

Abstract

Security has become an important aspect in data communication. Usually, data or information only shown for specific person. Because of that, it is very important to keep that information from other hand.

In this final task, a system will be developed using the Borland Delphi 7 to analyze the difference HC-128 algorithm with Sosemanuk algorithm in performance. The comparison parameters are encryption and decryption process time, memory amount used in encryption and decryption process, and avalanche effect value.

Based on the simulation, encryption/decryption time process for HC-128 algorithm and Sosemanuk algorithm has the difference of time process because there are difference in keystream generate. The number of the memory which is used by both of these algorithm in encryption/decryption process are different too.

Keywords : cryptography, private key, HC-128, Sosemanuk