Abstract

This final assignment implements digital signature technology as one solution to verify data. With digital signature, integrity data and the identity of the owner can be evidenced. Algorithm that used in this final assignment is Digital Signature Algorithm (DSA) using Secure Hash Algorithm (SHA-1). DSA algorithm consist of three components, generate signature and generate key that implemented in client side, while verify the signature implemented in server side. Performance rate of DSA can be known with its avalanche effect. The avalanche effect of DSA in this final assignment is having good rate. Good avalanche effect will caused performance of DSA performance as good well. The security rate is analysed using correlation test and chi-square . From correlation test, can be known that between input and ouput has weak correlation. This weak correlation caused the security of digital signature is good. While chi-square is a test to know the randomness of digtal signature. if it's more random than the security is better.

Key Word: *digital signature, DSA, signing, verifying*