Abstract

Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation. Short Message Service (SMS) is the text communication service component of mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between mobile phone devices. SMS framework allows two peers to exchange encrypted and digitally signed SMS messages. The communication between peers is secured by using public key cryptography. The identity validation of the contacts involved in the communication is
implemented through ECDSA signature scheme. In the next part, there is the description of ECDSA approach and a modified approach based on ECDSA for mobile phones, which signs SMS. At the end, there is described attack on ECDSA for secured SMS and future extension of the application.

Reference


15. Sattar J Aboud, Mohammad A AL-Fayoumi1, Mustafa Al-Fayoumi and Haidar S Jabbar “An Efficient RSA Public Key Encryption Scheme” Fifth International Conference on Information Technology: New Generations, 2002 IEEE.

16. "A Performance Comparison of Data Encryption Algorithms," IEEE Information and


Index Terms

Computer Science
Communications

Key words

GSM
SMS security
ECDSA

ECDLP
public key cryptography