference Model. (July).

Damara Ardy, R., Indriani, O.R., Sari, C.A., Setiadi, D.R.I.M. & Rachmawanto, E.H. 2018. Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5). Proceeding of 2017 International Conference on Smart Cities, Automation and Intelligent Computing Systems, ICON-SONICS 2017, 2018-Janua(November): 87–92.

Indriyono, B.V. 2016. Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher. Sisfo, 06(01): 1–16.

Lekso Budi Handoko, Chaerul Umam, C.A.S. 2018. Autentikasi Citra RGB Menggunakan Kombinasi Fungsi HASH MD5 dan … (Handoko dkk.). 28–33.

Muchlis, B.S., Budiman, M.A. & Rachmawati, D. 2017. Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik. SinkrOn, 2(2): 49–64. (http://jurnal.polgan.ac.id/index.php/sinkron/article/view/75).

Munir, R. 2019. KRIPTOGRAFI.

Pangaribuan, L.J. & Simbolon, F.H. 2017. Kriptografi Hybrida Menggunakan

Algoritma Hill Cipher Dan. I: 1–11.

Prasetiyo, B., Gernowo, R. & Noranita, B. 2015. Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data. Scientific Journal of Informatics, 1(1): 79–93.

Sulaiman, O.K., Ihwani, M. & Rizki, S.F. 2016. Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (Des) Algorithm. InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan), 1(1): 14–19.

Utami, E. 2007. Implementasi Steganografi Teknik Eof Dengan Gabungan Enkripsi Rijndael ,. 2007(November): 1–16.