ABSTRAK

Perkembangan *Internet of Things* (IoT) yang pesat, semakin memungkinkan objek fisik untuk berbagi informasi satu sama lain dan mengoordinasikan keputusan. Implementasi IoT yang akan diterapkan di berbagai bidang, memiliki persyaratan sumber daya dan kapasitas memori perangkat yang terbatas, namun keamanan data yang dikirimkan tetap terjamin. Sebuah ide penelitian telah diusulkan untuk menyelesaikan permasalahan mengenai penggunaan algoritma enkripsi dalam aplikasi IoT. Sedangkan untuk menemukan metode enkripsi *lightweight stream cipher* yang paling efektif, melalui Tugas Akhir ini akan melakukan analisis terhadap beberapa metode enkripsi.

Algoritma Grain v1 mewakili standar stream cipher oleh NIST (*National Institute of Standards and Technology*) untuk profil implementasi *hardware*. Serta algoritma Espresso yang dikembangkan untuk mengakomodasi komunikasi nirkabel 5G. Lalu dilakukan skema pengujian keacakan dan ketidakpastian untuk data keluaran dari masing-masing algoritma. Mengimplementasikan masing-masing program pada sistem aplikasi RFID serta menguji performansinya, seperti *memory usage* dan waktu komputasi pada mikrokontroler, serta performansi jaringannya.

Oleh karena itu, setelah melewati serangkaian pengujian, penelitian Tugas Akhir ini dapat memperoleh hasil berupa hasil analisis dan kesimpulan algoritma *lightweight stream cipher* yang paling efektif. Sehingga dapat menangani permasalahan keamanan dalam pengiriman data untuk studi kasus aplikasi RFID dengan menggunakan mikrokontroler NodeMCU ESP8266.

Kata Kunci: *Internet of Things* (IoT), RFID, *Lightweight Stream Cipher*, Grain v1 Algorithm, Espresso Algorithm