

Abstrak

Tanda tangan digital merupakan sebuah alat kriptografi yang digunakan untuk menandatangani dan memverifikasi sebuah dokumen elektronik. Tanda tangan digital sudah banyak digunakan terutama sejak pandemi Corona Virus Disease 2019 (COVID-19) yang memaksa banyak orang untuk melakukan pekerjaan dari rumah sehingga harus melakukan pengiriman dokumen secara digital. Sudah banyak algoritma tanda tangan digital telah diusulkan sebelumnya, namun demikian algoritma yang paling sesuai untuk dokumen PDF dari segi keamanan dan *processing time* tanda tangan digital belum diketahui. Disamping hal tersebut, sistem layanan tanda tangan digital yang tersedia relatif mahal. Untuk mengatasi hal di atas, penelitian tugas akhir ini mengusulkan analisis algoritma tanda tangan digital dari segi keamanan, *processing time*, dan penggunaan memori pada dokumen PDF. penelitian ini juga mengusulkan pengembangan *prototype* yang menggunakan algoritma tanda tangan digital terbaik yang telah dianalisis sebelumnya sebagai *proof of concept* hasil analisis yang telah dibuat oleh penelitian ini. Metode yang digunakan dalam penelitian tugas akhir ini adalah 1. Studi literatur tentang algoritma tanda tangan digital, 2. Analisis algoritma tanda tangan digital, 3. Pengembangan *prototype*, 4. Pengujian performansi dan analisis. Hasil dari penelitian ini adalah DSA merupakan algoritma yang paling cocok untuk melakukan tanda tangan digital dibandingkan RSA dan ECDSA, karena DSA lebih unggul pada waktu proses tanda tangan dan verifikasi tanda tangan valid maupun invalid serta unggul pada penggunaan memori. Namun untuk keamanan dari algoritma, ketiga algoritma ini memiliki keamanan yang sama untuk mendeteksi perubahan konten pada sebuah dokumen PDF yang memiliki tanda tangan digital. Penelitian ini juga membuat *prototype* yang dapat melakukan tanda tangan digital pada dokumen PDF dan melakukan pengecekan tandatangandigital.

Kata Kunci: Tanda tangan digital, RSA, ECDSA, DSA, Dokumen PDF.