IMPLEMENTASI ALGORITMA EdDSA UNTUK PENGAMAN DOKUMEN DIGITAL ATAU SURAT BERHARGA

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

MA'RIFAH HADAINA FAZA

22.83.0842

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

IMPLEMENTASI ALGORITMA EdDSA UNTUK PENGAMAN DOKUMEN DIGITAL ATAU SURAT BERHARGA

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh

MA'RIFAH HADAINA FAZA

22.83.0842

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

IMPLEMENTASI ALGORITMA EdDSA UNTUK PENGAMAN DOKUMEN DIGITAL ATAU SURAT BERHARGA

yang disusun dan diajukan oleh

Ma'rifah Hadains Faza

22.83.0842

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 20 Februari 2026

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T.

NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA EdDSA SEBAGAI AUTENTIKASI DOKUMEN DIGITAL SURAT BERHARGA

yang disusun dan diajukan oleh
Ma'rifah Hadaina Faza
22.83.0842
Telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Februari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
1. **Melwin Syafrizal, S.Kom., M.Eng., Ph.D.** **NIK. 190302105**	
Joko Dwi Santoso, S.Kom., M.Kom. **NIK. 190302181**	
Jeki Kuswanto, S.Kom. M.Kom. **NIK. 190302456**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Februari 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ma'rifah Hadaina Faza
NIM : 22.83.0842

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI ALGORITMA EdDSA UNTUK PENGAMAN DOKUMEN DIGITAL ATAU SURAT BERHARGA

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Februari 2026
Yang Menyatakan,

Ma'rifah Hadaina Faza

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, karunia, dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang dengan baik dan tepat waktu. Dalam proses penyusunan skripsi ini, penulis menyadari bahwa tanpa bantuan, dukungan, dan bimbingan dari berbagai pihak, penelitian ini tidak akan dapat terselesaikan dengan baik. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih kepada:

1. Ibu Prof. Dr. Kusrini, M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM YOGYAKARTA.
2. Bapak Dr. Dony Ariyus, M.Kom selaku Ketua Program Studi Teknik Komputer.
3. Bapak Wahid Miftahul Ashari, S.Kom., M.T. selaku Dosen Pembimbing yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan bimbingan serta arahan selama penyusunan skripsi ini.
4. Seluruh dosen dan staf pengajar dilingkungan Program Studi Teknik Komputer yang telah memberikan ilmu pengetahuan kepada penulis selama perkuliahan.
5. Kedua orang tua tercinta, Bapak Wajidin dan Ibu Eko Trisnowati yang senantiasa memberikan doa, kasih sayang, serta dukungan moral dan materil yang tak terhingga.

Semoga skripsi ini dapat memberikan manfaat dan kontribusi bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan informasi dan kriptografi.

Yogyakarta, 20 Februari 2026
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

Perkembangan teknologi digital mendorong meningkatnya penggunaan dokumen digital di berbagai sektor, namun juga diikuti oleh ancaman terhadap keaslian dan integritas dokumen digital. Pemalsuan dan modifikasi dokumen bernilai hukum, seperti ijazah, kontrak, dan surat keputusan, menimbulkan risiko serius sehingga diperlukan mekanisme keamanan yang mampu menjamin autentikasi dan integritas dokumen secara kriptografis. Penelitian ini mengimplementasikan algoritma EdDSA khususnya Ed25519, sebagai metode autentikasi dokumen digital berformat .docx.

Sistem yang dikembangkan berupa aplikasi web berbasis Python dengan *framework* Django dan dijalankan pada sistem operasi macOS. Proses penandatanganan dilakukan dengan menghitung nilai hash dokumen menggunakan algoritma SHA-256, kemudian menghasilkan tanda tangan digital menggunakan Ed25519. Proses verifikasi dilakukan dengan mencocokkan tanda tangan digital terhadap nilai hash dokumen menggunakan kunci publik yang sesuai. *QR Code* dimanfaatkan sebagai media bantu untuk menampilkan dan mendistribusikan informasi autentikasi tanpa menggantikan proses verifikasi kriptografis utama.

Pengujian sistem dilakukan menggunakan metode black-box untuk memastikan fungsionalitas sistem berdasarkan input dan output. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi perubahan dokumen secara akurat, memverifikasi keaslian dokumen, serta membedakan dokumen yang valid dan tidak valid. Dengan demikian, penerapan algoritma EdDSA terbukti memberikan solusi autentikasi dokumen digital yang aman, efisien, dan andal, serta dapat digunakan sebagai alternatif praktis dalam menjaga keaslian dan integritas dokumen digital bernilai penting.

Kata kunci: EdDSA, Ed25519, Tanda Tangan Digital, Autentikasi Dokumen, Kriptografi

ABSTRACT

The rapid growth of digital technology has increased the use of electronic documents in various sectors, accompanied by rising threats to document authenticity and integrity. Digital document forgery and unauthorized modification pose serious risks, especially for valuable documents with legal significance. Therefore, a secure cryptographic mechanism is required to ensure document authenticity and integrity. This research implements the Edwards-curve Digital Signature Algorithm (EdDSA), specifically Ed25519, as a digital authentication method for electronic documents in .docx format.

The proposed system is developed as a web-based application using the Python programming language and the Django framework on the macOS platform. The system applies SHA-256 hashing to generate a document digest, which is then digitally signed using Ed25519. The verification process is performed by validating the digital signature against the document hash using the corresponding public key. QR Code is utilized as a supporting medium to present and distribute authentication information without replacing the cryptographic verification process.

System validation is conducted using black-box testing to evaluate functional correctness based on input and output behavior. The testing results demonstrate that the implemented system is able to accurately detect document modifications, verify digital signatures, and distinguish between valid and invalid documents. The implementation proves that EdDSA provides a secure, efficient, and reliable solution for digital document authentication. This system can be applied as a practical alternative for protecting the integrity and authenticity of valuable digital documents in electronic environments.

Keyword: *EdDSA, Ed25519, Digital Signature, Document Authentication, Cryptography*