ABSTRAK

Perkembangan *Internet of Things* (IoT) mendorong meningkatnya kebutuhan komunikasi *Machine-to-Machine* (M2M) yang aman, meskipun perangkat IoT umumnya memiliki keterbatasan memori, daya, dan kemampuan komputasi. Algoritma kriptografi konvensional tidak selalu efisien untuk perangkat dengan sumber daya terbatas, sehingga dibutuhkan enkripsi ringan yang efektif dan hemat sumber daya. Penelitian ini berfokus pada perbandingan kinerja empat algoritma kriptografi ringan, yaitu ASCON, PRESENT, LED, dan TWINE, dalam skenario komunikasi M2M berbasis Arduino. Evaluasi dilakukan terhadap kecepatan, penggunaan memori, jumlah instruksi mesin, serta efektivitas confusion dan diffusion.

Metode yang digunakan melibatkan implementasi algoritma pada dua unit Arduino Uno, masing-masing berperan sebagai *transmitter* (TX) dan *receiver* (RX) melalui komunikasi serial UART. Pengujian dilakukan secara virtual menggunakan platform Tinkercad, dengan parameter yang diukur meliputi waktu enkripsi-dekripsi, persentase diffusion, nilai Hamming Distance, kompleksitas algoritma (Big O), serta penggunaan memori program dan data. Setiap algoritma diuji sebanyak lima kali untuk memperoleh data yang konsisten. Proses ini dilakukan untuk memastikan hasil bebas dari pengaruh variabel lingkungan fisik.

Hasil pengujian menunjukkan bahwa ASCON memiliki performa terbaik dengan waktu enkripsi rata-rata 318 µs dan dekripsi 367 µs, disertai nilai diffusion mendekati 50% dan efisiensi penggunaan memori yang tinggi. PRESENT dan LED unggul dalam konsumsi memori yang lebih rendah, namun memiliki waktu proses yang lebih lama dibandingkan ASCON. TWINE memberikan kinerja seimbang namun tidak seoptimal ASCON dari sisi kecepatan. Berdasarkan hasil ini, ASCON direkomendasikan sebagai algoritma kriptografi ringan yang paling optimal untuk komunikasi M2M pada perangkat IoT.

Kata kunci: IoT, M2M, Kriptografi ringan, Arduino Uno, Confusion, Diffusion