ABSTRAK

Perkembangan teknologi internet dan kebutuhan manusia akan teknologi memicu berbagai inovasi, salah satunya Internet of Things (IoT) yang kini menjadi tren yang digunakan hampir oleh seluruh industri di dunia. Dalam implementasi IoT, keamanan data harus tetap terjaga walaupun sumber daya perangkat yang dimiliki terbatas. Untuk mengatasi permasalahan tersebut, diusulkan berbagai algoritma enkripsi yang baik untuk aplikasi IoT. Tugas akhir ini membahas mengenai implementasi penerapan *lightweight stream cipher* yaitu algoritma SNOW 3G dan algoritma *block cipher* RSA sebagai pembanding.

Algoritma SNOW 3G dirancang untuk digunakan sebagai algoritma dasar dari kerahasiaan (*confidentiality*) 3GPP dan algoritma integritas. Selain itu terdapat algoritma RSA, yang kini sudah menjadi standar pilihan algoritma enkripsi yang sudah digunakan dalam banyak aplikasi. Oleh karena itu Tugas akhir ini menguji dan menganalisa kedua algoritma tersebut untuk mengetahui mana yang lebih baik untuk diimplementasikan pada IoT.

Dari hasil penelitian Tugas Akhir ini, didapatkan bahwa algoritma SNOW 3G memiliki nilai *Avalanche Effect* yang lebih baik daripada algoritma RSA, dengan nilai 52% yang menjamin tiap satu bit *input* yang diubah data akan berubah banyak. Selain itu nilai *Entropy* SNOW 3G juga lebih tinggi yang menjamin ketidakpastian data terenkripsi. Untuk aplikasi IoT dengan studi kasus RFID, didapatkan hasil komunikasi jaringan dengan nilai *Quality of Service* (QoS) yang sangat bagus dan memenuhi standar.

Kata Kunci: *Internet of Things (IoT), RFID, Lightweight Stream Cipher, SNOW 3G algorithm, RSA algorithm*