

ABSTRAK

Internet of Things (IoT) kini menjadi sebuah inovasi dan tren yang digunakan hampir di seluruh industri di dunia. IoT memiliki kemampuan dalam menghubungkan berbagai objek untuk saling bertukar informasi dan bekerja sama mencapai suatu keputusan. Dalam implementasi IoT, keamanan data yang baik harus tetap terjaga walaupun memiliki sumber daya perangkat terbatas. Untuk mengatasi permasalahan tersebut, maka diusulkan berbagai algoritma enkripsi yang efektif dalam aplikasi IoT. Tugas Akhir ini membahas dan menganalisa performansi algoritma *stream cipher* dan *block cipher* yaitu SNOW 3G dan *Advanced Encryption Standard* (AES).

Algoritma SNOW 3G dirancang dan digunakan sebagai algoritma dasar dalam kerahasiaan dan integritas untuk teknologi 3GPP. Serta, algoritma AES yang ditetapkan menjadi salah satu algoritma terbaik dalam penyimpanan data rahasia dan implementasi pada perangkat lunak maupun perangkat keras. Dari masing-masing algoritma kemudian dilakukan pengujian keacakan dan ketidakpastian data enkripsi melalui sebuah simulasi. Lalu, membandingkan kedua hasil tersebut untuk menentukan algoritma yang paling baik dan aman jika akan diimplementasikan pada teknologi IoT.

Setelah dilakukan pengujian, penelitian Tugas Akhir ini memperoleh hasil keacakan dan ketidakpastian data berupa nilai *avalanche effect* dan *entropy* dari masing-masing algoritma. Algoritma AES menghasilkan nilai *avalanche effect* dan *entropy* yang lebih tinggi, yaitu sebesar 50,695% dan 3,60603. Sedangkan, algoritma SNOW 3G menghasilkan nilai sebesar 49,574% dan 3,56136.

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