ABSTRACT

The development of information technology increasingly rapid, information can be obtained easily from various sources. Unfortunately the development of information technology is often misused by the parties who are not responsible, the data containing important information often spread and harm many parties.

In order that the information is not misused, it can be anticipated by applying the science of cryptography, so that the information is kept confidential. Many new methods of cryptography can be used to keep confidential information at the software or hardware level.

In this final project, Trivium stream cipher algorithm will be implemented on Altera Cyclone IV Field-programmable Gate Arrays (FPGA) at hardware level or more precisely on prototype IC. The input used is binary. The random number generator method used in this research is NFSR (Non-Linear Feedback Shift Register) and will use Verilog programming language to describe various functions of digital circuit. Then the hardware can perform the encryption process to convert the original message (plaintext) into an encrypted message (ciphertext) and vice versa (decryption). The results of the implementation will be analyzed based on the specified aspects of the test. Then the performance of the Trivium algorithm will be compared with the performance of other hardware-oriented stream cipher algorithms.

Keywords: Cryptography, Trivium, Altera