DIGITAL SIGNATURE ON SMS USING ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

Name : YOHANES KHOSIAWAN
NRP  : 5107 100 105
Major : Informatics Engineering, IT Department-ITS
Supervisor I : Yudhi Purwananto, S.Kom, M.Kom
Supervisor II : Baskoro Adi Pratomo, S.Kom

Abstract

In this growing mobile technologies era, SMS has become a common communication media for all levels of society. Not only for sending greetings, but SMS is also used for sending important message, where some modifications to the SMS content or the sender’s identity information could harm some innocent parties. This background is underlying the implementation of the digital signature on SMS. By using proper method, the data integrity and the sender’s identity couldn’t be compromised anymore.

This mobile application is made to be able to run on an Android mobile device version 2.2 and above. The digital signature algorithm used is Elliptic Curve Digital Signature Algorithm (ECDSA). This application guarantees the SMS content and the sender’s identity are valid. This is done by padding the SMS content with the signature information. However, this method would decrease the maximum length (of characters) available to compose a message itself. The SMS verification would need a key which could be downloaded from the key server via internet connection. The protocol and the SMS transmission still work normally, so this application could work on any mobile device with Android 2.2 (Froyo) operating system and above using any cellular provider.

Various testing has been conducted on this research with satisfying results. The experiment results show a reliable SMS
content verification process and fast signature generation. The time needed for generating a signature in Signed-SMS is 0.6686 second at the average, which is clearly almost similar to time needed for generating a Normal SMS (without signature). Therefore, the ECDSA technique is an excellent choice to implement digital signature for SMS.

Keyword: SMS, digital signature, Android, ECDSA