BAB I
PENDAHULUAN

1.1 Latar Belakang

Ledakan ekosistem *Internet of Things (IoT)* menempatkan miliaran perangkat berdaya, memori, dan komputasi terbatas di lingkungan yang rawan ancaman. Pada perangkat terbatas, generator bilangan acak sering kali memiliki entropi rendah [24]. Jika algoritma enkripsi itu sendiri menghasilkan ciphertext yang memiliki pola statistik (tidak acak sempurna), maka penyerang dapat melakukan *distinguishing attack* atau bahkan memulihkan kunci melalui korelasi statistik, tanpa perlu memecahkan matematika rumit algoritma tersebut [7, 21]. Pada konteks ini, diperlukan kriptografi yang ringan namun andal, sehingga mendorong *National Institute of Standards and Technology (NIST)* menyelenggarakan *Lightweight Cryptography (LWC) Standardization Project* untuk memilih rancangan yang memenuhi kebutuhan keamanan sekaligus efisiensi di perangkat terbatas [1]. Di tingkat tata kelola, kebutuhan akan kontrol keamanan yang terukur dan kerangka kerja berbasis risiko juga ditekankan oleh studi adopsi kerangka *NIST* dalam infrastruktur TI modern [14], sedangkan aspek efisiensi energi dan jejak memori pada *cipher* ringan menjadi perhatian kunci di lingkungan tertanam/IoT [15].

Hasil proses standardisasi menempatkan *ASCON* sebagai keluarga algoritma terstandar untuk *AEAD*, *hash*, dan *XOF*, diformalkan dalam *NIST SP 800-232* dengan parameter, antarmuka, dan vektor uji resmi [2]. Di sisi lain, *TinyJAMBU* (*permutation-based* yang sangat ringkas) dan *Grain-128AEAD (stream-cipher AEAD)* terdokumentasi melalui spesifikasi finalis dengan detail desain, *parameter*, serta batasan operasional [6, 9]. Perbandingan *throughput* menunjukkan *ASCON* kompetitif terhadap algoritma populer lain pada skenario *IoT* tertentu [19], sementara literatur efisiensi menyoroti *trade-off* konsumsi daya vs. kekokohan kripto pada *cipher* ringan [16]. Dengan ekosistem dan pilihan desain yang beragam tersebut, dibutuhkan evaluasi yang adil dan dapat direplikasi atas artefak keluaran algoritma.

Salah satu aspek fundamental keamanan kriptografi adalah kerandoman pada keluaran (*keystream*/*ciphertext*). Survei mengenai kerandoman dan sumber acak di kriptografi menegaskan bahwa derajat acak yang memadai berperan sentral dalam menutup peluang bias statistik yang dapat dieksploitasi [7]. Rastoceanu et al. (2023) menyoroti bahwa pembangkitan bilangan acak yang aman secara kriptografis adalah krusial untuk menjamin kerahasiaan dan *forward secrecy* pada perangkat IoT [24]. Pada *Grain-128AEAD*, sifat

stream-cipher menuntut kepatuhan ketat pada batas panjang keystream karena korelasi jangka panjang potensial dapat dieksploitasi [17]. Sejalan dengan itu, penggunaan *NIST SP 800-22 Statistical Test Suite (STS)* sebagai *sanity check* terhadap *ciphertext* membantu mendeteksi indikasi pola/bias yang tidak semestinya pada keluaran, melengkapi analisis desain struktural.

Studi *statistical fault analysis* terhadap *TinyJAMBU* menunjukkan bahwa injeksi kesalahan tertentu dapat menimbulkan perubahan struktur pada *ciphertext/tag* [20], sementara *persistent faults* pada *ASCON* berpotensi memunculkan sinyal statistik terkait kunci melalui distorsi *S-box* [10]. Dengan demikian, inspeksi kerandoman *ciphertext* berfungsi sebagai indikator dini anomali implementasi maupun penggunaan di luar batas aman spesifikasi. Analisis keamanan *ASCON* yang lain [12] turut menegaskan perlunya verifikasi multi-perspektif (desain, *fault*, dan statistik) atas keluaran.

Berangkat dari celah pelaporan komparatif, banyak riset berfokus pada desain/standar, performa, atau fault, namun relatif sedikit yang membandingkan kerandoman *ciphertext* lintas algoritma LWC dengan metodologi STS yang seragam. Untuk mengisi celah tersebut, penelitian ini menetapkan Klaim Utama (*Core Claim*) yang hendak diuji kebenarannya secara ilmiah: "Penyederhanaan arsitektur matematis pada algoritma Kriptografi Ringan (ASCON-128, TinyJAMBU-128, dan Grain-128AEAD) demi efisiensi sumber daya *IoT*, tidak mendegradasi kualitas kerandoman statistik output *ciphertext*-nya jika dibandingkan dengan algoritma baseline global AES-128". Rancangan uji memanfaatkan parameter dan vektor uji dari dokumen resmi [2], berfokus pada sifat statistik ciphertext (bukan metrik performa) [19]. Kontribusi yang diharapkan ialah pelaporan empiris derajat kerandoman keluaran untuk membuktikan klaim tersebut, interpretasi konservatif hasil STS sebagai pelengkap kriptanalisis, serta rekomendasi awal pemilihan algoritma untuk perangkat terbatas.

1.2 Rumusan Masalah

Berdasarkan latar belakang dan klaim utama yang telah ditetapkan, rumusan masalah dalam penelitian ini diformulasikan ke dalam pertanyaan ilmiah sebagai berikut:

1. Sejauh mana tingkat kerandoman statistik *ciphertext* dari algoritma LWC (ASCON-128, TinyJAMBU-128, dan Grain-128AEAD) jika dibandingkan dengan *baseline*

AES-128, ketika dievaluasi menggunakan instrumen pengujian *NIST Statistical Test Suite*?

2. Apakah terdapat deviasi atau bias statistik yang terdeteksi secara empiris pada output *ciphertext* algoritma LWC sebagai konsekuensi dari penyederhanaan arsitektur kriptografisnya (seperti minimnya *logic gates* pada TinyJAMBU atau penggunaan LFSR pada Grain)?

1.3 Tujuan

Sejalan dengan rumusan masalah di atas, maka tujuan utama dari penelitian ini adalah sebagai berikut:

1. Mengevaluasi dan membuktikan hipotesis (Klaim Utama) terkait kualitas kerandoman statistik *ciphertext* dari algoritma ASCON-128, TinyJAMBU-128, dan Grain-128AEAD terhadap AES-128 berdasarkan metrik *pass rate* dan *p-value uniformity* dari NIST STS.
2. Mengidentifikasi secara empiris ada tidaknya bias statistik (kegagalan distribusi bit lokal/global) pada algoritma-algoritma LWC yang diuji, guna menentukan kelayakan keamanannya untuk perangkat IoT yang memiliki sumber entropi rendah.

1.4 Manfaat

Penelitian ini diharapkan memberikan manfaat serta kontribusi keilmuan yang secara spesifik terbagi ke dalam tiga dimensi utama:

1. Penelitian ini memberikan validasi teoretis terhadap desain arsitektur Kriptografi Ringan (LWC). Hasil penelitian ini menguji teori bahwa mekanisme difusi dan konfusi pada desain efisien seperti *sponge construction* (ASCON) [2], *Non-linear Feedback Shift Register* (Grain) [9], dan *Keyed Permutation* (TinyJAMBU) [4, 5] memiliki kekuatan matematis yang ekuivalen dengan *Substitution-Permutation Network* konvensional pada AES dalam menghasilkan entropi data.
2. Menyediakan dataset evaluasi *randomness* secara *head-to-head* dan komprehensif antara standar LWC terbaru dari NIST (ASCON) melawan finalis lain dan AES. Pembuktian empiris (berupa rasio kelulusan dan keseragaman *p-value*) ini mengisi celah *state-of-the-art* dalam literatur keamanan IoT, memberikan landasan data

faktual bagi peneliti dan praktisi industri dalam memilih algoritma LWC yang tidak rentan terhadap serangan analisis statistik [21].

3. Menawarkan kerangka kerja evaluasi (*evaluation framework*) yang ketat dan *reproducible* untuk menguji output *cipher*. Metodologi ini memperkenalkan standar validasi internal yang kuat melalui penerapan *Known Answer Tests* (KAT) sebelum pembangkitan korpus, dipadukan dengan strategi *Low-Entropy Input* (injeksi *null-plaintext*) yang memastikan bahwa kerandoman yang terukur murni berasal dari sifat intrinsik algoritma, bukan bias masukan (*input bias*).

1.5 Ruang Lingkup

Penelitian ini memiliki ruang lingkup sebagai berikut:

- Objek algoritma: *ASCON-128* (standar *LWC*), *TinyJAMBU* dan *Grain-128AEAD* (finalis *LWC*), serta *AES-128* sebagai baseline.
- Alat uji: *NIST STS (SP 800-22)* untuk evaluasi statistik ciphertext.
- Cakupan evaluasi: Fokus pada sifat statistik *ciphertext* (*pass ratio*, distribusi *p-value*, indikator *outlier*); tidak mencakup *benchmarking* performa/energi maupun kriptanalisis aktif.
- Kondisi uji: *Parameter* dan *vektor* uji mengikuti dokumen standar/finalis; ukuran korpus memenuhi kebutuhan minimal STS; variasi panjang pesan, kunci, dan *nonce/IV* dikontrol untuk kesetaraan uji.