Abstract

MMS (*Multimedia Messaging Service*) is messaging delivery service in mobile communications environment with standard specified by forum WAP and 3GPP. In delivering of message with MMS, 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 one-way 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 key cryptography algorithm which is often used for digital signature forming is RSA algorithm. While one-way hash function which is often used is SHA(Secure Hash Algorithm).

From the result of experience, RSA algorithm is one of suitable algorithm to be used in making digital signature for delivery MMS message. Because digital signature size measure addition in MMS message is minimized (64-140 byte), so it is not influence delivery charge of MMS message

Keywords : MMS, RSA, *hash* function, message digest, *digital signature*