

ABSTRAK

Smart Card is a tool that is used for fast and practical data transactions in the form of chips embedded in the card. This card is very helpful for the process of identification and administration such as patient cards in hospitals, especially in emergencies. However, patient data can only be accessed by certain people, therefore the card requires a security mechanism such as cryptographic algorithms to secure the contents of the data. Therefore the algorithm needed for the patient card is an algorithm that has fast processing capabilities and a high level of security. In this paper, we try to implement the Tiny Encryption Algorithm on a Smart Card and calculate the processing time and measure the level of security using the Avalance Effect.

Based on the results in this study the time of encryption and decryption of patient data with a total of 600 lines of patient medical history measuring 30.6 Kb resulted in an average encryption time of 20.17 ms while decryption required time of 17.21 ms that indicate processing time is very small. The Avalance Effect test performed on the TEA encryption process produces an Avalance Effect of 77% which shows that encrypted data has very random ciphertext results so that the data content is kept confidential with a high level of security. The test results of process time and AE can be concluded that the TEA is an algorithm that can process a fast data securing with high security and time that can be tolerated by smart card users.

Keywords: Smart Card, TINY ENCRYPTION ALGORITM, Encryption, Decryption.