**Implementasi dan Analisis Performa Algoritma Enkripsi ChaCha20 Berbasis Protokol Komunikasi ESP-NOW Pada Wireless Sensor Network**

**Naufal Farras Trikusuma1, Agung Setia Budi2**

Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Brawijaya

Email: 1naufalfarr@student.ub.ac.id, 2penulis.dua@ub.ac.id

**Abstrak**

*Wireless Sensor Network* (WSN) telah berkembang pesat dalam mendukung proses otomasi, seperti pengumpulan data sensor, pengendalian sistem nirkabel, dan *monitoring*. Namun, keamanan data pada WSN menjadi tantangan penting karena data yang ditransmisikan sering kali bersifat sensitif dan rentan terhadap akses tidak sah. Selain itu, perangkat pada WSN memiliki keterbatasan sumber daya seperti memori, daya komputasi, dan energi, sehingga tidak memungkinkan penggunaan algoritma kriptografi konvensional yang memerlukan sumber daya tinggi. Oleh karena itu, diperlukan pendekatan *lightweight* *cryptography* yang efisien namun tetap memberikan perlindungan keamanan yang optimal. Penelitian ini menganalisis performa algoritma enkripsi ChaCha20 pada protokol komunikasi ESP-NOW menggunakan perangkat berbasis ESP8266. Evaluasi dilakukan dengan membandingkan kecepatan enkripsi, konsumsi energi, serta pengujian aspek keamanan terkait kerahasiaan data terhadap algoritma lain, yaitu AES-CBC, Clefia, dan Snow-V. Hasil penelitian menunjukkan bahwa ChaCha20 memiliki waktu komputasi tercepat dibandingkan algoritma lainnya, baik untuk ukuran data 5 KB maupun 10 KB. Selain itu, konsumsi energinya juga paling rendah, menjadikannya pilihan yang efisien untuk aplikasi WSN yang memiliki keterbatasan sumber daya. Temuan ini mendukung penggunaan ChaCha20 sebagai alternatif algoritma enkripsi yang efektif untuk meningkatkan keamanan data pada sistem WSN dengan tetap mempertimbangkan efisiensi komputasi dan penggunaan energi.

.

**Kata kunci**: *Wireless Sensor Network, ChaCha20, Lightweight Cryptography, ESP-NOW, Keamanan Data, Efisiensi Sumber Daya, Algoritma Enkripsi.*

**Abstract**

*Wireless Sensor Networks (WSN) has rapidly advanced in supporting automation, such as sensor data collection, wireless system control, and monitoring. However, data security in WSN poses a significant challenge, as the transmitted data is often sensitive and vulnerable to unauthorized access. Furthermore, WSN devices have limited resources, such as memory, computational power, and energy, making conventional cryptographic algorithms that require high resource consumption impractical. Therefore, an efficient lightweight cryptography approach is required to provide optimal security while maintaining resource efficiency. This study analyses the performance of the ChaCha20 encryption algorithm on the ESP-NOW communication protocol using ESP8266-based devices. The evaluation compares encryption speed, energy consumption, and security aspects related to data confidentiality against other algorithms, namely AES-CBC, Clefia, and Snow-V. The results indicate that ChaCha20 achieves the fastest computation time among the tested algorithms for both 5 KB and 10 KB data sizes. Additionally, its energy consumption is the lowest, making it an efficient choice for WSN applications with limited resources. These findings support the use of ChaCha20 as an effective encryption algorithm alternative to enhance data security in WSN systems while maintaining computational and energy efficiency.*

*.*

**Keywords**: *Wireless Sensor Network, ChaCha20, Lightweight Cryptography, ESP-NOW, Data Security, Energy Efficiency.*

# PENDAHULUAN

Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK) terbit dua belas kali setahun. J-PTIIK diterbitkan oleh Fakultas Ilmu Komputer (FILKOM), Universitas Brawijaya sejak Januari 2017. J-PTIIK memuat naskah hasil-hasil penelitian di bidang Teknologi Informasi dan Ilmu Komputer.

Naskah yang ditulis untuk J-PTIIK meliputi hasil-hasil penelitian di bidang Teknologi Informasi dan Ilmu Komputeri. Naskah diketik pada kertas berukuran standar A4 (21 cm x 29,7 cm) dalam format dua kolom dan satu spasi. Gunakan margin 3-3-2-2 cm (left-top-right-bottom), lebar tiap kolom 7,5 cm dengan jarak antar kolom 1 cm, menggunakan huruf Times New Roman 11 point dengan spasi tunggal. Naskah dalam bentuk file Microsoft Word dapat dikirimkan sewaktu-waktu melalui sistem OJS di <http://www.j-ptiik.ub.ac.id>.

Makalah dapat ditulis dalam Bahasa Indonesia dan Bahasa Inggris. Panjang naskah diharapkan tidak melebihi 10 halaman. Penulis diharuskan mengikuti petunjuk penulisan ini dan templatenya bisa didapatkan pada <http://www.j-ptiik.ub.ac.id>.

Sistematika naskah adalah: judul yang harus ditulis secara ringkas dan menggambarkan isi naskah; nama penulis (tanpa gelar akademik); afiliasi penulis; alamat email; abstrak (150 – 200 kata); kata kunci (minimal tiga buah); pendahuluan yang berisi latar belakang dan tujuan atau ruang lingkup tulisan; bahasan utama (dapat dibagi ke dalam beberapa sub-bagian); penutup atau kesimpulan; daftar pustaka (hanya memuat sumber-sumber yang dirujuk).

Isi pendahuluan mengandung latar belakang, tujuan, identifikasi masalah dan metode penelitian, yang dipaparkan secara tersirat (implisit). Kecuali bab Pendahuluan dan bab Kesimpulan, penulisan judul-judul bab sebaiknya eksplisit menyesuaikan isinya. Tidak harus implisit dinyatakan sebagai Dasar Teori, Perancangan, dan sebagainya.

# PERSAMAAN MATEMATIKA

Persamaan matematika harus diberi nomor urut dalam kurung biasa dan harus diacu dalam tulisan.

Persamaan matematika dinomori dengan angka Arab di dalam tanda kurung buka-tutup pada posisi rata kanan kolom. Persamaan ditulis menjorok ke dalam sejauh 6 mm.

Untuk persamaan yang tidak cukup ditulis dalam lebar 1 kolom, penulisannya dapat melintasi 2 kolom, ditulis di bagian bawah halaman dan diberi nomor urut yang sesuai. Perhatikan contoh penulisan Persamaan (1).

(1)

# TABEL DAN GAMBAR

Tabel dan gambar harus diberi nomor dan judul lengkap serta harus diacu dalam tulisan. Contoh: Tabel 1, Tabel 2(a), Gambar 1, Gambar 2(a). Berikut ini diberikan contoh penulisan tabel dan gambar.

## 3.1. Penulisan Tabel

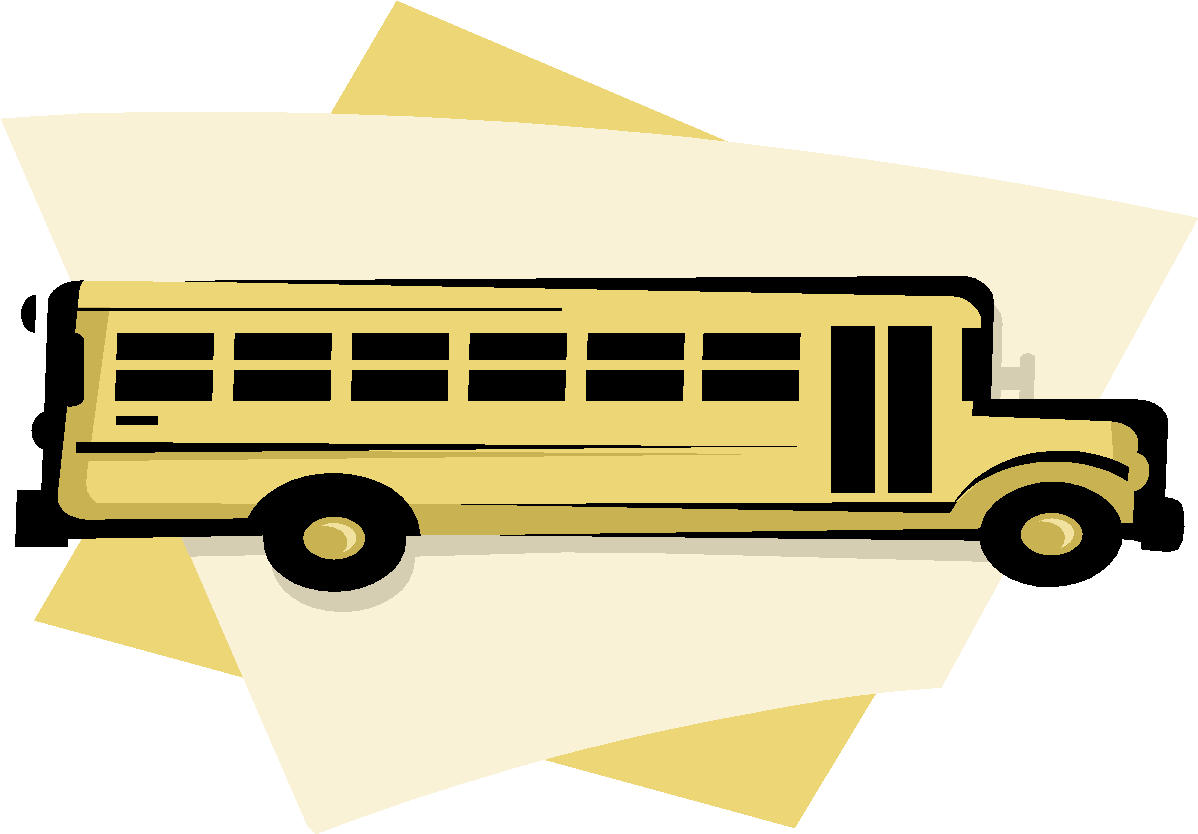
Perhatikan contoh penulisan Tabel 1. Keterangan tabel dituliskan pada bagian atas tabel. Sebisa mungkin hindari penggunaan garis vertikal.

Tabel 1. Rancangan Analisis Komputasi

|  |  |  |
| --- | --- | --- |
| **mesin** | **operasi** | **waktu(menit)** |
| 1 | 5 | 10 |
|  | 4 | 12 |
|  | 4 | 16 |
| 2 | 3 | 18 |
|  | 4 | 20 |

## 3.2. Penggunaan Gambar

Perhatikan contoh penggunaan Gambar 1. Keterangan gambar dituliskan pada bagian bawah gambar.



Gambar 1. Contoh penggunaan gambar

# SUMBER PUSTAKA/RUJUKAN

Sumber pustaka/rujukan sedapat mungkin merupakan pustaka-pustaka terbitan 10 tahun terakhir. Pustaka yang diutamakan adalah sumber-sumber primer berupa laporan penelitian (termasuk Skripsi/Tugas Akhir, Tesis, Disertasi) atau naskah-naskah penelitian dalam jurnal dan/atau majalah ilmiah.

Cara penulisan di daftar pustaka bisa dilihat pada contoh Daftar Pustaka. Sumber pustaka dituliskan terurut alfabetis dan kronologis.

Sumber pustaka yang digunakan bisa berupa:

* makalah jurnal;
* makalah konferensi ilmiah (*proceeding*);
* buku teks;
* laporan penelitian;
* skripsi atau thesis;
* makalah dalam buku kumpulan makalah ilmiah (*book section*).

# ATURAN LAIN

Semua naskah ditelaah secara blind-review oleh mitra bestari (reviewers) yang ditunjuk oleh redaksi menurut bidang kepakarannya. Penulis naskah diberi kesempatan untuk melakukan perbaikan (revisi) naskah atas dasar rekomendasi/saran dari mitra bestari dan redaksi pelaksana. Kepastian pemuatan atau penolakan naskah akan diberitahukan secara tertulis melalui email.

Pemeriksaan dan penyuntingan cetak-coba dikerjakan oleh redaksi dan/atau dengan melibatkan penulis. Naskah yang sudah dalam bentuk cetak-coba dapat dibatalkan pemuatannya oleh redaksi jika diketahui bermasalah.

Segala sesuatu yang menyangkut perijinan pengutipan atau penggunaan software komputer untuk pembuatan naskah atau hal lain yang terkait dengan HAKI yang dilakukan oleh penulis naskah, berikut konsekuensi hukum yang mungkin timbul karenanya, menjadi tanggung jawab penuh penulis naskah tersebut.

# CONTOH DAFTAR PUSTAKA

Dao, S. D. & Marian, R. 2011. Optimisation of precedence-constrained production sequencing and scheduling using genetic algorithms. *Proceedings of the International Multi Conference of Engineers and Computer Scientists*, 16-18 March, Hong Kong.

Gen, M. & Cheng, R. 2000. *Genetic Algorithms and Engineering Optimization.* John Wiley & Sons, Inc., New York.

Liliana, D. Y. & Mahmudy, W. F. 2006. Penerapan Algoritma Genetika pada Otomatisasi Penjadwalan Kuliah. *Laporan Penelitian DPP/SPP.* FMIPA Universitas Brawijaya, Malang.

Marian, R. M., Luong, L. & Dao, S. D. 2012. Hybrid genetic algorithm optimisation of distribution networks—a comparative study. *Dalam:* AO, S. I., CASTILLO, O. & HUANG, X. (editor.) *Intelligent Control and Innovative Computing.* Springer, US.

Phanden, R. K., Jain, A. & Verma, R. 2013. An approach for integration of process planning and scheduling. *International Journal of Computer Integrated Manufacturing*, 26(4), 284-302.

Ridok, A. 2014. Peringkasan dokumen Bahasa Indonesia berbasis non-negative matrix factorization. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 1(1), 39-44.

Tala, F. Z. 2003. A Study of Stemming Effects on Information Retrieval in Bahasa Indonesia. *Ph.D. Thesis*. Universiteit van Amsterdam.

Wang, L. 2007. *Process planning and scheduling for distributed manufacturing.* Springer, London.

Wibawa, A. P., Nafalski, A. & Mahmudy, W. F. 2013. Javanese `speech levels machine translation: improved parallel text alignment based on impossible pair limitation. *IEEE International Conference on Computational Intelligence and Cybernetics*, 3-4 December, Yogyakarta, Indonesia. 16-20.