ABSTRACT

YAZRI HAFIZ. The Development of Digital Signature Application for SMS Using MD5-RSA Algorithm. Supervised by HENDRA RAHMAWAN.

Cellular phone is one of the most popular communication device. Unfortunately, this popularity also increases number of crime using cellular phone. SMS fraud is one kind of crime using cellular phone. Another method of sender verification is required to avoid this kind of crime.

Digital signatures can be used to verify the sender. The sender is sending SMS with digital signature and the receiver will verify the signature. This application is developed using J2ME and MD5-RSA algorithm as the signature method. This application also uses Bouncy Castle lightweight cryptography API for J2ME as cryptography library.

Key pair parameters can be generated in 15 seconds to 4 minutes depends on the cellular phone technology. The digital signature can be formed with an average time of 1.35 seconds to 1.97 seconds. Digital signature verification can be done with an average time of 3.73 seconds to 12.09 seconds. The digital signature is generated using private key parameters and verified using public key parameters. Only the correct key pair will provide a valid result. Time to send signed-SMS depends on the network capability. There is no difference compared to sending normal SMS.

Keywords: Bouncy Castle, Digital signature, J2ME, MD5-RSA, SMS