Abstrak

Tandatangan digital pada umumnya menggunakan tipe kunci asimetrik yaitu pasangan kunci yang berbeda. Penentuan pasangan kunci diperoleh melalui tahapan algoritma yang panjang. Pada tugas akhir ini akan dibahas proses penandatanganan digital menggunakan metode Digital Signature Algorithm (DSA) dan Elliptic Curve Digital Signature Algorithm (ECDSA). Kedua metode tersebut beranalogi satu sama lain. DSA lebih menekankan pada tingkat kesulitan faktorisasi integer dan logaritma diskrit, sedangkan pada ECDSA selain kedua skematik tsb juga menekankan pada kesulitan penentuan nilai pada kurva ellips. Dengan kata lain kedua metode tsb memiliki domain yang berbeda. Kekuatan penting dalam tandatangan digital terletak pada tingkat keamanannya. Tingkat keamanan metode akan dianalisa melalui uji korelasi dan kompleksitas proses algoritma *cracking* yang pernah ada. Uji korelasi adalah pengujian untuk melihat tingkat keterhubungan antara dua nilai yang berbeda. Uji korelasi dilakukan terhadap nilai bit tandatangan dengan sidik jari pesan yang dihasilkan oleh fungsi *hash*. Keamanan juga akan dianalisa dengan kompleksitas waktu algoritma *cracking* yang pernah ada untuk memecahkan metode DSA dan ECDSA. Perbandingan kecepatan metode dianalisa pada saat proses penandatanganan dan verifikasi pesan.

Kata kunci: Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), uji korelasi, *cracking*, Faktorisasi integer, logaritma diskrit, kurva ellips.