ABSTRACT

SYAMSUL ARIFIN, Implementation of Public Key Infrastructure for Security System of Local Elections Data Transmission Via Mobile. Supervised by SHELVIE NIDYA NEYMAN

Cryptography is a process of encrypting data into a form that can be read only by a system. The system has a key to read the encrypted data. Based on the method, cryptographic algorithms can be divided into asymmetric key cryptography, symmetric key cryptography, and public key cryptography. This research attempts to develop Public Key Infrastructure (PKI) with integrity service, which is implemented in the transmission of voting results in mobile election process. The benefits of this research is to simplify and improve the efficiency of the counting process and improving the security of the data transmission using mobile communication.

The method employed is the Life Cycle Security System in which a sequence of steps following the life cycle of security system by eliminating the operational and maintenance step. The algorithm used in this research are RSA and MD5 Hash Function. RSA Algorithm is used to facilitate the distribution of keys that was used in the message encryption, and MD5 hash functions as an authentication function. The result of this research is the security system of the transmission of local elections vote via mobile which overcome the threat of sniffing or snooping, camouflage, and alteration with provides security services of authentication, integrity, and availability.

Keywords: Election of Regional Head, Java, J2ME, Public Key, RSA Algorithm.