Abstract

SMS (*Short Messaging Service*) is messaging delivery service in mobile communications environment. In delivering of message with SMS, messages security is very important. Messages which is saved, not only at the time of messages will be dilivered, but also how messages at the time of delivered are not changed by someone so that messages stills original. To solve this problem needed by digital signature.

One of way to make message digital signature is uses hash function. Digital signature forming is count message digest from message with using oneway hash function. Then message digest is encrypted with public key cryptography algorithm. Digital signature which is formed placed to the message, then both are delivered by communication channel. One of public keycryptography algorithm which is often used for digital signature forming is ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm. While one way hash function which is often used is SHA(Secure Hash Algorithm).

ECDSA is most suitable algorithm to be implentated in SMS which is use mobile device that has limited resource. It is becouse ECDSA relatively has smaller key then other public key cryptography.

From the experiment,ECDSA performance in SMS security is affeceted by the size of the key that used in *signing* and *verifying*. SHA algorithm that used in ECDSA is not giving some effect.

Keywords : SMS, ECDSA, *hash* function, message digest, *digital signature*