Tanda Tangan Digital Menggunakan Algoritma MD5 dan Algoritma *Modified ElGamal Cryptosystem*

Diajukan Sebagai Syarat Untuk Menyelesaikan Pendidikan Program Strata-1
Pada Jurusan Teknik Informatika Fakultas Ilmu Komputer UNSRI

Oleh:

Muhammad Irsyad Masyhudin
09021181621030

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN TUGAS AKHIR

Tanda Tangan Digital Menggunakan Algoritma MD5
dan Algoritma *Modified ElGamal Cryptosystem*

Oleh:

MUHAMMAD IRSYAD MASYHUDIN
NIM: 09021181621030

Palembang, 05 Mei 2021

Pembimbing I

Dian Palupi Rini, M.Kom., Ph.D.
NIP. 197802232006042002

Pembimbing II

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Kamis tanggal 12 April 2021 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Muhammad Irsyad Masyhudin
NIM : 09021181621030
Judul : Tanda Tangan Digital Menggunakan Algoritma MD5 dan Algoritma *Modified ElGamal Cryptosystem*

1. Pembimbing I

   Dian Palupi Rini, M.Kom., Ph.D. ..... 
   NIP. 197802232006042002

2. Pembimbing II

   Mastura Diana Marieska, M.T. ..... 
   NIP. 198603212018032001

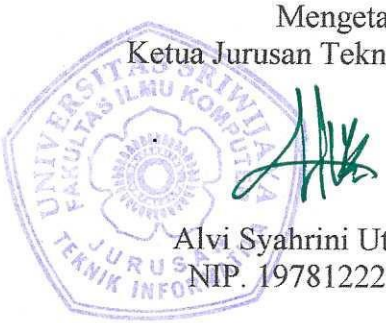
3. Penguji I

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

4. Penguji II

   Rizki Kurniati, S.Kom, MT ..... 
   NIP. 199107122019032016

Mengetahui,
Ketua Jurusan Teknik Informatika



Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Irsyad Masyhudin

NIM : 09021181621030

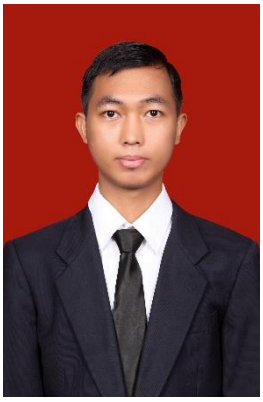
Program Studi : Teknik Informatika

Judul : Tanda Tangan Digital Menggunakan Algoritma MD5 dan Algoritma *Modified ElGamal Cryptosystem*

Hasil Pengecekan Software *iThenticate/Turnitin* : 11%

Menyatakan bahwa Laporan Proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan proyek 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, 19 Mei 2021

Muhammad Irsyad Masyhudin
NIM. 09021181621030

MOTTO DAN PERSEMBAHAN

"Do what you love and love what you do."

- Somebody -

"The first step to getting the things you want out of life is this:

Decide what you want."

- Ben Stein –

Kupersembahkan karya tulis ini kepada:

- ❖ Allah SWT
- ❖ Bapak dan Ibuku
- ❖ Saudaraku
- ❖ Keluarga besarku
- ❖ Dosen pembimbing dan penguji
- ❖ Kawan seperjuangan
- ❖ Fakultas ilmu komputer
- ❖ Universitas Sriwijaya

Digital Signature Using MD5
and Modified ElGamal Cryptosystem Algorithm

By

Muhammad Irsyad Masyhudin
09021181621030

ABSTRACT

Digitalization of files provides many advantages, especially for companies or organizations, but there are things that hinder the process of digitizing files, namely doubts about the originality of digital files because digital files are easy to manipulate. Digital signatures can be a solution to doubts about the originality of digital files. Digital signatures use hashing algorithms and cryptographic algorithms with two actors, one as the sender (signer) and the other as the receiver. This study is to determine whether the MD5 as a hashing algorithm and the Modified ElGamal Cryptosystem as a cryptographic algorithm can maintain the originality of digital files with many signatories. Tests were carried out on digital files with the extentions pdf, docx, and xlsx with the number of signers 10, 11, 20, 21, 30, 31, 40, 41, 50, 51, 99 and 100. Based on the results of tests performed showed 100% MD5 and Modified ElGamal Cryptosystem can recognize the original and modified files, so that the MD5 and Modified ElGamal Cryptosystem algorithm can maintain the originality of digital files.

keywords: Digital Signature, MD5, Modified ElGamal Cryptosystem

Palembang, 05 Mei 2021

Supervisor I

Dian Palupi Rini, M.Kom., Ph.D.
NIP. 197802232006042002

Supervisor II

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Approve,
Head of the Informatics Department

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Tanda Tangan Digital Menggunakan Algoritma MD5 dan Algoritma *Modified ElGamal Cryptosystem*

Oleh

Muhammad Irsyad Masyhudin
09021181621030

ABSTRAK

Digitalisasi pada berkas dokumen memberikan banyak keuntungan terutama pada perusahaan atau organisasi, tetapi ada hal yang menghambat dalam proses digitalisasi berkas dokumen yaitu keraguan terhadap keaslian berkas dokumen digital karena dokumen digital mudah untuk dimanipulasi. Tanda tangan digital dapat menjadi solusi dari keraguan keaslian berkas dokumen digital. Tanda tangan digital menggunakan algoritma *hashing* dan algoritma kriptografi dengan dua orang pelaku yaitu satu penanda tangan sekaligus pengirim dan satu orang sebagai penerima. Penelitian ini untuk mengetahui apakah algoritma MD5 sebagai algoritma *hashing* dan algoritma *Modified ElGamal Cryptosystem* sebagai algoritma kriptografi dapat menjaga keaslian berkas dokumen digital dengan banyak penanda tangan. Pengujian dilakukan pada berkas dokumen digital yang berekstensi pdf, docx, dan xlsx dengan jumlah penanda tangan 10, 11, 20, 21, 30, 31, 40, 41, 50, 51, 99 dan 100. Berdasarkan hasil pengujian yang dilakukan didapatkan hasil 100% algoritma MD5 dan algoritma *Modified ElGamal Cryptosystem* dapat mengenali berkas dokumen digital yang asli dan berkas dokumen digital yang sudah dimodifikasi sehingga algoritma MD5 dan algoritma *Modified ElGamal Cryptosystem* dapat menjaga keaslian berkas dokumen digital.

Kata kunci: Tanda Tangan Digital, MD5, *Modified ElGamal Cryptosystem*

Palembang, 05 Mei 2021

Pembimbing I

Dian Palupi Rini, M.Kom., Ph.D.
NIP. 197802232006042002

Pembimbing II

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

KATA PENGANTAR

Puji syukur kepada Allah SWT atas rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penelitian dan karya tulis ini yang berjudul Tanda Tangan Digital Menggunakan Algoritma MD5 dan Algoritma *Modified ElGamal Cryptosystem.* Penelitian dan karya tulis ini diciptakan untuk memenuhi salah satu sarat kelulusan dalam meraih derajat sarjana Komputer program Strata satu (S-1) Fakultas Ilmu Komputer Universitas Sriwijaya.

Selama proses penelitian dan pembuatan karya tulis ini, penulis mendapat beberapa masalah dan kendala, hal tersebut dapat teratasi dengan doa, bantuan serta dukungan dari banyak pihak. Penulis ingin menyampaikan rasa terima kasih kepada:

1. Kedua orang tuaku, Bapak Sunarno dan Ibu Yurmiati, serta saudaraku Ahmad Rosyidi Syahid dan Muhammad Ihsan Almuttaqin yang telah memberikan dukungan baik berupa moral dan material.
2. Rini Lestari, selaku orang spesial dalam kehidupan penulis yang mendukung dan memberikan motivasi kepada penulis dari awal masuk perkuliahan sampai selesai.
3. Jaidan Jauhari, M.T., selaku Dekan Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Alvi Syahrini Utami, M.Kom., selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya dan juga sebagai Penguji Skripsi Pertama yang memberikan komentar dan saran yang membantu.
5. Alm. Drs. Megah Mulya, M.T., selaku Pembimbing Skripsi Pertama yang banyak sekali membantu dan membimbing saya dari awal pembuatan sampai selesai bab terakhir skripsi ini.

6. Dian Palupi Rini, Ph.D., selaku Pembimbing Skripsi Pertama yang membantu saya melengkapi dan menyempurnakan skripsi ini.
7. Mastura Diana Marieska, M.T., selaku Pembimbing Skripsi Kedua yang banyak sekali membantu dan membimbing saya dari awal pembuatan skripsi sampai selesai.
8. Rizki Kurniati, S.Kom, M.T, selaku Penguji Skripsi Kedua yang memberikan masukan, saran, dan koreksi dalam pembuatan skripsi.
9. Pak Ricy dan seluruh staff fakultas yang telah membantu dalam proses administrasi dan akademik selama proses perkuliahan.
10. Bro Muhammad Irfan TP dan Moh. Sultan AU, Abdi Priyangga selaku kawan seperjuangna pencari receh selama perkuliahan dan juga sharing *slice of life*.
11. Bro Zikry Kurniawan, M. Ramadhandi SA, M. Edu A, Acmad Fadli A, Ahmad Ryad, Alif M., Daniel FR, M. Farid L, M. Shafrullah, Reyhan NSH, selaku Bro Inforgen Men yang bersama-sama berjuang melawan kerasnya skripsi.
12. Sis Kartika R BR Sitohang, Rifdah Yumna FM, Dwi Novitasari, dan Sis Inforgen Girl lainnya yang membantu penulis dalam perkuliahan.
13. Seluruh rekan Teknik Informatika Universitas Sriwijaya, yang telah membantu penulis semasa menjalani perkuliahan, baik secara langsung maupun tidak langsung.

Penulis menyadari karya yang dibuat manusia tidak ada yang sempurna, oleh karena itu kritik dan saran yang membangun sangat diharapkan agar karya tulis selanjutnya dapat menjadi lebih baik lagi. Akhir kata semoga karya tulis ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, Mei 2021

Muhammad Irsyad Masyhudin
NIM. 09021181621030

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1.1 Pendahuluan

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

Pendahuluan dimulai dengan penjelasan singkat tanda tangan digital. Selanjutnya dijelaskan masalah pada integritas *file* dengan banyak penanda tangan digital yang menjadi latar belakang masalah penelitian ini, serta algoritma MD5 dan *Modified ElGamal Cryptosystem* yang menjadi solusinya.

1.2 Latar Belakang Masalah

Pada masa sekarang ini, teknologi sudah berkembang dengan pesat terutama pada teknologi informasi dan komunikasi. Berkat berkembangnya kemampuan teknologi informasi dan komunikasi itu membuat orang-orang dapat berkomunikasi dengan mudah terutama melalui internet, dengan internet orang-orang dapat bertukar informasi baik berupa teks, suara, dan video.

Kemampuan teknologi informasi dan komunikasi yang sudah berkembang memungkinkan untuk digitalisasi pada surat menyurat atau berkas-berkas dokumen sebuah insitusi pemerintah maupun institusi swasta, dengan melakukan digitalisasi dapat membuat pekerjaan sebuah institusi menjadi lebih mudah dan efisien serta dapat menghemat penggunaan kertas *(Abraham et al., 2018)*.

Digitalisasi pada sebuah perusahaan atau instansi mengalami beberapa masalah seperti kepercayaan pada keaslian dokumen digital yang dibuat, apalagi pada dokumen yang bersifat rahasia atau penting, hal ini bertambah buruk jika dokumen tersebut dikirimkan melalui jaringan internet yang bersifat umum karena sulit memperkirakan apakah dokumen yang diterima adalah dokumen yang asli.

Menjaga integritas data sangat penting ketika data tersebut dikirimkan melalui jaringan internet. Data yang memiliki integritas yang bagus yaitu data yang tidak berubah dari pengirim sampai ke tangan penerima. Algoritma MD5 merupakan salah satu algoritma yang mengamankan integritas data. Algoritma MD5 bekerja dengan membangkitkan nilai *message digest* sebuah data digital dengan panjang *message digest* konstan yaitu 128 bit. Tingkat keamanan algoritma MD5 bergantung pada kombinasi 2^{128} sehingga sulit untuk mencari data yang berbeda isinya dan memiliki nilai *message digest* yang sama (Kasgar *et al.*, 2013).

Banyak cara untuk menjaga keaslian dokumen digital, salah satunya yaitu dengan menggunakan tanda tangan digital pada dokumen yang telah dibuat. Tanda tangan digital dapat menjaga keaslian isi dan melalukan validasi si pengirim sehingga dapat menjaga dokumennya. Selain itu, tanda tangan digital dapat menandai berbagai dokumen digital yang umum digunakan seperti *file* teks, suara, dan video (Hutasuhut *et al.*, 2019).

Tanda tangan digital menggunakan algoritma *hashing* untuk menghasilkan *message digest* dan algoritma kriptografi kunci publik untuk mengenkripsi *message digest*. Iqbal *et al.*, (2018) melakukan penelitian tentang tanda tangan

digital ini menggunakan algoritma MD5 sebagai pembangkit *message digest* dan algoritma kriptografi kunci publik elgamal. Penelitian ini menghasilkan laporan dari gabungan algoritma MD5 dan algoritma kriptografi kunci publik elgamal dapat menjaga keaslian *file* dan pengirim serta membutuhkan waktu yang lama untuk memodifikasi informasi yang dikirim.

Pada kasus tertentu sebuah dokumen membutuhkan lebih dari satu penanda tangan, sehingga Ordonez *et al.*, (2018) melakukan penelitian tanda tangan digital dengan banyak penanda tangan menggunakan algoritma kriptografi kunci publik elgamal yang dimodifikasi, hasil penelitian ini cukup memuaskan yaitu dilakukan percobaan dengan banyak penanda tangan sampai seratus penanda tangan dan tetap memliki waktu pemberian tanda tangan yang singkat.

Berdasarkan penelitian diatas, tanda tangan digital sangat diperlukan untuk menjaga keaslian dokumen digital, dengan itu penulis ingin melakukan penelitian tanda digital dengan algoritma MD5 untuk menghasilkan *message digest* karena memiliki panjang *message digest* yang konsisten yaitu 128 bit yang tepat untuk membangkitkan nilai *message digest* dari sebuah dokumen yang berukuran besar. Selain itu, peneliti juga akan menggunakan algoritma *Modified ElGamal Cryptosystem* yang dapat memuat banyak penanda tangan untuk tanda tangan digital, karena pada kasus tertentu sebuah dokumen memerlukan lebih dari satu penanda tangan.

1.3 Rumusan Masalah

Pertanyaan penelitian pada masalah ini adalah :

1. Bagaimana mengembangkan perangkat lunak tanda tangan digital dengan banyak tanda tangan menggunakan algoritma MD5 dan *Modified ElGamal Cryptosystem?*
2. Bagaimana menjaga keaslian dari file dengan banyak tanda tangan digital pada perangkat lunak tanda tangan digital menggunakan algoritma MD5 dan *Modified ElGamal Cryptosystem?*

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Mengembangkan perangkat lunak tanda tangan digital dengan banyak tanda tangan menggunakan algoritma MD5 dan *Modified ElGamal Cryptosystem.*
2. Mengetahui bagaimana keaslian *file* dokumen digital berekstensi pdf, docx, dan xlsx dengan membandingkan nilai *message digest* sebelum dan sesudah tanda tangan digital menggunakan algoritma MD5 dan *Modified ElGamal Cryptosystem*.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Hasil dari penelitian ini diharapkan dapat menunjang proses penerapan digitalisasi pada berkas dokumen di sebuah perusahaan atau instansi tanpa ada rasa keraguan dalam keaslian berkas dokumen.
2. Hasil dari penelitian dapat digunakan sebagai rujukan untuk penelitian-penelitian tanda tangan digital.

1.6 Batasan Masalah

Batasan masalah yang ditentukan pada penelitian ini adalah:

1. Dokumen digital yang digunakan untuk tanda tangan digital berupa *file* berekstensi pdf, docx, dan xlsx.
2. Tidak membahas sisi keamanan pada saat proses *key exchange* algoritma kriptografi kunci publik.
3. Tidak melihat proses pengiriman berkas dokumen digital.
4. Pengamanan dokumen digital hanya pada keaslian *file* dokumen yang meliputi isinya.

1.7 Sistematika Penulisan

Sistematika penulisan metodologi penelitian adalah sebagai berikut :

BAB I. PENDAHULUAN

Bab I menguraikan latar belakang dan rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika penulisan penelitian.

BAB II. KAJIAN LITERATUR

Bab II berisi landasan teori yang digunakan pada penelitian ini seperti algoritma MD5 dan algoritma *Modified ElGamal Cryptosystem*. Selain itu bab II juga membahas penelitian-penelitian lain yang relevan dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Bab III berisi pembahasan mengenai tahapan yang akan dilaksanakan pada penelitian ini. Rencana tahapan penelitian akan dideskripsikan dengan rinci dengan mengacu pada suatu kerangka kerja.

1.8 Kesimpulan

Pada bab ini telah dibahas latar belakang masalah penelitian ini dalam menjaga keaslian dokumen dengan tanda tangan digital. Karena itu, penelitian ini akan mengimplementasikan algoritma *Modified ElGamal Cryptosystem* dan algoritma MD5.

.

DAFTAR PUSTAKA

Basani, M.D. 2017. Jurnal perkembangan tanda tangan elektronik di indonesia. (November).

Bhandari, A., Bhuiyan, M. & Prasad, P.W.C. 2017. Enhancement of MD5 Algorithm for Secured Web Development. Journal of Software, 12(4): 240–252.

Hutasuhut, B.K., Efendi, S. & Situmorang, Z. 2019. Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA. 2: 5–10.

Iqbal, M., Siahaan, A.P.U. & Sundari, R.P. 2018. Combination of MD5 and ElGamal in Verifying *File* Authenticity and Improving Data Security. International Journal For Innovative Research in Multidisciplinary Field, 4(10): 96–101.

Karyanto, N.W. & Prasetya, N.I. 2005. Optimalisasi Enkripsi Untuk Proses Pengamanan Data Menggunakan Algoritma Vegenere. 43–48.

Kasgar, A.K., Dhariwal, M.K., Tantubay, N. & Malviya, H. 2013. A Review Paper of Message Digest 5 (MD5). International Journal of Modern Engineering & Management Research, 1(4): 29–35.

Martino, R. & Cilardo, A. 2020. SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey. IEEE Access, 8: 28415–28436.

Munir, R. 2019. KRIPTOGRAFI Edisi Kedua. bandung: Informatika.

Ordonez, A.J., Gerardo, B.D. & Medina, R.P. 2018. Digital signature with multiple signatories based on Modified ElGamal Cryptosystem. Proceedings of 2018 5th International Conference on Business and Industrial Research: Smart Technology for Next Generation of Information, Engineering, Business and Social Science, ICBIR 2018, 89–94.

Pabokory, F.N., Astuti, I.F. & Kridalaksana, A.H. 2016. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi *File* Dokumen, Dan *File* Dokumen Menggunakan Algoritma Advanced Encryption Standard. Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer, 10(1): 20.

Perangin-angin, R., Jaya, I.K., Rumahorbo, B. & Marpaung, B.J.R. 2019. Analisa Alokasi Memori dan Kecepatan Kriptograpi Simetris Dalam Enkripsi dan Dekripsi. 4(1).

Refialy, L., Sediyono, E. & Setiawan, A. 2015. Pengamanan Sertifikat Tanah Digital menggunakan Digital Signature SHA-512 dan RSA. Jurnal Teknik

Informatika dan Sistem Informasi, 1(3): 229–234.

Rivest, R. 2013. The MD5 Message-Digest Algoritm. 53(9): 1689–1699. (http://tools.ietf.org/pdf/rfc1321.pdf).

Saputra, R.A. & Purnomo, A.S. 2018. Implementasi Algoritma Schnorr Untuk Tanda Tangan Digital. JMAI (Jurnal Multimedia & Artificial Intelligence), 2(1): 21–26.

Yusmantoro, S., Hermansyah, E. & Efendi, R. 2014. Rancang Bangun Aplikasi Pengamanan Keaslian Surat Izin Tempat Usaha Menggunakan Algoritma Elgamal Dan Secure Hash Algorithm 256 Studi Kasus: Badan Pelayanan Perizinan Terpadu (Bppt) Kota Bengkulu. Jurnal Rekursif, 2(1): 28–36. (https://ejournal.unib.ac.id/index.php/rekursif/article/view/303).