ABSTRACT

Cryptography becomes a fully integrated part of network security system in global information era. There are some parameters for cryptography system, they are level of algorithm security, flexibility, characters appearance distribution frequency, distribution variance, avalanche effect, brute force attack, and data execution time. Those parameters are then could be uses as the guidance for the users to choose the suitable cryptography system based on their needs.

Advanced Encryption Standard (AES) and Camellia are the examples of the cipher block-based cryptography system. Both cryptography systems using the same symmetric keys, 128 bit block size, and 128, 192, 256 length of keys.

This final project measures and analyzes the comparison of AES and Camellia algorithm performance. This comparison facilitated by the software which simulated the cryptography process for both algorithms. The performance parameters measurements including the time process, the influence of operation mode, avalanche effect, and brute force attack. This final project use Java programming language as the software development system.

Keywords: Camellia, Advanced Encryption Standard, Cryptography, cipher block, avalanche effect, brute force attack.