Abstract

A digital signature is a cryptographic tool used to sign and verify an electronic document. Digital signatures have been widely used, especially since the Corona Virus Disease 2019 (COVID-19) pandemic forced many people to do work from home, so they had to send documents digitally. Many digital signature algorithms have been proposed before, however, the most suitable algorithm for PDF documents from the point of view of security and digital signature processing time is unknown. Apart from this, the available digital signature service systems are relatively expensive. To overcome the above, this final project research proposes an analysis of digital signature algorithms in terms of security, processing time, and memory usage in PDF documents. This study also proposes the development of a prototype that uses the best digital signature algorithm that has been previously analyzed as a proof of concept from the analysis made by this study. The methods used in this final project research are 1. Literature study on digital signature algorithms, 2. Digital signature algorithm analysis, 3. Development of prototype, 4. Performance testing and analysis. The results of this study are that DSA is the most suitable algorithm for performing digital signatures compared to RSA and ECDSA because DSA is superior in signature processing time and valid or invalid signature verification and superior in memory usage. However, for the security of the algorithms, these three algorithms have the same security for detecting content changes in a PDF document that has a digital signature. This research also makes a prototype that can digitally sign PDF documents and check digitalsignatures.

Keywords: Digital Signature, RSA, ECDSA, DSA, PDF Document.