Abstrak

Tugas akhir ini membahas tentang teknik *digital signature* sebagai salah satu solusi untuk melakukan verifikasi. Dengan adanya *digital signature* maka integritas data dan identitas pemilik data dapat dibuktikan. Algoritma yang digunakan pada tugas akhir ini adalah *Digital Signature Algorithm* (DSA) menggunakan *Secure Hash Algorithm* (SHA-1). Algoritma DSA terdiri dari tiga proses yaitu proses *generate* kunci dan proses *signing* yang diimplemetasikan pada aplikasi *client* serta proses *verifying* yang diimplementasikan pada aplikasi *server*. Tingkat performansi dari algoritma DSA dapat diketahui dengan mengetahui *avalanche effect*. Dari hasil analisis performansi didapatkan tingkat avalanche effect yang baik. Semakin baik tingkat avalanche effect yang diperoleh maka performansi algoritma DSA juga semakin baik.Tingkat keamanan pada *digital signature* yang dihasilkan dianalisa dengan menggunakan uji korelasi dan uji *chi-square*. Dari hasil pengujian dengan uji korelasi diperoleh tingkat korelasi yang lemah antara nilai hash dan tandatangan digital. Tingkat korelasi yang lemah ini menyebabkan tingkat keamanan digital signature yang dihasilkan baik. Sedangkan dengan uji *chi-square* diperoleh tingkat kerandoman dari digital signature yang baik. Semakin random digital signature yang dihasilkan maka semakin baik tingkat kemanannya

Kata kunci: *digital signature, DSA, signing, verifying*