ABSTRAK

Perkembangan teknologi dan ilmu pengetahuan dewasa ini sangat pesat. Data yang diterima menjadi suatu barang yang berharga. Oleh karena itu, perlu dilakukan pelindungan terhadap data yang didapat dengan berbagai cara. Perlindungan data dengan menggunakan tanda tangan yang melambangkan identitas pemilik. Tanda tangan ini dapat dipalsukan dan ditiru oleh orang lain.

Pemecahan dari maslah yang diatas adalah tanda tangan digital atau *Digital Signature*. *Digital Signature* bukan tanda tangan yang di-digitalisasi- kan tetapi merupakan bit-bit yang melambangkan identitas pemilik data tersebut. *Digital Signature* dihasilkan dengan menggunakan algoritma *Digital Signature Standard* yang diantaranya adalah *Digital Signature Algorithm* (DSA) dan *Rivest Shamir Adleman* (RSA) serta menggunakan fungsi *Hash* SHA-256 dan SHA-512. Pada penelitian dilakukan analisa performansi *Digital Signature* menggunakan *Digital Signature Algorithm* dan RSA. Analisa dilakukan dengan parameter waktu proses, distribusi frekuensi, *Brute Force Attack* dan Variansi.

Dari penelitian ini, diharapkan terdapat pengembangan *digital signature* dengan penggabungan fungsi *Hash* sehingga dapat digunakan untuk bit lebih besar, efisien dalam waktu proses, tahan terhadap *attacker*, dan dapat digunakan pada berbagai aplikasi.

Kata Kunci *: Digital Signature, Digital Signature Standard, Fungsi Hash*