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**

   International Conference on Wireless and Mobile Communications, 2010@IEEE, pp. 448-452.
2. Alfredo De Santis, Aniello Castiglione and Umberto Ferraro Petrillo “An Extensible
   Framework for Efficient Secure SMS” International Conference on Complex, Intelligent and
   Software Intensive Systems, 2010@IEEE, pp. 843-850.
   Governmental Transactions”, 2009 Second International Conference on Computer and
4. M. Toorani and A. Beheshti Shirazi, “SSMS-A secure SMS messaging protocol for the
   m-payment systems”, in Computers and Communications, IEEE Symposium on, July
   2008@IEEE, pp. 700–705.
5. D. Lisonenk and M. Drahansky, “SMS Encryption for Mobile Communication”, in Security
   Technology, SECTECH '08. International Conference on, Dec. 2008@IEEE, pp. 198–201.
   Security Architecture for Mobile Banking System”, 978-1-4244-2829-8/08/$25.00, 2008@IEEE.
7. Mahmoud Reza Hashemi, Elahe Sorouch, “A Secure m-Payment Protocol for Mobile
   Weaknesses”, the Second International Conference on Next Generation Mobile Applications,
   International Conference on Software Engineering, Artificial Intelligence, Networking and
   Parallel/Distributed Computing (SNPD’06), pp.413-418, June 2006@IEEE.
    Raphael C.-W. Phan “Fixing the Integrated Diffie-Hellman - DSA Key Exchange Protocol” IEEE
    Communications Letters, Vol. 9, No. 6, JUNE 2005
    58-309.
14. Jiezhao Peng, Qi Wu “Research and implementation of RSA algorithm in Java”
    International Conference on Management of e-Commerce and e-Government, 2001 IEEE.
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
A Secure Digital Signature Approach for SMS Security


**Index Terms**

Computer Science

Communications

**Key words**

GSM

SMS security

ECDSA

ECDLP

public key cryptography