BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa algoritma EdDSA dengan varian Ed25519 berhasil diimplementasikan pada sistem autentikasi dokumen digital berbasis web. Sistem ini melakukan proses penandatanganan dokumen digital berformat .docx dengan terlebih dahulu membangkitkan nilai hash menggunakan algoritma SHA-256, kemudian menandatanganinya menggunakan kunci privat Ed25519. Hasil pengujian menunjukkan bahwa sistem mampu menjamin keaslian dan integritas dokumen digital, yang ditandai dengan keberhasilan proses verifikasi tanda tangan menggunakan kunci publik Ed25519 serta terdeteksinya setiap perubahan isi dokumen yang menyebabkan tanda tangan digitalmenjadi tidak valid. Pengujian fungsional menggunakan metode *black-box* juga menunjukkan bahwa fungsi sistem berjalan sesuai dengan kebutuhan fungsional yang telah ditetapkan dengan kurangnya kesempurnaan pada uji kode G-03. Dengan demikian, penerapan algoritma EdDSA dapat digunakan sebagai solusi autentikasi dokumen digital untuk memastikan keaslian dan integritas dokumen digital.

5.2 Saran

Berdasarkan hasil penelitian dan keterbatasan yang ada, maka saran untuk pengembangan selanjutnya adalah sebagai berikut:

1. Menyempurnakan validasi proses pembuatan tanda tangan kode G-03 sesuai dengan skenario agar pesan eror dapat ditampilkan.
2. Penelitian selanjutnya bisa menambah skenario pengujian untuk menyempurnakan web.
3. Sistem dapat dikembangkan agar mendukung format dokumen lain sehingga dapat digunakan pada lebih banyak jenis dokumen digital.
4. Penelitian selanjutnya dapat mempertimbangkan integrasi dengan CA atau PSrE guna meningkatkan aspek legalitas tanda tangan.
5. Pengujian keamanan lanjutan dapat dilakukan untuk menganalisis ketahanan sistem terhadap berbagai jenis serangan kriptografi.