BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital memudahkan penyimpanan, distribusi, dan verifikasi dokumen digital di berbagai sektor seperti pendidikan, kesehatan, pemerintahan, dan bisnis. Namun, kemajuan ini disertai meningkatnya ancaman siber terhadap keamanan dan keaslian dokumen digital. Cybersecurity Ventures (2024) mencatat kerugian global akibat kejahatan siber mencapai 9,5 triliun dolar AS per tahun [1], sementara BSSN menemukan lebih dari 150 juta anomali siber di Indonesia sepanjang 2023, termasuk pemalsuan sertifikat digital dan identitas elektronik [2]. Ancaman ini menimbulkan risiko serius terhadap keabsahan dokumen penting seperti ijazah, kontrak, dan surat keputusan yang memiliki nilai hukum.

Diperlukan mekanisme keamanan berbasis kriptografi yang mampu menjamin integritas dan autentikasi dokumen secara matematis. Salah satu pendekatan efektif adalah *Digital Signature Algorithm* atau DSA dan turunannya. Namun, karena kebutuhan efisiensi dan keamanan yang lebih tinggi, algoritma *Edwards curve Digital Signature Algorithm* atau EdDSA menjadi alternatif unggul dengan sifat deterministik, efisiensi tinggi, serta ketahanan terhadap serangan kunci privat.

Beberapa penelitian sebelumnya memang telah membahas penerapan EdDSA dalam konteks keamanan data, tetapi belum dapat digunakan secara langsung untuk menjamin integritas dan autentikasi dokumen digital pada sistem verifikasi elektronik. Penelitian ini bertujuan mengimplementasikan EdDSA pada dokumen digital serta menganalisis performa proses tanda tangan dan verifikasinya untuk menciptakan sistem autentikasi yang aman, sah, dan terpercaya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka permasalahan yang menjadi fokus dalam penelitian ini dapat dirumuskan yaitu, bagaimana

mengembangkan implementasi algoritma EdDSA pada tanda tangan dokumen digital?

1.3 Batasan Masalah

Agar penelitian ini terfokus dan tidak melebar dari tujuan utama, maka ditetapkan batasan masalah sebagai berikut:

1. Dokumen digital yang digunakan dalam penelitian terbatas pada format teks .docx dengan variasi ukuran bebas.
2. Web menggunakan bahasa pemrograman Python dan *framework* Django.
3. Pengujian dilakukan pada satu perangkat secara lokal dengan asumsi faktor eksternal dianggap konstan.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengimplementasikan algoritma EdDSA ke dalam sistem web. Melalui implementasi ini, sistem web yang dikembangkan telah mampu menghasilkan tanda tangan digital yang berfungsi untuk menjamin keaslian dan integritas dokumen digital berformat .docx. Selain itu, penelitian ini juga dilakukan untuk menguji proses verifikasi tanda tangan digital menggunakan algoritma EdDSA sehingga dapat memastikan bahwa setiap perubahan pada dokumen dapat terdeteksi secara akurat.

1.5 Manfaat Penelitian

Penelitian ini menghasilkan aplikasi web yang mampu melakukan proses penandatanganan dan verifikasi dokumen digital berformat .docx untuk menjamin keaslian dan integritas dokumen. Sistem yang dikembangkan dapat dimanfaatkan sebagai solusi alternatif autentikasi dokumen digital pada lingkungan pendidikan, administrasi, maupun organisasi yang membutuhkan validasi dokumen secara kriptografis tanpa bergantung pada otoritas sertifikasi eksternal. Selain itu, penelitian ini juga memberikan gambaran implementatif mengenai penggunaan EdDSA dan *hashing* dalam sistem nyata, sehingga dapat dijadikan acuan dalam pengembangan sistem keamanan dokumen digital di masa mendatang.

1.6 Sistematika Penulisan

Skripsi ini dirancang ke dalam beberapa bab dengan pokok permasalahan yang ditulis dengan susunan sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas latar belakang penelitian yang berkaitan dengan permasalahan keamanan, keaslian, dan integritas dokumen digital surat berharga. Selain itu, bab ini juga memuat rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan sebagai gambaran umum isi skripsi.

BAB II TINJAUAN PUSTAKA

Bab ini berisi kajian pustaka dan dasar teori yang mendukung penelitian. Pembahasan meliputi konsep kriptografi, fungsi hash, tanda tangan, algoritma EdDSA khususnya Ed25519, autentikasi dokumen digital, format dokumen .docx, serta penelitian-penelitian terdahulu yang relevan sebagai landasan teoritis penelitian.

BAB III METODE PENELITIAN

Bab ini menjelaskan metode penelitian yang digunakan dalam perancangan dan pengembangan sistem autentikasi dokumen digital. Pembahasan meliputi alur penelitian, perancangan sistem, desain antarmuka, implementasi algoritma EdDSA, teknologi yang digunakan, serta skenario pengujian sistem.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil implementasi sistem autentikasi dokumen digital berbasis algoritma EdDSA. Pembahasan meliputi implementasi antarmuka sistem, proses pembuatan dan verifikasi tanda tangan, serta analisis hasil pengujian sistem menggunakan metode black box untuk menilai keaslian dan integritas dokumen digital.

BAB V PENUTUP

Bab ini berisi kesimpulan yang diperoleh dari hasil penelitian serta saran yang dapat digunakan sebagai bahan pertimbangan untuk pengembangan sistem dan penelitian selanjutnya.