Abstract

MMS (Multimedia Messaging Service) messaging is a communication service that has been set by the WAP and 3GPP standards. In the MMS security seemed to be a very important along with the development in this technology. Users who want to communicate not just looking for privacy just in terms of communicating, but the authenticity of the message also becomes a matter of equal importance in terms of communicating. Because of this requirement, the provision of applications that require the existence of a message encryption and digital signature.

One solution for maintaining data authenticity, data integrity, authentication and non-denial is to combine encryption algorithms and digital signatures. Encryption algorithm used is the Rijndael algorithm, while the digital signature algorithm it uses ECDSA. The result of encryption of messages generated by the Rijndael algorithm will be combined with the signature produced by the ECDSA signature algorithm and will be delivered through communication channels. merging algorithm produces confidentiality, data integrity, authentication, and non-repudiation.

ECDSA and Rijndael algorithm can be used in the MMS who have limited hardware resources such as mobile phones. From the experiments we can conclude that the performance of a merger between the ECDSA signature algorithm and an encryption algorithm Rijndael key length is influenced by the algorithm.

Keywords: MMS, Rijndael, ECDSA, hash functions, message digest, digital signature