Abstract

This final assignment does mechanism for convincing that SMS receiver receive SMS from the real SMS sender by implementing digital signature in sending and receiving SMS using RSA algorithm and MD5 hash function. Digital signature comprises security aspect such as non-repudiation that makes SMS sender can't deny that he has sent SMS, authentication that convinces SMS receiver about SMS sender identity, and data integrity that declare about message originality.

This final assignment made an application for generating digital signature using RSA algorithm and MD5 hash function in SMS sending. Technology that is used for developing application is J2ME. The goals of digital signature usage on SMS application is to convince sender authentication, keep data integrity, and prevent denial from sender.

This final assignment does testing about generating and verificating digital signature. The result of testing is that the increment of key bit length causes exponentially increment of digital signature generation and verification time. The increment of key bit length also causes the increment of size of signature generated.

Keywords: SMS, digital signature, RSA algorithm, MD5 hash function, digital signature generation and verificaton time, size of signature.