EVALUASI EFEKTIVITAS ALGORITMA ENKRIPSI RINGAN TERHADAP KINERJA DAN KEAMANAN DATA PADA PERANGKAT IOT

SKRIPSI NON REGULER - SCIENTIST

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

DAMAR INDRAJATI

21.83.0700

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

EVALUASI EFEKTIVITAS ALGORITMA ENKRIPSI RINGAN TERHADAP KINERJA DAN KEAMANAN DATA PADA PERANGKAT IOT

SKRIPSI NON REGULER - SCIENTIST

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

DAMAR INDRAJATI

21.83.0700

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI NON REGULER - SCIENTIST

EVALUASI EFEKTIVITAS ALGORITMA ENKRIPSI RINGAN TERHADAP KINERJA DAN KEAMANAN DATA PADA PERANGKAT IOT

yang disusun dan diajukan oleh

DAMAR INDRAJATI

21.83.0700

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 24 Juni 2025

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T.
NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI NON REGULER - SCIENTIST

EVALUASI EFEKTIVITAS ALGORITMA ENKRIPSI RINGAN TERHADAP KINERJA DAN KEAMANAN DATA PADA PERANGKAT IOT

yang disusun dan diajukan oleh

Damar Indrajati

21.83.0700

Telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Juni 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Jeki Kuswanto, S.Kom., M.Kom. **NIK. 190302456**	
Senie Destya, S.T., M.Kom. **NIK. 190302312**	
Wahid Miftahul Ashari, S.Kom., M.T. **NIK. 190302452**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 24 Juni 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Damar Indrajati
NIM : 21.83.0700

Menyatakan bahwa Laporan dengan judul berikut:

Evaluasi Efektivitas Algoritma Enkripsi Ringan Terhadap Kinerja Dan Keamanan Data Pada Perangkat IoT

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 24 Juni 2025

Yang Menyatakan,

Damar Indrajati

HALAMAN PERSEMBAHAN

Puji syukur saya panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat, kesehatan, dan kesempatan yang telah diberikan, sehingga saya dapat menyelesaikan laporan ini dengan baik.

Laporan ini saya persembahkan kepada:

- Kedua orang tua saya, yang selalu memberikan dukungan moral, semangat, doa, dan kepercayaan tanpa henti sepanjang proses pendidikan dan penyusunan laporan ini.
- Dosen pembimbing dan seluruh dosen di lingkungan program studi, atas ilmu, arahan, serta bimbingan yang sangat berarti selama masa perkuliahan dan penelitian ini berlangsung.
- Teman-teman dan rekan seperjuangan, yang selalu memberikan motivasi, masukan, dan bantuan, baik secara langsung maupun tidak langsung.
- Semua pihak yang telah mendukung, baik secara akademis maupun non-akademis, yang tidak dapat saya sebutkan satu per satu.

Semoga laporan ini dapat memberikan manfaat, menambah wawasan, serta menjadi bagian kecil dari kontribusi terhadap pengembangan ilmu pengetahuan, khususnya di bidang teknologi dan keamanan sistem IoT.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan kemudahan yang diberikan sehingga laporan dengan judul "Evaluasi Efektivitas Protokol Enkripsi Ringan terhadap Kinerja dan Keamanan Data pada Perangkat IoT" ini dapat diselesaikan dengan baik.

Laporan ini disusun sebagai dokumentasi ilmiah atas penelitian yang membandingkan efektivitas lima algoritma enkripsi ringan, yaitu SIMON, SPECK, XTEA, PRESENT, dan AES, pada perangkat Raspberry Pi yang banyak digunakan dalam sistem IoT.

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu, terutama kepada:

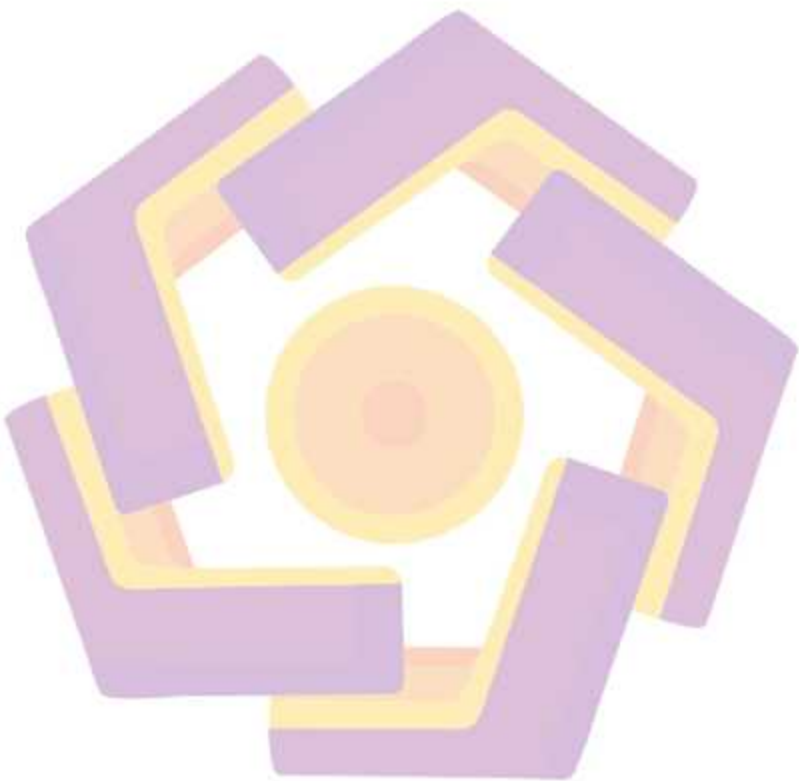
- Kedua orang tua atas doa dan dukungan moral yang diberikan.
- Dosen pembimbing atas bimbingan dan arahannya.
- Rekan-rekan yang turut memberi masukan selama proses penyusunan laporan ini.

Penulis menyadari laporan ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran sangat diharapkan demi perbaikan di masa mendatang. Semoga laporan ini bermanfaat bagi pengembangan ilmu, khususnya di bidang keamanan sistem IoT.

Yogyakarta, 24 Juni 2025

Penulis

DAFTAR ISI



DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

AES	Advanced Encryption Standard
ASIC	Application-Specific Integrated Circuit
BIC	Bit Independence Coefficient
CPU	Central Processing Unit
CTR	Counter Mode
DRS	Differential Resistance Score
DU	Differential Uniformity
ECB	Electronic Code Book
FPGA	Field Programmable Gate Array
GHz	Gigahertz
IoT	Internet of Things
ISO	International Organization for Standardization
MB	Megabyte
NSA	National Security Agency
NPCR	Number of Pixels Change Rate
TEA	Tiny Encryption Algorithm
UACI	Unified Average Changing Intensity
USB	Universal Serial Bus
XTEA	Extended Tiny Encryption Algorithm

DAFTAR ISTILAH

Algoritma Enkripsi Ringan	Algoritma kriptografi yang ringan untuk sistem.
Avalanche Effect	Ukuran perubahan pada plaintext ke ciphertext.
Block Cipher	Algoritma kriptografi yang mengenkripsi data dalam blok.
Cryptanalysis	Teknik membongkar enkripsi tanpa kunci.
Differential Cryptanalysis	Serangan dengan menganalisis input dan output.
Edge Computing	Komputasi data dilakukan di perangkat dekat sumber data.
IoT (Internet of Things)	Perangkat yang saling terhubung melalui internet.
Keamanan Data	Upaya melindungi data dari akses, modifikasi, atau perusakan.
Konsumsi Daya	Jumlah energi listrik yang digunakan oleh perangkat
Kriptografi	Ilmu dan teknik untuk mengamankan informasi.
Raspberry Pi	Komputer mini yang digunakan dalam prototype sistem IoT.
Throughput	Jumlah data yang ditransfer dalam periode waktu tertentu.

INTISARI

Keamanan data merupakan tantangan krusial dalam Internet of Things (IoT) karena keterbatasan daya komputasi, memori, dan konsumsi energi pada perangkat IoT. Algoritma enkripsi ringan telah dikembangkan untuk memberikan keseimbangan antara keamanan dan efisiensi dibandingkan dengan skema enkripsi konvensional.

Studi ini mengevaluasi efektivitas lima algoritma enkripsi SIMON64/128, SPECK64/128, XTEA64/128, PRESENT64/128, dan AES128 pada perangkat IoT dengan menganalisis kekuatan keamanannya, kecepatan eksekusi, penggunaan CPU, konsumsi memori, dan efisiensi daya. Eksperimen dilakukan pada Raspberry Pi 3B+ menggunakan implementasi berbasis bahasa C untuk mensimulasikan lingkungan IoT secara realistis.

Hasil penelitian menunjukkan bahwa AES-128 memberikan tingkat keamanan tertinggi dengan efek avalanche 39,29% dan skor ketahanan diferensial (DRS) 6,76/10, namun dibarengi konsumsi sumber daya tinggi (CPU 0,97 GHz, daya 0,63 A, memori 4,13 MB). SIMON64/128 dan SPECK64/128 menawarkan efisiensi terbaik dalam hal kecepatan, penggunaan daya, dan CPU, cocok untuk IoT berdaya rendah, namun terdapat kekhawatiran isu backdoor dari NSA. XTEA64/128 menjadi alternatif seimbang dengan tingkat keamanan sedang (DRS 5,07/10) dan konsumsi daya rendah (0,50 A), layak dipilih untuk perangkat IoT terbatas daya. Untuk IoT kelas menengah ke atas (contoh: Raspberry Pi), AES-128 direkomendasikan bila prioritasnya keamanan. Sebaliknya, untuk perangkat daya rendah seperti ESP8266 atau ARM Cortex-M, SIMON, SPECK, atau XTEA lebih realistis dipertimbangkan. Temuan ini menjadi acuan dalam menentukan algoritma enkripsi yang optimal berdasarkan kebutuhan spesifik perangkat IoT terkait keseimbangan antara keamanan, efisiensi, dan konsumsi daya.

Kata Kunci : IoT, Keamanan Informasi, Kriptografi, Perbandingan Kriptografi

ABSTRACT

Data security is a critical challenge in Internet of Things (IoT) due to the limited computational power, memory, and energy constraints of IoT devices. Lightweight encryption algorithms have been developed to provide a balance between security and efficiency compared to conventional encryption schemes.

This study evaluates the effectiveness of five encryption algorithms—SIMON64/128, SPECK64/128, XTEA64/128, PRESENT64/128, and AES128—on IoT devices by analyzing their security strength, execution speed, CPU utilization, memory consumption, and power efficiency. The experiments were conducted on a Raspberry Pi 3B+ using C-based implementations to simulate a realistic IoT environment.

The results indicate that AES-128 provides the highest level of security, with an avalanche effect of 39.29% and a Differential Resistance Score (DRS) of 6.76/10, but this comes at the cost of high resource consumption (CPU usage of 0.97 GHz, power consumption of 0.63 A, and memory usage of 4.13 MB). SIMON64/128 and SPECK64/128 demonstrate the best overall efficiency in terms of speed, power consumption, and CPU usage, making them suitable for low-power IoT environments. However, concerns remain regarding potential NSA-implemented backdoors in these algorithms. XTEA64/128 offers a balanced alternative with moderate security (DRS 5.07/10) and low power consumption (0.50 A), making it a viable choice for energy-constrained IoT devices. For mid-range IoT devices such as Raspberry Pi, AES-128 is recommended for applications prioritizing security. In contrast, for low-power devices such as ESP8266 or ARM Cortex-M, SIMON, SPECK, or XTEA are more practical options. These findings serve as a reference for selecting the most appropriate encryption algorithm based on the specific requirements of IoT devices, considering the balance between security, computational efficiency, and power consumption.

Keywords : *IoT, Information Security, Cryptography, Cryptography Comparison*