ABSTRACT

Internet of Things (IoT) is now an innovation and trend that is used in almost all industries in the world. IoT has the ability to connect various objects to exchange information and work together to reach a decision. In the implementation of IoT, good data security must be maintained even though it has limited device resources. To overcome these problems, various encryption algorithms that are effective in IoT applications are proposed. This final project discusses and analyzes the performance of stream cipher and block cipher algorithms, namely SNOW 3G and Advanced Encryption Standard (AES).

The SNOW 3G algorithm is designed and used as the basic algorithm in confidentiality and integrity for 3GPP technology. In addition, the AES algorithm is set to be one of the best algorithms for secret data storage and implementation on software and hardware. Each algorithm is then tested for randomness and uncertainty of encryption data through a simulation. Then, compare the two results to determine the best and safest algorithm if it will be implemented on IoT technology.

After the test, this Final Project research obtained the results of randomness and data uncertainty in the form of the avalanche effect and entropy values of each algorithm. The AES algorithm produces higher avalanche effect and entropy values, which are 50.695% and 3.60603. Meanwhile, the SNOW 3G algorithm produces values of 49.574% and 3.56136.

Keywords: Internet of Things (IoT), Stream Cipher, Block Cipher, SNOW3G algorithm, Advanced Encryption Standard (AES) algorithm.