ABSTRAK

Digital Signature Algorithm (DSA) adalah metode kriptografi yang digunakan untuk memastikan integritas dan keaslian data dengan cara menghasilkan tandatangan digital yang unik untuk setiap dokumen. Dalam penelitian ini, penulis mengkaji langkah-langkah implementasi DSA, termasuk proses kunci publik dan privat, serta bagaimana tandatangan digital dapat digunakan untuk memverifikasi identitas pengirim dan mencegah pemalsuan. Hasil implementasi menunjukkan bahwa penggunaan DSA secara signifikan meningkatkan keamanan dokumen digital, memberikan perlindungan yang kuat terhadap manipulasi data. Temuan ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem keamanan informasi yang lebih efektif dan dapat diandalkan di era digital.

Kata Kunci: Kriptografi, Fungsi *Hash*, Kunci Asimetris, *Digital Signature Algorithm*, *Secure Hash Algorithm-256.*