1. Pendahuluan

Latar Belakang

Perkembangan teknologi informasi berkembang pesat dalam beberapa tahun ini. Saat ini, karena kemajuan teknologi yang berkembang pesat, *smart devices* dapat saling terhubung, berkomunikasi, dan berinteraksi melalui internet. Teknologi tersebut membuat kegiatan manusia menjadi lebih mudah dan efisien. *Internet of Things* (IoT) adalah teknologi inovatif yang berkembang pesat dengan berbagai aplikasi, fungsi, dan layanan dalam kehidupan sehari-hari dan dalam berbagai domain [1]. IoT merupakan jaringan antar perangkat fisik, kendaraan, bangunan, dan benda-benda lain yang disematkan dengan elektronik, perangkat lunak, sensor, aktuator, dan jaringan konektivitas yang memungkinkan objek-objek ini mengumpulkan dan bertukar data [2].

Semakin banyak perangkat IoT yang berkembang memunculkan banyak celah dalam keamanan data dan privasi. Masalahnya berkaitan dengan bagaimana data rentan terhadap pelanggaran dan pengawasan [3]. Perangkat IoT terhubung ke internet sehingga rentan terhadap serangan siber yang memengaruhi sistem komputer lainnya [3]. Maka dari itu, banyak perhatian yang perlu diberikan pada perangkat-perangkat ini, terutama dalam hal pemrosesan data [4]. Keamanan perangkat IoT sangat penting untuk mencegah pencurian informasi ketika perangkat IoT diretas. Area utama dalam bidang keamanan IoT meliputi *authentication*, *non-repudiation*, *access control*, *confidentiality*, *integrity*, dan *availability* [5]. Dengan bantuan kriptografi tradisional, semua tujuan ini dapat dipenuhi, namun metode ini membutuhkan alokasi sumber daya yang besar. Di sisi lain, perangkat IoT memiliki daya komputasi yang terbatas, memori yang terbatas, dan daya tahan baterai yang terbatas [4, 5]. Maka dari itu, dibutuhkan sebuah algoritma kriptografi yang ringan untuk dijalankan pada perangkat berdaya komputasi rendah.

Hingga saat ini, sudah banyak yang mengembangkan algoritma kriptografi ringan atau *Lightweight Cryptography* (LWC) yang menggunakan metode enkripsi simetri, seperti *Advanced Encryption Standard* (AES), *Data Encryption Standard* (DES), LED, dan Blowfish. Pada tahun 2021, Thabit dkk. [6] mengembangkan sebuah algoritma baru bernama *New Lightweight Cryptographic Algorithm* (NLCA). NLCA adalah *cipher* blok kunci simetris dan idenya terinspirasi oleh kombinasi metode arsitektur Feistel dan *Substitution Permutation* (SP) untuk meningkatkan kompleksitas enkripsi [6]. Pada ukuran file 50MB, NLCA menghasilkan waktu yang lebih cepat daripada algoritma DES, 3DES, AES, Blowfish, dan LED [6]. Namun, NLCA baru hanya diuji pada *cloud network* dan belum pernah diuji pada perangkat berdaya komputasi rendah seperti IoT. Oleh karena itu, diperlukan sebuah analisis terhadap performa NLCA pada perangkat berdaya komputasi rendah seperti IoT.

Topik dan Batasannya

Pada penelitian ini, NLCA akan diimplementasikan menggunakan bahasa Python yang kemudian diubah menjadi MicroPython. Selanjutnya waktu eksekusi dihitung setiap percobaan dan akan dibandingkan dengan algoritma kriptografi *cipher* blok lainnya. Adapun pembatasan masalah yang dikaji dalam penelitian ini, yaitu :

1. Implementasi dilakukan dengan menggunakan simulasi pada web wokwi.com [7] menggunakan *microcontroller* ESP32 yang akan dijelaskan pada bagian 3.
2. Beberapa detail proses *key generation,* enkripsi, dan dekripsi yang tidak dijelaskan disesuaikan, antara lain :
    a. *Left shift* dilakukan sebanyak satu bit.
    b. *Rail-fence* dilakukan menggunakan kunci 3.
    c. Kombinasi matriks pada langkah *key generation* disesuaikan dengan paper yang dirujuk oleh paper utama, yaitu algoritma *Secure IoT* (SIT) [8].

Tujuan

Penelitian ini bertujuan untuk mengetahui waktu eksekusi *New Lightweight Cryptographic Algorithm* (NLCA) pada sebuah perangkat berdaya komputasi rendah serta membandingkan algoritma NLCA dengan algoritma enkripsi blok *cipher* lainnya.

Organisasi Tulisan

Penyusunan penelitian dimulai dengan mengeksplorasi studi sebelumnya tentang kriptografi ringan dan *Internet of Things* (IoT). Rencana metodologi akan diuraikan dalam bagian ketiga, disusul oleh presentasi hasil dan diskusi dalam bagian keempat, dan akhirnya kesimpulan disajikan dalam bagian kelima.