Abstract

Short Message Service (SMS) message is communication mechanism that is still widely used, because it is still considered cheap, fast, and simple. When confidential information is exchange using SMS, it is important to protect secrecy and integrity of the message, as well as ensure that message is sent and received by authorized user. One commonly used technique to provide security is encryption. There are many encryption scheme that have been implemented on SMS, such as hybrid encryption scheme, which is combining symmetric and asymmetric scheme. One of the implementation is using AES and Elliptic Curve Diffie-Hellman (ECDH). But as we all know, the Diffie-Hellman protocol does not provide authentication of the communicating parties which means that Man-In-The-Middle attack is possible. Third party server is the most widely used to provide authentication. This research aims to propose an alternative solution that provide an end-to-end security that guarantees confidentiality, integrity, authentication, and non-repudiation security services that needed to secure SMS. The proposed solution is expected to solve the problem without any additional hardware or any negative effects on mobile phone device performance. On this research have been designed and implemented peer-to-peer hybrid encryption scheme, which provide security services confidentiality, integrity, authentication, and non-repudiation, by using the combination of Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve Digital Signature (ECDSA) and AES. ECDSA is used to solve the key exchange authentication problem. According to the functionality testing, designed system has successfully implemented on the android operating system. According to performance testing on 218 plaintext characters, the encryption execution time is 5.57 ms, the decryption execution time is 2.45 ms and the length of ciphertext is 333 characters. This SMS encryption system can provide quite fast computing time, but the results are long ciphertext.

Keywords: ECDH, ECDSA, AES, encryption, SMS, Android