Abstract

The development of information technology is increasingly rapidly create the need for more important information. This is what inspires a bank to implement a transaction service that is often referred as SMS-Banking. However, sms-banking are implemented at this time does not guarantee the data security of its customers. Security threats include third parties who want to tap transaction between customer and bank. One way to overcome these vulnerabilities is to implement cryptographic algorithm. The method used is ECDSA for digital signature and an ECC algorithm that called ECIES for message encryption. ECDSA and ECIES is one of public key algorithm based on elliptic curves. This application will be implemented in java programming language that consist of a client who uses J2ME and server that used J2EE.

This undergraduate thesis will analyze the time performance parameters off each domain parameters that recommended by NIST, security parameters, and parameters of cryptography(authentication, non repudiation, integrity, and confidentiality). Based on research results obtained the conclusion that the combination of algorithm ECDSA and ECIES cam guarantee the fulfillment of all aspects cryptography security such as aspects authentication, non repudiation, integrity, and confidentiality. In this research also concluded that the most suitable domain parameters for cell phone is NIST 163.

Key Words : ECDSA,ECIES,domain parameters, encryption, digital signature