ABSTRACT

In the era of information and communication technology now, generally occurs through the exchange of digital information public network such as E-mail, SMS and other messenger applications. This resulted prone to theft of information by unauthorized parties. So it needs a security mechanism which guarantees the security of the information contained in the message. In this final project has been built an application that is useful to improve the security of the information contained in the message, whether it be text or images on communication via Android smartphones. This can be done with the encryption-decryption process running on Android smartphones.

In this final project use two algorithms namely Rijndael or AES algorithm (Andvanced Encryption Standard) and AES which has been modified. The use of the modified AES algorithm is intended to determine the performance capability of these algorithms. Is it better than the AES algorithm itself, given the AES algorithm has been used for more than ten years.

The results obtained from tests performed in this final performance of the system using the AES algorithm is similar to the performance of a system that uses the AES algorithm modified. Both systems have values similar avalanche effect which ranges from 0.5 and the duration of time required to perform a brute force attack that is 2.6×10^{21} *years. However, different computation time and robustness performance on both systems. Computing time on a system that uses the AES algorithm is faster than systems using the AES algorithm modified. While the robustness test, the system performance using the modified AES algorithm is better than a system that uses the AES algorithm.*

Keywords: Android, encryption, decryption, AES.