Abstract

Digital signatures are commonly implemented through the use of asymmetric keys, which is a pair of non identical 'keys'. The formulation of these 'key pairs' is done through long (mathematical) algorithms. In this final assignment we will discuss about digital signing process using the Digital Signature Algorithm(DSA) method and Elliptic Curve Digital Signature Algorithm(ECDSA) method. Both of those methods mentioned above are paralled to each other. Process in aquiring each points has different steps, therefore the quality of the points is different. DSA puts more emphasize on rigid integer factorization and discrete logarithm,while ECDSA applies point determination on elliptical curve in addition to those two schematic mentioned above. In other words, those two methods have a different domain. The important point on digital signature lies on its security level. This security level would be analyze through corelation test. Corelation test's objective is to determine link between two different points. Corelation test done against signature bit point and using fingerprint value that computed by hash function. Security level will also be analyzed by time complexity algorithm cracking DSA method and ECDSA method have been ever.
Comparison speed of metode would be analyze throuh assignment signature and verification signature.

Key words: Digital Signature Algorithm(DSA), Elliptic Curve Digital Signature Algorithm(ECDSA), Corelation test, cracking, Integer factorization, Discrete logarithm, Elliptical curve.