Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 Pada Proses Legalisasi Ijazah

Fitri Nuraeni[1)], Yoga Handoko Agustin[2)], Irman Maulana Muharam[3)]
[1,2, 3]Teknik Informatika, TMIK Tasikmalaya
Jl. R.E. Martadinata No. 272 A Tasikmalaya, Telp. (0265) 310830
e-mail: [1]nufi3@stmik-tasikmalaya.ac.id , [2]abeogink@gmail.com , [3] irmanmuh@gmail.com

Abstrak

Ijazah adalah suatu dokumen pengakuan prestasi belajar dan penyelesaian suatu jenjang pendidikan yang diselenggarakan oleh perguruan tinggi, dimana dalam penggunaanya untuk suatu kepentingan, ijazah biasa dilampirkan dengan di fotocopy kemudian dilegalisasi oleh institusi pendidikan yang mengeluarkannya. Namun saat ini maraknya penggunaan file digital hasil scanning ijasah untuk berbagai keperluan memunculkan kehawatiran adanya perubahan data pada file ijazah tersebut sehingga memunculkan ijazah palsu. Dengan perkembangan sistem kriptografi terdapat fasilitas tanda tangan digital yang dapat memberikan layanan keamanan data berupa authentication dan integrasi data yang dapat menghilangkan kekhawatiran ijasah palsu. Tanda tangan digital ini dibangun dengan menerapkan fungsi hashing yaitu SHA-512 dan algoritma kriptografi asimetris RSA. Kedua algoritma tersebut memiliki keamanan yang handal untuk mendukung proses sign dan verify pada sistem tanda tangan digital yang dibangun dengan berbasis web. Dengan adanya sistem ini, perguruan tinggi dapat menerbitkan ijazah berserta tanda tangan digitalnya dan menyediakan fasilitas verify berbasis web yang dapat dimanfaatkan oleh pihak-pihak yang berkepentingan untuk mengecek keaslian file ijasah yang didapatnya dengan mudah dan cepat.

Kata kunci : *ijazah, rsa, tanda tangan digital, SHA-512*

1. Pendahuluan

Ijazah adalah suatu dokumen pengakuan prestasi belajar dan penyelesaian suatu jenjang pendidikan tinggi sesudah lulus ujian yang diselenggarakan oleh perguruan tinggi. Dalam penggunaanya untuk suatu kepentingan seperti melamar pekerjaan atau untuk mendapatkan pendidikan yang lebih tingi, ijazah biasa dilampirkan dengan *fotocopy* kemudian di legalisasi oleh institusi pendidikan yang mengeluarkannya. Banyak perguruan tinggi masih menggunakan stempel untuk melegalisasi ijazah, salah satunya adalah perguruan tinggi tempat penulis melakukan penelitian, cara tersebut masih memiliki kekurangan yang harusnya bisa antisipasi. Diantaranya: 1) belum cukup membuktikan bahwa ijazah yang dilampirkan benar-benar asli. Saat ini banyak sekali jasa pembuatan ijazah palsu yang dijalankan oleh suatu badan usaha atau perorangan. Ijazah palsu tersebut dibuat sangat mirip dengan aslinya sehingga sulit dibedakan; 2) jika seseorang ingin melegalisasi ijazah, sedangkan yang bersangkutan berada jauh dari institusi pendidikan yang mengeluarkan ijazahnya.

Saat ini, penggunaan ijasah sudah dalam bentuk file digital, khususnya untuk lampiran persyaratan pada sistem online baik melamar pekerjaan, pendaftaran studi atau pembaharuan data pegawai. Penggunaan file digital rentan dengan adanya perubahan data oleh pihak-pihak yang tidak bertanggung jawab sehingga memunculkan kekhawatiran adanya ijasah palsu. Oleh karena itu perlu adanya suatu fasilitas yang dapat memberikan layanan pengecekan keaslian dokumen dan kebenaran data pada dokumen tersebut dengan cepat dan mudah.

Sistem kriptografi bisa digunakan untuk mengatasi masalah keaslian suatu dokumen, dalam hal ini ijazah dan transkrip nilai. Salah satu teknik kriptografi yang dapat dimanfaatkan adalah tanda tangan digital (*digital signature*). Tanda tangan digital bukanlah tanda tangan dari seseorang yang di-scan atau dimasukkan ke komputer menggunakan scanner atau sejenisnya, tapi memiliki fungsi sebagai penanda data yang memastikan bahwa data tersebut adalah data yang sebenarnya. Tanda tangan digital merupakan salah satu cara dari kriptografi untuk autentifikasi dari sebuah pesan atau dokumen[1]. Tanda tangan digital sebenarnya adalah suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan[2], sehingga dengan adanya *digital signature*, otentikasi dan identitas penulis pesan secara konseptual dapat terjamin[3].

Pembuatan tanda tangan digital dimulai dengan proses mendapatkan ringkasan isi dokumen, kemudian ringkasan dienkripsi menggunakan algoritma kunci asimetris sehingga menghasilkan kode

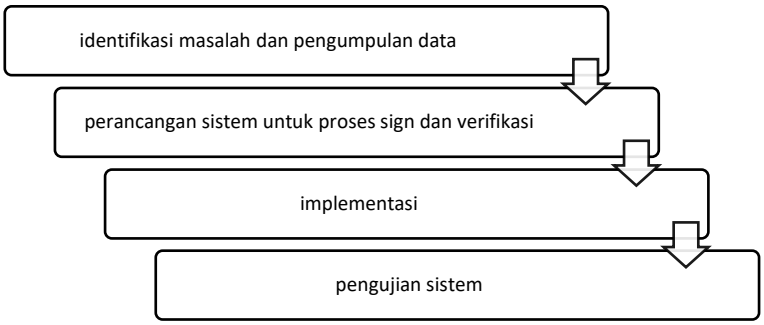
yang merupakan tanda tangan digital untuk dokumen tersebut, dan terakhir penyisipan tanda tangan digital ke dokumen.

Proses mendapatkan ringkasan isi dokumen dapat menggunakan fungsi hash, yaitu suatu fungsi satu arah yang menerima masukan pesan dengan panjang sembarang dan mengkonversinya menjadi kode pesan acak dengan panjang tetap yang disebut *message digest*. Salah satu fungsi hash yang terbukti aman adalah SHA-2 yang dapat menghasilkan output berukuran 512 bit atau SHA-512[4]. SHA-512 memiliki kehandalan antara lain[5]: 1)menghasilkan nilai hash terpanjang yaitu 512bit; 2) tahan serangan *birthday attack*;3) lebih cepat walaupun bukan fungsi hash paling cepat. Algoritma SHA bukan dibuat untuk *digital signature* dan tidak menggunakan kunci dalam penggunaanya sehingga keamanan data tidak terjamin atau bisa dirubah oleh pihak yang tidak memiliki wewenang. Sehingga akan lebih baik lagi jika dikombinasikan dengan algoritma kriptografi lainnya.

RSA merupakan algoritma kriptografi yang dapat digunakan untuk *digital signature* dimana algoritma ini termasuk kelompok kriptografi kunci asimetris, artinya mempunyai kunci berbeda untuk enkripsi dan dekripsi[6]. RSA memiliki 2 kunci yaitu kunci publik yang boleh diketahui oleh siapa saja dan kunci privat yang bersifat rahasia dan hanya diketahui oleh pihak-pihak tertentu saja[7]. Dengan penggunaan kunci yang berbeda untuk enkripsi dan dekripsi keamanan dan keaslian data lebih terjamin karena hanya orang yang mempunyai kunci saja yang bisa membuat dan merubah data *digital signature*.

2. Metode Penelitian

Dalam pembangunan sistem berbasis web yang mengimplementasikan tanda tangan digital ini digunakan metode pengembangan sistem waterfall yang terbagi dalam tahapan-tahapan seperti pada gambar 1, yaitu tahapan identifikasi masalah dan pegumpulan data, tahapan perancangan sistem untuk proses sign dan verifikasi dengan menggunakan algoritma SHA-512 dan algoritma RSA, tahapan implementasi dengan membuat website, dan terakhir tahapan pengujian sistem.



Gambar 1. Tahapan penelitian

2.1 Tahapan identifikasi masalah dan pengumpulan data

Untuk tahapan pengumpulan data dilakukan proses wawancara dengan staf akademik suatu perguruan tinggi kemudian melakukan observasi untuk mengamati proses penerbitan ijazah serta proses legalisasi ijazah yang ada. Kemudian dilakukan proses analisis untuk mengetahui kelemahan sistem yang berjalan dan kebutuhan dari sistem yang baru. Analisis yang dilakukan analisa PIECES (*Performance, Information, Economics, Control, Efiency, Service*) untuk menganalisis sistem lama dan didapatkan hasil seperti pada tabel 1.

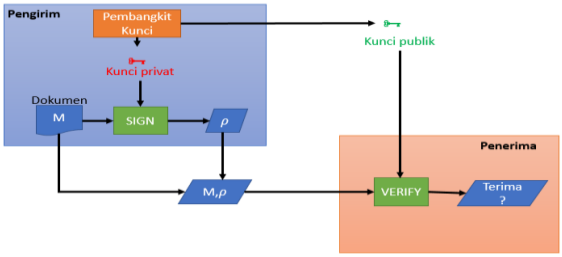
Tabel 1. Hasil analisis PIECES

	Sistem Berjalan	Kebutuhan
Performance	Proses legalisasi ijazah dan transkrip nilai yang saai ini berjalan masih lambat dan akan menghabiskan tenaga jika ijazah dan transkrip nilai yang akan dilegalisasi sangat banyak, karena diproses satu persatu.	Diusulkan : alumni bisa melegalisasi ijazahnya sendiri.

	Sistem Berjalan	Kebutuhan
Information	Susahnya membedakan mana ijazah palsu dan mana yang asli, hal tersebut akan merugikan beberapa pihak misalnya sebuah perusahaan menerima pelamar kerja dengan ijazah palsu atau menggunakan ijazah palsu untuk mendapatkan beasiswa. Sedangkan masalah bagi seseorang pemegang ijazah asli yang akan melegalisasi ijazah yaitu kurangnya informasi seperti kapan petugas libur atau kapan kantor tutup menyebabkan kerugian waktu dan materi bagi yang akan melegalisasi ijazah.	diusulkan : dibuatkan aplikasi untuk mengecek kelegalitasan ijazah dan transkrip nilai lewat dokumen legal-isasinya. Aplikasi untuk mengecek legal-isasi terdapat di website kampus sehingga bisa di-gunakan oleh siapa saja.
Economics	Membutuhkan banyak biaya bagi seseorang yang berdomisili jauh dari institusi pendidikan yang mengeluarkan ijazahnya untuk melagalisasi ijazah.	diusulkan : dengan menggunakan aplikasi melegalisasi ijazah tidak perlu datang ke kampus atau kantor BAAK. Sehingga tidak me-merlukan biaya per-alanan.
Control	Alat untuk melegalisasi tidak bisa dikontrol dalam hal ini stempel tidak bersifat rahasia, bisa saja seseorang membuat ulang stempel untuk memalsukan ijazah.	diusulkan : dengan legalisasi mengguna-kan digital signature alat disini berupa file kunci private dan publik yang akan sulit digandakan selama disimpan aman.
Eficiency	Proses legalisasi yang saat ini dilakukan kurang efisien, artinya akan memakan banyak waktu bagi seseorang yang ingin melegalisasi ijazahnya sedangkan yang bersangkutan berdomisili jauh dari institusi pendidikan yang mengeluarkan ijazahnya.	diusulkan : memperbarui legalisasi ijazah bisa dimana saja dan kapan saja.

2.2 Perancangan sistem

Perancangan sistem ini terbagi untuk 3 proses yaitu proses pembangkitan kunci publik dan privat, proses sign dan proses verifikasi dokumen. Perancangan tanda tangan digital ini tidak terlepas dari rangkaian langkah-langkah dalam algoritma SHA dan Algoritma RSA.



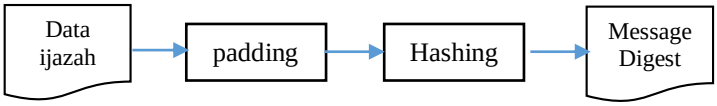
Gambar 2. Skema sistem tanda tangan digital pada legalisasi ijazah

Pembangkitan kunci publik dan privat menggunakan algoritma pembangkit kunci pada RSA. Berikut ini adalah proses pembentukan pasangan kunci dalam algoritma RSA[7]:

1) memilih 2 bilangan prima yaitu p dan q dimana nilai p tidak boleh sama dengan q;
2) menghitung nilai n = p.q (p ≠ q);
3) hitung $\varphi(n) = (p-1)(q-1)$;
4) memilih kunci publik e yang relatif prima terhadap (n);
5) membangkitkan kunci private d dengan persamaan $e.d \equiv 1(mod\ \varphi(n))$ dimana 1 < d < $\varphi(n)$;
6) didapatlah pasangan kunci yaitu:
   a. kunci publik (e,n);
   b. kunci privat (d,n).

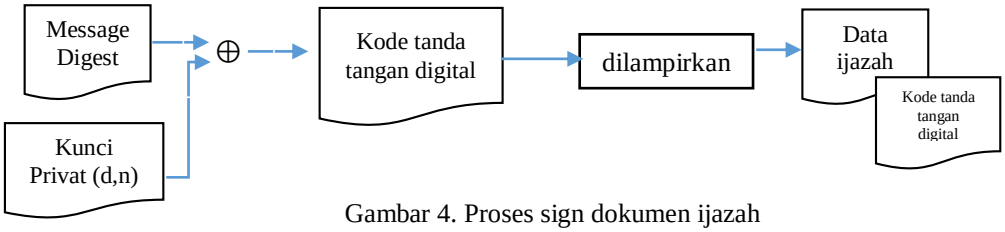
Untuk proses *sign* pertama-tama isi dokumen ijazah diinput pada sistem kemudian masuk pada proses hashing menggunakan metode SHA-512 menghasilkan message digest. Secara garis besar

pembuatan *message digest* ditempuh melalui empat langkah seperti pada gambar 2, yaitu proses padding, inisalisasi diggest awal, dan fungsi kompresi yang terdiri dari 80 round. Dari proses hashing ini dihasilkan suatu *message digest* sepanjang 512bit atau 64 byte.



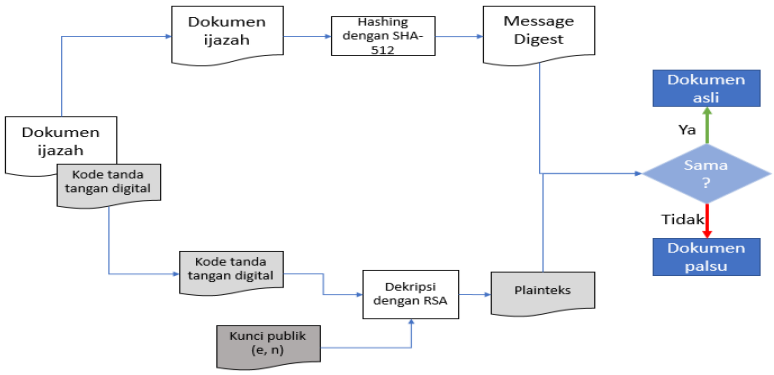
Gambar 3. Proses kerja SHA-512

Kemudian masuk tahapan enkripsi *message digest* hasil dari proses hashing(m) dengan kunci privat (d,n) yang dihasilkan dari algoritma RSA, yaitu $c_i = m_i^d mod\ n$. Susun hasil enkripsi sehingga diperoleh cipherteks dari *message digest* (m).



Gambar 4. Proses sign dokumen ijazah

Selanjutnya proses verifikasi dokumen ijazah yaitu proses mencocokan hasil dekripsi dari tanda tangan digital dengan *message digest* dokumen yang akan dicek seperti pada gambar 5. Dokumen yang akan dicek masuk proses hashing dengan SHA-512 sehingga didapat *message digest* (m'). Kemudian kode tanda tangan digital yang dilampirkan bersama dokumen ijazah didekripsi menggunakan kunci publik sehingga didapat plainteks (m). Jika plainteks (m) sama dengan *message digest* (m') maka dapat dipastikan dokumen tersebut asli dan tidak ada perubahan. Namun jika berbeda, maka dokumen ijazah tersebut sudah mengalami perubahan dan bukan dokumen yang asli.

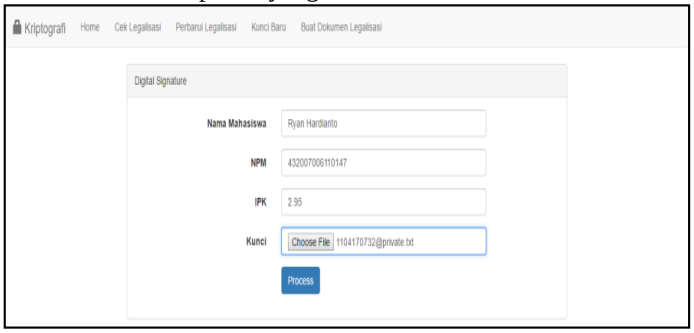


Gambar 5. Proses verifikasi dokumen ijazah

3. Hasil dan Pembahasan

Rancangan tanda tangan digital kemudian diwujudkan dalam suatu sistem berbasi web yang mempermudah proses sign dan verifikasi dokumen untuk selanjutnya. Pada awal pembangkitan kunci RSA dilakukan tiap periode yang dapat ditentukan oleh pengguna (penerbit ijazah) kemudian disimpan pada suatu file rahasia.

Saat akan menerbitkan ijazah, maka data isi ijazah tersebut diinput dalam sistem seperti pada gambar 6. Kemudian dimasukan kunci privat yang sudah dibuat kemudian tekan tombol proses.

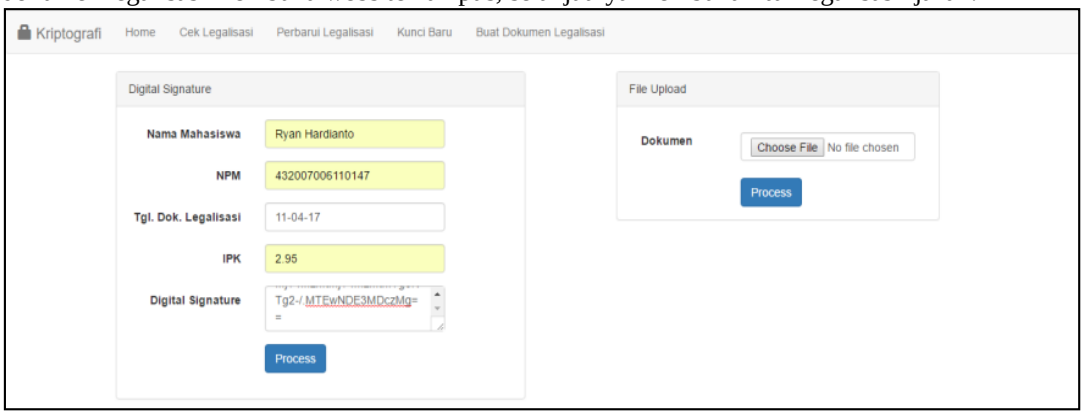


Gambar 6. Proses pembuatan dokumen tanda tangan digital

Gambar 7. Dokumen tanda tangan digital yang siap dilampirkan

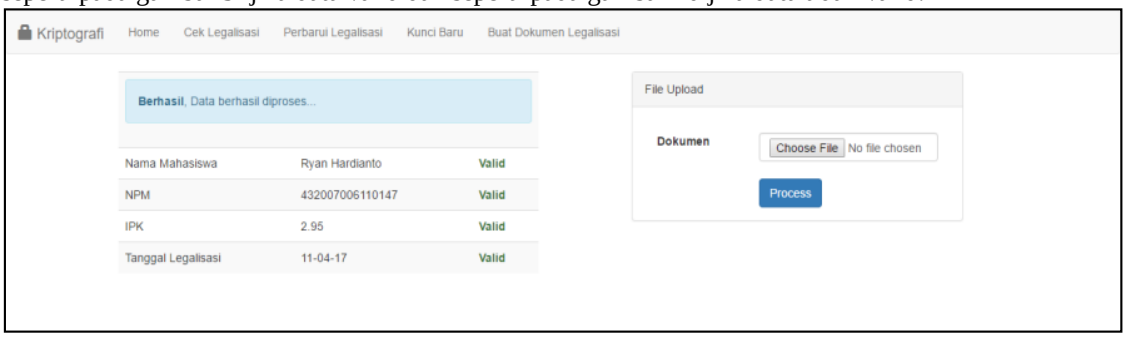
Hasil dari proses sign pada gambar 6 berupa kode tanda tangan digital yang siap untuk dilampirkan pada ijazah yang akan diberikan pada mahasiswa seperti pada gambar 7. Kode tanda tangan digital ini dapat disisipkan pada dokumen ijazah (*watermarking*) atau sekeda dicetak pada kertas yang dilampirkan bersama dokumen ijazah.

Sedangkan untuk proses verifikasi dokumen ijazah yang akan dicek keasliannya dilakukan pada form seperti gambar 8. Seorang alumni/ perusahaan (selanjutnya disebut pengguna) yang memiliki dokumen legalisasi membuka website kampus, selanjutnya membuka fitur legalisasi ijazah.

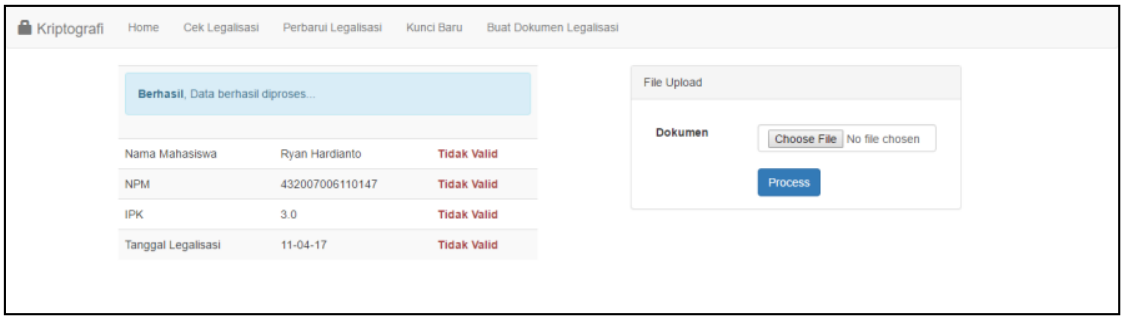


Gambar 8. Proses verifikasi dokumen ijazah

Pengguna akan menemukan form untuk mengecek keaslian dokumen legalisasi ijazah. Pengguna memasukan data-data yang terdapat pada dokumen legalisasi ijazah atau langsung memasukan file softcopy pada sistem. Sistem akan memberikan output berupa valid atau tidaknya dokumen tersebut seperti pada gambar 9 jika data valid dan seperti pada gambar 10 jika data tidak valid.



Gambar 9. Hasil verifikasi yang menghasilkan nilai valid



Gambar 10. Hasil verifikasi yang menghasilkan nilai tidak valid

4. Simpulan

Setelah mempelajari permasalahan yang dihadapi serta solusi pemecahan masalah yang diajukan, maka dapat ditarik kesimpulan diantaranya : 1) *Digital signature* dapat digunakan untuk mengamankan dokumen-dokumen penting dalam hal ini adalah ijazah dan transkrip nilai; 2) Dengan sistem yang baru pengecekan keaslian ijazah nilai dapat dilakukan dengan mudah tinggal mengakses web kampus saja; 3) Penerapan Algoritma RSA dan SHA-512 pada *digital signature* telah teruji aman, hal tersebut terbukti melalui proses pengujian dimana dilakukan modifikasi data pada dokumen legalisasi dan program berhasil mengetahuinya.

Untuk proses penelitian selanjutnya dapat diupayakan agar penyisipan atau pelampiran kode tanda tangan digital pada ijazah lebih mudah lagi dengan menggunakan steganografi atau watermarking. Hal tersebut juga akan mempermudah proses verifikasi dimana pengguna tidak perlu memasukan kode tanda tangan digital yang cukup banyak.

Daftar Pustaka

[1] D. P. Precilia dan A. Izzuddin, "Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5)," *Energy*, vol. 5, no. 1, hal. 14–19, 2016.

[2] M. Ray Rizaldy, "Perbandingan Tanda Tangan Digital RSA dan DSA Serta Implementasinya untuk Antisipasi Pembajakan Perangkat Lunak," Bandung, 2009.

[3] A. Yudo Husodo, "Penerapan Metode Digital Signature dalam Legalisasi Ijazah dan Transkrip Nilai Mahasiswa," Bandung, 2010.

[4] R. Leonardo, S. Eko, dan S. Adi, "Pengamanan Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan RSA," *J. Tek. Inform. dan Sist. Inf. Unversitas Kristen Satya Wacana*, vol. 1, hal. 229–234, 2015.

[5] M. Mulya, "PENGGUNAAN ALGORITMA SHA-512 UNTUK MENJAMIN INTEGRITAS DAN KEOTENTIKAN PESAN PADA INTRANET," in *Konferensi Nasional Sistem dan Informatika 2009*, 2009, no. 1, hal. 107–111.

[6] Z. Arifin, "Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman," *Inform. Mulawarman*, vol. 4, no. 3, hal. 7–14, 2009.

[7] R. Y. Rifai, Y. Christyono, dan I. Santoso, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIVEST CODE 4, RIVEST SHAMIR ADLEMAN, DAN METODE STEGANOGRAFI UNTUK PENGAMANAN PESAN RAHASIA PADA BERKAS TEKS DIGITAL," *TRANSIENT*, vol. 5, no. 1, hal. 87, 2016.