ANALISIS STATISTIK KERANDOMAN OUTPUT CIPHERTEXT DARI ALGORITMA KRIPTOGRAFI RINGAN MENGGUNAKAN NIST STATISTICAL TEST SUITE

TESIS

Oleh:

DEDE EKA PRASETYA
NIM. 241231099

PROGRAM STUDI S-2 TEKNOLOGI INFORMASI
FAKULTAS INFORMATIKA
UNIVERSITAS MIKROSKIL
MEDAN
2025

STATISTICAL ANALYSIS OF RANDOMNESS IN CIPHERTEXT OUTPUT FROM LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS USING THE NIST STATISTICAL TEST SUITE

THESIS

By:

DEDE EKA PRASETYA
ID NUMBER. 241231099

MAJOR OF S-2 INFORMATION TECHNOLOGY
FACULTY OF INFORMATICS
UNIVERSITAS MIKROSKIL
MEDAN
2025

LEMBARAN PENGESAHAN

ANALISIS STATISTIK KERANDOMAN OUTPUT CIPHERTEXT DARI ALGORITMA KRIPTOGRAFI RINGAN MENGGUNAKAN NIST STATISTICAL TEST SUITE

TESIS

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Magister
Program Studi S-2 Teknologi Informasi

Oleh:

DEDE EKA PRASETYA
NIM. 241231099

Disetujui Oleh:

Dosen Pembimbing,

Dr. Ronsen Purba, M.Sc,

Medan, 13 Maret 2026
Diketahui dan Disahkan Oleh:

Ketua Program Studi
S-2 Teknologi Informasi,

Ir. Erwin Setiawan Panjaitan, M.M.S.I., Ph.D.

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-2 Teknologi Informasi Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Dede Eka Prasetya
NIM : 241231099

Saya telah melaksanakan penelitian dan penulisan Tesis dengan judul dan tempat penelitian sebagai berikut:

Judul Tesis : Analisis Statistik Kerandoman Output Ciphertext dari Algoritma Kriptografi Ringan Menggunakan NIST Statistical Test Suite

Tempat Penelitian : -
Alamat Tempat Penelitian : -
No. Telp. Tempat Penelitian : -

Sehubungan dengan Tesis tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Tesis tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Tesis saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tugas Tesis saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Tugas Tesis saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 13 Januari 2026
Saya yang membuat pernyataan,

Dede Eka Prasetya

ANALISIS STATISTIK KERANDOMAN OUTPUT CIPHERTEXT DARI ALGORITMA KRIPTOGRAFI RINGAN MENGGUNAKAN NIST STATISTICAL TEST SUITE

Abstrak

Pertumbuhan pesat ekosistem Internet of Things (IoT) menghadirkan tantangan keamanan pada perangkat dengan sumber daya terbatas, di mana algoritma kriptografi konvensional sering kali terlalu berat untuk diimplementasikan. Kriptografi ringan (Lightweight Cryptography/LWC) menjadi solusi utama, namun keamanan algoritma ini sangat bergantung pada kualitas kerandoman ciphertext untuk mencegah serangan pola statistik. Penelitian ini bertujuan untuk mengevaluasi dan membandingkan kualitas kerandoman statistik dari algoritma standar NIST LWC baru, yaitu ASCON-128, serta finalis TinyJAMBU-128 dan Grain-128AEAD, dengan AES-128 sebagai tolak ukur (baseline). Pengujian dilakukan menggunakan standar NIST Statistical Test Suite (NIST SP 800-22) yang mencakup 15 uji statistik terhadap korpus data ciphertext sebesar 400 juta bit yang dibangkitkan melalui simulasi terkontrol. Hasil penelitian menunjukkan bahwa ASCON-128 memiliki karakteristik statistik superior dengan tingkat kelulusan (pass rate) rata-rata di atas 99% dan distribusi P-value yang seragam, identik dengan AES-128. Grain-128AEAD terbukti tangguh terhadap uji Linear Complexity meskipun berbasis stream cipher, sementara TinyJAMBU-128 menunjukkan keseimbangan yang baik antara efisiensi dan keamanan statistik. Disimpulkan bahwa ketiga algoritma LWC tersebut memenuhi standar keacakan kriptografis dan aman untuk diadopsi pada perangkat IoT, dengan ASCON-128 sebagai rekomendasi utama untuk aplikasi yang membutuhkan margin keamanan tertinggi.

Kata kunci: *Kriptografi Ringan, NIST STS, Kerandoman Statistik, IoT.*

Abstract

The rapid growth of the Internet of Things (IoT) ecosystem presents security challenges for resource-constrained devices, where conventional cryptographic algorithms are often too heavy to implement. Lightweight Cryptography (LWC) has emerged as a key solution, but the security of these algorithms relies heavily on the randomness quality of their ciphertext to prevent statistical pattern attacks. This study aims to evaluate and compare the statistical randomness quality of the new NIST LWC standard, ASCON-128, as well as finalists TinyJAMBU-128 and Grain-128AEAD, using AES-128 as a baseline. Testing was conducted using the NIST Statistical Test Suite (NIST SP 800-22) standard, which includes 15 statistical tests on a ciphertext data corpus of 400 million bits generated through controlled simulation. The results indicate that ASCON-128 exhibits superior statistical characteristics with an average pass rate above 99% and a uniform P-value distribution, identical to AES-128. Grain-128AEAD proved robust against Linear Complexity tests despite being a stream cipher, while TinyJAMBU-128 showed a good balance between efficiency and statistical security. It is concluded that all three LWC algorithms meet cryptographic randomness standards and are safe for adoption in IoT devices, with ASCON-128 being the primary recommendation for applications requiring the highest security margins.

Keywords: *Lightweight Cryptography, NIST STS, Statistical Randomness, IoT.*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas berkat, rahmat, dan karunia-Nya, sehingga penulis dapat menyelesaikan Tesis ini dengan judul "**Analisis Statistik Kerandoman Output Ciphertext dari Algoritma Kriptografi Ringan Menggunakan NIST Statistical Test Suite**".

Tesis ini disusun sebagai salah satu syarat untuk memperoleh gelar Magister Komputer (M.Kom.) pada Program Studi S-2 Teknologi Informasi, Fakultas Informatika, Universitas Mikroskil.

Penulis menyadari bahwa selesainya Tesis ini tidak terlepas dari bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Bapak Dr. Ronsen Purba, M.Sc, selaku Dosen Pembimbing yang telah memberikan bimbingan dan arahan kepada penulis dalam penyelesaian tesis ini.
2. Bapak Muhammad Fermi Pasha, B.Sc., M.Sc., PhD., selaku Dosen Pendamping Pembimbing yang telah turut membimbing dan mendukung penulis dalam proses penyelesaian tesis ini.
3. Bapak Hardy, S.Kom., M.Sc., Ph.D., selaku Rektor Universitas Mikroskil Medan.
4. Bapak Sunaryo Winardi, S.Kom., M.T., selaku Dekan Fakultas Informatika Universitas Mikroskil Medan.
5. Bapak Ir. Erwin Setiawan Panjaitan, M.M.S.I., Ph.D., selaku Ketua Program Studi S-2 Teknologi Informasi Fakultas Informatika Universitas Mikroskil Medan.
6. Orang tua, istri dan keluarga tercinta yang senantiasa memberikan doa, motivasi, dan dukungan moral maupun materiil yang tak terhingga.

Penulis menyadari bahwa Tesis ini masih jauh dari kesempurnaan dikarenakan keterbatasan pengetahuan dan pengalaman penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang bersifat membangun demi penyempurnaan Tesis ini di masa mendatang.

Medan, 13 Januari 2026

Penulis,

Dede Eka Prasetya

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN