**JURNAL ELTEK**
Vol. 23, No. 2, Oktober 2025, hal. 62 ~ 71
p-ISSN: 1693 – 4024 | e-ISSN: 2355-0740
DOI: 10.33795/eltek.v23i2.8614 

# Perbandingan performansi pengiriman data antar node *wireless sensor* menggunakan kriptografi RSA dan RC 4

**M. Nanak Zakaria[1], Yoyok Heru Prasetyo Isnomo[2], Martanti Puri Rahayu[3]**
**e-mail:** [1]nanakzach@polinema.ac.id, [2]urehkoyoy@polinema.ac.id,
[3]2141160122@student.polinema.ac.id
[1,2,3]Jurusan Teknik Elektro, Politeknik Negeri Malang, Indonesia

**Informasi Artikel**

***Riwayat Artikel***

Diterima 25 Agustus 2025
Direvisi 1 Oktober 2025
Diterbitkan 28 Oktober 2025

**Kata kunci:**

Jaringan Sensor Nirkabel
Keamanan Data
Rivest Cipher
Rivest Shamir Adleman

**ABSTRAK**

*Wireless Sensor Network* (WSN) adalah teknologi jaringan nirkabel untuk mengumpulkan dan mengirimkan data, namun rentan terhadap penyadapan sehingga memerlukan pengamanan menggunakan kriptografi. Penelitian ini membandingkan algoritma RSA (asimetris) dan RC4 (simetris) pada komunikasi antar node berbasis LoRa E220, menggunakan Arduino Nano, sensor DHT22, sensor tegangan, dan sensor arus ACS712 pada node pengirim serta node penerima untuk dekripsi. Pengujian menggunakan data sensor dan data string sepanjang 8–100 karakter, dengan kedua algoritma mencapai keberhasilan enkripsi dan dekripsi 100%. Waktu enkripsi rata-rata RSA adalah 0,0104 detik dan dekripsi 9,1284 detik, sedangkan RC4 mencatat 0,1894 detik untuk enkripsi dan 0,1616 detik untuk dekripsi. RC4 lebih cepat pada data pendek hingga menengah (0,027–0,132 ms) namun lebih lambat pada data besar (0,389 ms vs RSA: 0,092 ms). Dari sisi keamanan, pengujian *brute force* menunjukkan RSA sangat tahan karena tidak terbobol hingga 952,871–1001,652 s (±15 16 menit) pada berbagai variasi pesan dan kunci, sedangkan RC4 lebih rentan dengan kunci ditemukan dalam 52,871–85,983 s (±0,88–1,43 menit) dan seluruh pesan berhasil didekripsi. RC4 mengonsumsi energi lebih rendah (0,233–0,322 joule) dibanding RSA (0,2954–0,4024 joule). Kesimpulannya, RC4 unggul untuk komunikasi data pendek yang efisien, sedangkan RSA lebih andal dalam keamanan distribusi kunci.

***Keywords:***

*Data Security*
*Rivest Cipher*
*Rivest Shamir Adleman*
*Wireless Sensor Network*

***ABSTRACT***

*Wireless Sensor Network (WSN) is a wireless network technology for collecting and transmitting data, but it is vulnerable to interception and therefore requires security using cryptography. This study compares the RSA (asymmetric) and RC4 (symmetric) algorithms in LoRa E220-based node-to-node communication, using an Arduino Nano, DHT22 sensor, voltage sensor, and ACS712 current sensor on both the transmitter and receiver nodes for decryption. Testing was conducted using sensor data and string data ranging from 8 to 100 characters, with both algorithms achieving 100% encryption and decryption success rates. The average encryption time for RSA was 0.0104 seconds and decryption was 9.1284 seconds, while RC4 recorded 0.1894 seconds for encryption and 0.1616 seconds for decryption. RC4 is faster for short to medium-length data (0.027–0.132 ms) but slower for large data (0.389 ms vs. RSA: 0.092 ms). In terms of security, brute force testing showed that RSA is highly resistant, as it remained unbroken for 952.871–1001.652 seconds (±15–16 minutes) across various message and key variations, while RC4 is more vulnerable, with keys found in 52,871–85,983 s (±0.88–1.43 minutes) and all messages successfully decrypted. RC4 consumes less energy (0.233–0.322 joules) compared to RSA (0.2954–0.4024 joules). In conclusion, RC4 is superior for efficient short-term data communication, while RSA is more reliable in key distribution security.*

***Penulis Korespondensi:***
M. Nanak Zakaria,
Jurusan Teknik Elektro,
Politeknik Negeri Malang
Jl. Soekarno Hatta No. 9, Malang, Jawa Timur, Indonesia.
Email: nanakzach@polinema.ac.id

## 1. PENDAHULUAN

Perkembangan *Internet of Things* (IoT) telah membawa perubahan signifikan dalam berbagai bidang dengan memungkinkan proses otomatisasi yang meningkatkan kenyamanan, efisiensi, dan kecepatan [1]. Namun, tantangan seperti keterbatasan jangkauan komunikasi dan konsumsi daya tinggi masih menjadi hambatan dalam implementasi IoT [2]. Untuk mengatasi hal tersebut, diperlukan sistem yang hemat energi dan mampu beroperasi secara efisien tanpa bergantung penuh pada infrastruktur internet [3]. Salah satu solusi relevan adalah penerapan *Wireless Sensor Network* (WSN), yakni jaringan nirkabel ad-hoc yang terdiri dari perangkat sensor berdaya rendah yang mampu mengumpulkan dan mengirimkan data secara mandiri [4]. Dalam konteks WSN, teknologi *Long Range* (LoRa) menjadi populer karena mendukung komunikasi jarak jauh dengan konsumsi daya yang sangat rendah [5]**.** Modul komunikasi LoRa E220 banyak digunakan dalam penelitian karena memiliki kestabilan yang baik dalam mentransmisikan data pada jaringan sensor [6].

Meskipun LoRa unggul dari sisi efisiensi energi dan jangkauan, sistem ini memiliki kelemahan dalam aspek keamanan, khususnya kerentanan terhadap intersepsi data (*payload interception*) selama proses transmisi [7]. Karena komunikasi LoRa terjadi pada frekuensi terbuka, pihak ketiga yang menggunakan frekuensi yang sama dapat menerima atau bahkan memodifikasi data yang dikirim. Oleh karena itu, mekanisme pengamanan data seperti kriptografi menjadi sangat penting untuk menjamin integritas dan kerahasiaan informasi yang dikirim antar node sensor [8]. Algoritma kriptografi secara umum terbagi menjadi dua jenis yaitu simetris dan asimetris. Algoritma simetris seperti Rivest Cipher 4 (RC4) menggunakan satu kunci untuk proses enkripsi dan dekripsi, sedangkan algoritma asimetris seperti Rivest Shamir Adleman (RSA) menggunakan sepasang kunci publik dan privat [9]. Masing-masing algoritma memiliki karakteristik, efisiensi, dan tingkat keamanan yang berbeda sehingga pemilihannya harus disesuaikan dengan kebutuhan dan keterbatasan sistem.

Beberapa penelitian sebelumnya telah membandingkan algoritma RSA dan RC4 dalam berbagai konteks. Yosef dkk. [10] menunjukkan bahwa RSA lebih efisien dalam enkripsi data besar, sedangkan RC4 unggul pada proses dekripsi. Penelitian oleh Wardhana dkk. [11] menunjukkan RC4 lebih cepat dan ringan dibanding AES, namun kurang tangguh terhadap serangan modern. Rezaldy dkk. [12**]** mengamati performa kedua algoritma pada platform Android dan menemukan bahwa RC4 lebih unggul dalam kecepatan, sementara RSA menawarkan keamanan lebih tinggi [13].

Berdasarkan latar belakang tersebut, artikel ini bertujuan untuk mengevaluasi dan membandingkan performansi algoritma RSA dan RC4 pada pengiriman data antar node *Wireless Sensor Network* (WSN) berbasis LoRa E220. Evaluasi dilakukan dari aspek keberhasilan enkripsi-dekripsi, efisiensi waktu proses, serta konsumsi energi masing-masing algoritma. Hasil dari kajian ini diharapkan dapat menjadi acuan dalam memilih algoritma kriptografi yang paling sesuai untuk sistem sensor dengan keterbatasan sumber daya namun tetap memerlukan keamanan komunikasi yang memadai.

Penelitian ini dibatasi pada implementasi sistem komunikasi WSN dengan skala kecil yang terdiri dari satu node pengirim, satu node penerima, dan satu node *attacker* sebagai penyadap. Algoritma kriptografi yang diuji hanya RSA dan RC4, dengan ukuran kunci RSA 512 bit dan kunci RC4 sepanjang 16 karakter. Data yang dikirim berupa hasil pembacaan sensor DHT22, sensor tegangan, dan sensor arus, yang ditransmisikan dalam format JSON melalui modul LoRa E220. Evaluasi performa difokuskan pada aspek keberhasilan enkripsi/dekripsi, waktu proses, efisiensi energi, serta ketahanan terhadap serangan *brute force*.

## 2. METODE PENELITIAN

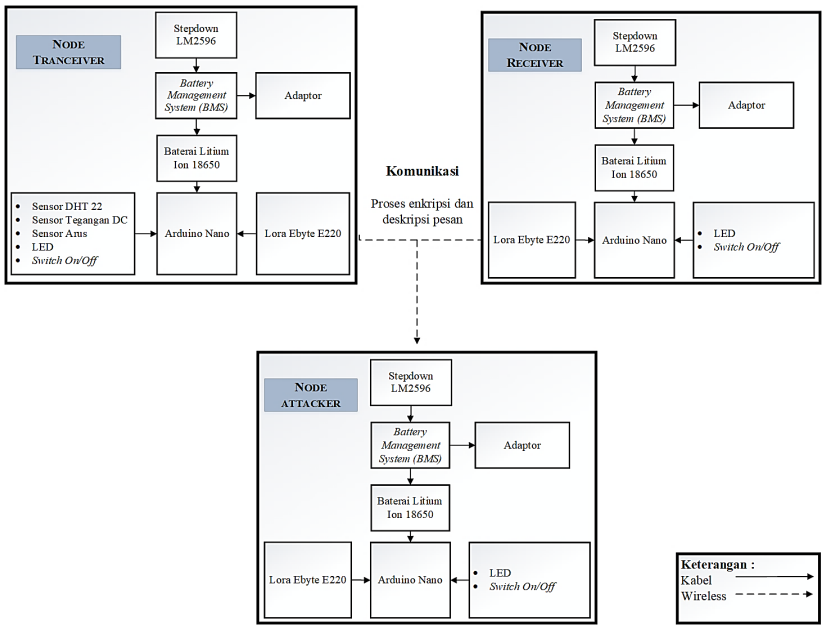
Penelitian ini menggunakan metode Research and Development (R&D) dengan tujuan mengembangkan sistem komunikasi antar-node Wireless Sensor Network (WSN) berbasis LoRa E220 yang dilengkapi algoritma kriptografi RSA dan RC4. Tahapan penelitian diawali dengan identifikasi masalah, yaitu perlunya sistem pengamanan data dalam komunikasi WSN agar tidak mudah disusupi pihak ketiga. Selanjutnya dilakukan studi literatur mengenai teknologi WSN, LoRa, serta algoritma RSA dan RC4 sebagai dasar teori. Tujuan penelitian kemudian dirumuskan untuk membandingkan performa kedua algoritma dari segi tingkat keberhasilan, waktu proses, efisiensi energi, dan aspek keamanan. Tahap perancangan sistem untuk perangkat yang digunakan meliputi Arduino Nano, LoRa E220, DHT22, ACS712, dan sensor tegangan, sesuai spesifikasi datasheet masing-masing komponen. Penentuan topologi node pengirim dan penerima, serta rancangan alur enkripsi dan dekripsi data. Implementasi dilakukan melalui pemrograman dan perakitan

perangkat sesuai rancangan. Setelah itu, sistem diuji untuk menilai fungsionalitas tiap node sekaligus mengukur ketahanan terhadap serangan brute force oleh pihak ketiga.

Data yang diakuisisi meliputi suhu (°C) dan kelembapan relatif (%RH) dari DHT22 serta tegangan dan arus dari rangkaian pembagi tegangan dan sensor ACS712. Hasil pembacaan analog (ADC 10-bit, 0–1023) dikonversi ke satuan fisik melalui kalibrasi dan offset compensation, kemudian dibulatkan hingga dua desimal [14]. Sensor dibaca secara berkala dengan interval 5 detik, lalu setiap nilai diproses menggunakan moving average filter dari 5 sampel terakhir untuk mereduksi noise sehingga data lebih stabil sebelum dikirim [15]. Untuk transmisi, field diserialisasikan dalam format JSON ringkas (contoh: {"T":"28.60","H":"67.10","V":"43.54","I":"0.151","ID":"polinema"}) dan dapat dienkripsi per-field atau sebagai payload utuh. Dalam eksperimen, enkripsi per-field lebih banyak digunakan agar hasil dekripsi tiap variabel mudah diverifikasi [16]. Waktu enkripsi dan dekripsi diukur dengan fungsi internal millis() atau micros(), sedangkan node attacker beroperasi pasif untuk menangkap ciphertext dan menjalankan skenario brute force (RC4 dengan ruang kunci terbatas dan RSA dengan variasi eksponen kecil). Hasil pengukuran dianalisis secara kuantitatif untuk membandingkan kinerja RSA dan RC4. Dari analisis ini disusun kesimpulan serta rekomendasi algoritma yang paling efisien dan aman untuk diterapkan pada jaringan WSN.

## 2.1 Blok Diagram Sistem

Pada Gambar 1 menampilkan diagram blok sistem yang dikembangkan, yang terdiri dari tiga node utama: Transceiver (pengirim), Receiver (penerima), dan Attacker (penyadap). Node Transceiver terhubung ke tiga sensor utama: sensor DHT22 untuk pengukuran suhu (°C) dan kelembapan relatif (%RH), sensor tegangan (voltage divider) untuk pengukuran tegangan DC, serta sensor arus ACS712 untuk pengukuran arus (mA). Semua node menggunakan Arduino Nano, modul LoRa E220 sebagai media komunikasi, serta catu daya berupa baterai Li-ion 18650 dan regulator step-down. Alur sistem adalah sebagai berikut: Transceiver membaca data sensor → preprocessing & kuantisasi → pembentukan payload → enkripsi (RSA atau RC4) → pengiriman via LoRa E220 → Receiver menerima ciphertext → dekripsi → konversi kembali ke nilai fisik untuk analisis. Node Attacker beroperasi pasif (sniffer) untuk menangkap payload terenkripsi dan melakukan serangan brute-force sesuai skenario pengujian.




Gambar 1. Blok Diagram Sistem

## 2.2 Sistem Kriptografi

### 2.2.1 Sistem Rivest Shamir Adleman (RSA)

Algoritma Rivest Shamir Adleman (RSA) terdiri dari tiga proses utama: pembentukan kunci, enkripsi, dan dekripsi, sebagaimana ditunjukkan pada Gambar 2. Kunci publik dan privat dibentuk dari dua bilangan prima besar ($p$ dan $q$), kemudian dihitung nilai modulus $n = p$ x $q$ dan fungsi $\varphi(n)$ yaitu $\varphi(n) = (p-1)(q-1)$. Eksponen publik e dipilih sehingga relatif prima terhadap $\varphi(n)$, sedangkan kunci privat $d$ dihitung agar memenuhi $d \times$ e = 1 mod $\varphi(n)$ [13]. Pesan asli $m$ dienkripsi menjadi ciphertext $c$ menggunakan rumus $c = m^e \ mod \ n$, dan proses dekripsi dilakukan dengan rumus $m = c^d \ mod \ n$**.** Mekanisme ini menjamin bahwa hanya pihak dengan kunci privat yang dapat mengakses data asli [14]. Alur kerja sistem RSA dalam penelitian ini

ditunjukkan pada Gambar 2. Node *Transceiver* membaca data sensor, lalu melakukan pembentukan kunci RSA dan enkripsi payload. Data yang telah dienkripsi dikirim melalui LoRa E220 ke Node *Receiver*. Setelah diterima, data diproses oleh Arduino Nano untuk didekripsi menggunakan kunci privat. Hasil dekripsi dikonversi dari bentuk ASCII ke karakter asli agar dapat ditampilkan atau dianalisis lebih lanjut [17].

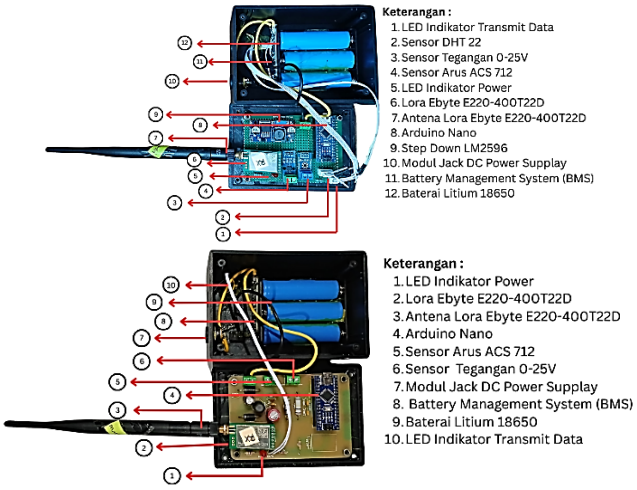
### 2.2.2 Sistem Rivest Cipher (RC4)

Pada algoritma RC4, proses diawali dengan aktivasi perangkat dan pembacaan data sensor oleh Node *Transceiver*. Data (*plaintext*) dienkripsi menggunakan RC4 melalui dua tahap utama: *Key Scheduling Algorithm* (KSA) untuk menghasilkan *state array* (S-box), dan *Pseudo-Random Generation Algorithm* (PRGA) untuk membentuk *keystream*. *Ciphertext* diperoleh melalui operasi XOR antara *plaintext* dan *keystream* [18]. Data terenkripsi dikirim melalui LoRa E220 ke Node *Receiver*. Di sisi penerima, proses dekripsi dilakukan dengan mengulang KSA dan PRGA, kemudian melakukan XOR antara *ciphertext* dan *keystream* untuk memperoleh kembali data asli. Jika dekripsi berhasil, maka data sensor ditampilkan.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Hasil Pembuatan Alat

Pada bagian ini disajikan hasil perancangan perangkat keras yang digunakan untuk implementasi algoritma kriptografi RSA dan RC4 pada jaringan *Wireless Sensor Network* (WSN). Modul LoRa E220-400T22D digunakan sebagai media komunikasi antar node, terhubung ke Arduino Nano melalui komunikasi serial (TX → D2, RX → D3). Mode komunikasi diatur ke *fixed transmission* dengan menghubungkan pin M0 dan M1 ke GND. Konfigurasi LoRa dilakukan menggunakan *software* RF_Setting (E220-RD) dengan pengaturan *Channel 25*, *Address 5*, dan fitur *Channel RSSI & Packet RSSI* diaktifkan.Sistem terdiri dari tiga node utama, yaitu Node *Transceiver* (pengirim), Node *Receiver* (penerima), dan Node *Attacker* (penyadap). Pada Gambar 4 ditunjukkan hasil perakitan Node *Transceiver*, sedangkan Gambar 4 menunjukkan Node *Receiver* dan Node *Attacker* yang telah selesai dirakit.




(a) (b) (c)

Gambar 2. (a) Node *Transceiver* (b) Node *Receiver* (c) Node *Attacker*

### 3.2 Hasil Pengujian

Tahap selanjutnya adalah pengujian kinerja sistem, yang mencakup empat aspek utama, yaitu: (1) pengujian keberhasilan enkripsi dan dekripsi, (2) pengujian waktu enkripsi dan dekripsi, (3) pengujian keamanan sistem, serta (4) pengujian penggunaan energi. Setiap aspek pengujian dibahas secara terstruktur pada subbab berikut ini untuk memberikan gambaran menyeluruh mengenai performa sistem.

### 3.2.1 Pengujian Keberhasilan Enkripsi dan Dekripsi

Pada bagian ini dilakukan pengujian ketepatan proses enkripsi dan dekripsi. Pengujian dilakukan dengan membandingkan kesesuaian antara data yang dikirim oleh Node *Transceiver* dan data yang diterima oleh Node *Receiver* setelah melalui proses enkripsi dan dekripsi. Data uji terdiri dari data sensor suhu, kelembapan, tegangan, arus, serta *string* "polinema". Hasil pengujian menunjukkan bahwa baik RSA maupun RC4 mampu melakukan proses enkripsi dan dekripsi dengan tingkat keberhasilan 100%, di mana seluruh nilai hasil dekripsi identik dengan nilai asli pada setiap iterasi. Sebagai contoh, nilai suhu 28,60 °C, kelembapan 67,10%, tegangan 43.54 mV dan arus 151 mA pada pengujian RSA, serta nilai suhu 28,60 °C, kelembapan 67,70%, tegangan 36.85 mV dan arus 150.40 mA pada pengujian RC4, seluruhnya dapat dipulihkan tanpa

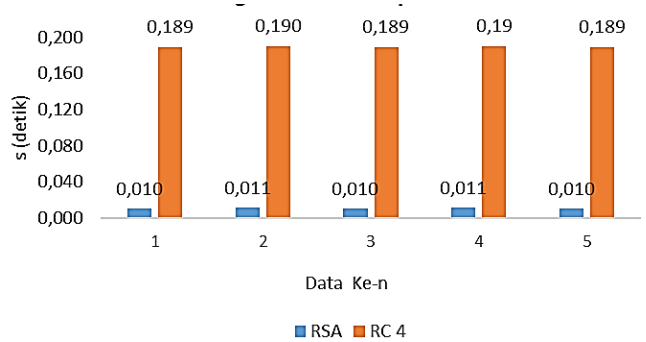
perubahan. Hal ini menunjukkan bahwa pembangkitan kunci pada RSA serta proses *Key Scheduling Algorithm* (KSA) dan *Pseudo Random Generation Algorithm* (PRGA) pada RC4 berjalan secara sinkron di kedua node.

### 3.2.2 Pengujian Waktu Enkripsi dan Dekripsi

**1) Data Sensor**

**a. Waktu Enkripsi**

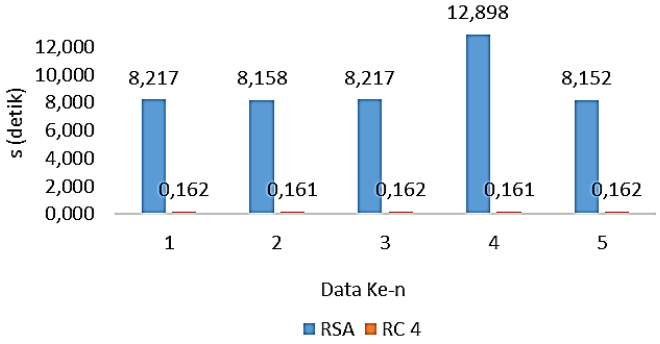
Pengujian waktu enkripsi dilakukan untuk membandingkan kinerja algoritma Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) pada sistem yang dikembangkan. Hasil pengujian menunjukkan bahwa RSA memerlukan waktu rata-rata 0,0104 detik, sedangkan RC4 membutuhkan 0,1894 detik. Pengukuran dilakukan pada Node *Transceiver* saat data sensor dibaca, kemudian dienkripsi sebelum dikirim melalui komunikasi LoRa. Dari hasil pengujian lima kali iterasi, waktu enkripsi RC4 secara konsisten lebih lama dibandingkan RSA, dengan selisih hampir 18 kali lipat. Perbedaan ini diperkirakan disebabkan oleh proses inisialisasi *Key Scheduling Algorithm* (KSA) dan *Pseudo Random Generation Algorithm* (PRGA) pada RC4 yang memerlukan iterasi per byte data, sehingga menambah *overhead*. Sebaliknya, RSA pada implementasi ini menggunakan eksponen publik berukuran kecil, sehingga operasi perkalian modular dapat berjalan lebih cepat.




Gambar 3. Grafik Perbandingan Waktu Enkripsi Kriptografi RSA dan RC 4

**b. Waktu Dekripsi**

Pengujian waktu dekripsi dilakukan untuk membandingkan performa algoritma Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) pada sistem yang dibangun. Hasil pengujian menunjukkan bahwa RSA memerlukan waktu rata-rata 9,1284 detik, sedangkan RC4 hanya membutuhkan 0,1616 detik. Pengukuran dilakukan pada Node Receiver saat menerima data terenkripsi melalui komunikasi LoRa, kemudian dilakukan proses dekripsi menggunakan kunci privat RSA atau kunci simetris RC4. Berdasarkan hasil lima kali pengujian, waktu dekripsi RSA secara konsisten lebih lama dibandingkan RC4, dengan selisih waktu yang signifikan. Waktu terlama tercatat pada pengujian keempat, yakni 12,898 detik, yang menggambarkan karakteristik kriptografi asimetris RSA. Proses dekripsi RSA memerlukan eksponen privat bernilai besar, sehingga operasi perkalian modular yang kompleks menjadi faktor utama lamanya waktu pemrosesan. Sebaliknya, RC4 menunjukkan waktu dekripsi yang singkat dan stabil di seluruh pengujian, dengan rata-rata sekitar 0,16 detik. Hal ini mencerminkan keunggulan algoritma simetris RC4 dalam hal kecepatan, karena proses dekripsi hanya melibatkan operasi XOR sederhana dengan aliran kunci yang dihasilkan secara sinkron.




Gambar 4. Grafik Perbandingan Waktu Dekripsi Kriptografi RSA dan RC 4

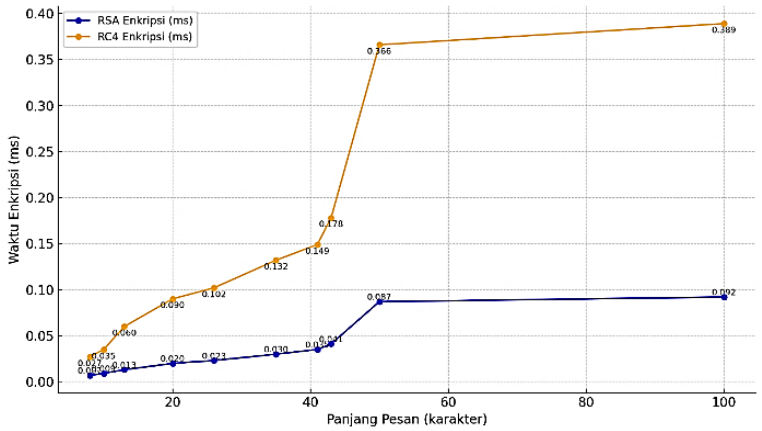
**2) Data String dengan Variasi Jumlah Karakter, Angka, dan Simbol Yang Berbeda**

**a. Waktu Enkripsi**

Pengujian pengaruh panjang pesan terhadap waktu enkripsi dilakukan untuk membandingkan performa algoritma Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4). Hasil pengujian yang

ditampilkan pada Gambar 7 menunjukkan bahwa panjang data yang dienkripsi memberikan pengaruh signifikan terhadap efisiensi kedua algoritma. Pada algoritma RC4, waktu enkripsi relatif singkat untuk pesan berukuran kecil, yaitu 0,027 ms pada panjang 8 karakter. Namun, peningkatan panjang pesan menyebabkan kenaikan waktu enkripsi yang cukup tajam, mencapai 0,389 ms pada panjang 50 karakter. Hal ini mengindikasikan bahwa RC4 menjadi kurang efisien ketika menangani data berukuran besar, karena proses Key Scheduling Algorithm (KSA) dan Pseudo Random Generation Algorithm (PRGA) harus diulang untuk setiap byte data.

Sebaliknya, algoritma RSA menunjukkan tren peningkatan waktu enkripsi yang lebih stabil. Pada pesan sepanjang 8 karakter, waktu enkripsi tercatat 0,007 ms, dan hanya meningkat menjadi 0,092 ms pada panjang 100 karakter. Meskipun RSA merupakan kriptografi asimetris yang secara umum membutuhkan komputasi lebih kompleks, hasil ini memperlihatkan bahwa RSA lebih konsisten dalam mempertahankan kestabilan waktu enkripsi terhadap variasi panjang pesan dibandingkan RC4.

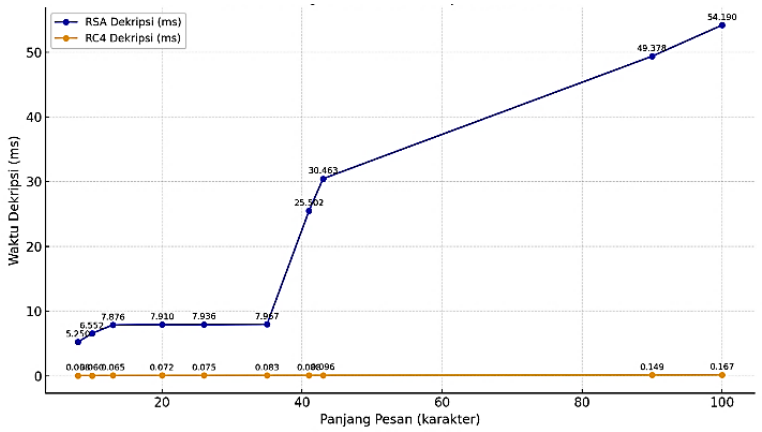



Gambar 5. Grafik Perbandingan Waktu Enkripsi Kriptografi RSA dan RC 4 Berdasarkan Panjang Pesan

**b. Waktu Dekripsi**

Pengujian pengaruh panjang pesan terhadap waktu dekripsi dilakukan untuk mengevaluasi kinerja algoritma Rivest Cipher 4 (RC4) dan Rivest Shamir Adleman (RSA) pada proses penerimaan data. Hasil pengujian yang divisualisasikan dalam grafik menunjukkan bahwa RC4 memiliki performa dekripsi yang jauh lebih cepat dan stabil dibandingkan RSA. Sebagai algoritma kriptografi simetris, RC4 menunjukkan waktu dekripsi yang konsisten rendah pada berbagai panjang pesan. Nilai waktu dekripsi tercatat mulai dari 0,058 ms untuk pesan sepanjang 8 karakter, dan hanya meningkat menjadi sekitar 0,167 ms pada pesan 100 karakter. Konsistensi ini mengindikasikan efisiensi RC4 dalam menangani proses dekripsi, bahkan pada ukuran data yang lebih besar, berkat mekanisme operasi XOR yang sederhana dan efisien terhadap aliran data.

Sebaliknya, RSA yang merupakan kriptografi asimetris memperlihatkan peningkatan waktu dekripsi yang signifikan seiring bertambahnya panjang pesan. Waktu dekripsi meningkat dari 5,250 ms pada pesan 8 karakter hingga mencapai 54,190 ms pada pesan 100 karakter. Lonjakan waktu ini mencerminkan kompleksitas tinggi pada proses dekripsi RSA, yang melibatkan perhitungan eksponensial modular dengan kunci privat berukuran besar.




Gambar 6. Grafik Perbandingan Waktu Dekripsi Kriptografi RSA dan RC 4 Berdasarkan Panjang Pesan

### 3.2.3 Pengujian Keamanan Sistem

#### 1) Rivest Shamir Adleman (RSA)

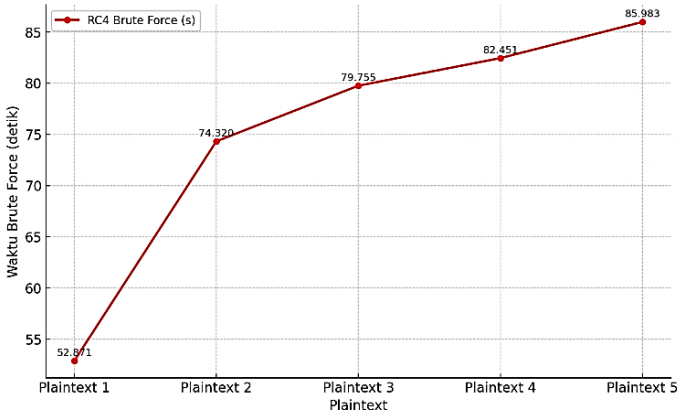
Pengujian keamanan menggunakan metode *brute force* pada algoritma Rivest Shamir Adleman (RSA) dilakukan untuk mengevaluasi ketahanan sistem terhadap upaya pembobolan kunci secara paksa. Pengujian ini melibatkan Node *Attacker* yang mencoba melakukan dekripsi ciphertext dengan berbagai nilai eksponen privat (*private exponent*, d) secara berulang hingga ditemukan *plaintext* yang sesuai. Berbeda dengan algoritma simetris seperti RC4 yang menggunakan satu kunci rahasia, RSA memanfaatkan pasangan kunci publik–privat yang dibangun dari bilangan prima besar. Kompleksitas matematis pada proses dekripsi RSA sangat bergantung pada ukuran kunci, sehingga metode *brute force* memerlukan pencarian pada ruang kunci yang sangat luas.

Hasil pengujian yang ditunjukkan pada Gambar 9 memperlihatkan bahwa seluruh percobaan *brute force* menghasilkan status gagal, tanpa satu pun nilai d yang benar ditemukan selama periode pengujian. Waktu yang dibutuhkan untuk setiap percobaan berkisar antara 952,871 detik hingga 1001,652 detik, dengan kecenderungan meningkat seiring variasi pesan yang diuji. Peningkatan ini disebabkan oleh bertambahnya jumlah iterasi dan tingginya kompleksitas perhitungan modular pada proses dekripsi.


Gambar 7. Grafik Hasil Pengujian *Brute Force* RSA terhadap Pesan Terenkripsi dan Variasi Kunci

#### 2) Rivest Cipher 4 (RC 4)

Pengujian keamanan terhadap algoritma Rivest Cipher 4 (RC4) dilakukan menggunakan metode *brute force* dengan pendekatan pencocokan kunci secara sistematis. Pada metode ini, sistem mencoba seluruh kemungkinan kunci hingga menemukan kombinasi yang menghasilkan *plaintext* identik dengan pesan asli. Berbeda dengan RSA yang memiliki ruang kunci sangat besar dan membutuhkan perhitungan matematis kompleks, RC4 memiliki ruang kunci yang relatif lebih kecil sehingga proses pencarian kunci dapat dilakukan dengan waktu yang jauh lebih singkat. Berdasarkan hasil pada Gambar 10, waktu rata-rata yang dibutuhkan untuk menemukan kunci RC4 berada pada kisaran 52,871 detik hingga 85,983 detik. Terlihat adanya tren kenaikan waktu *brute force* seiring bertambahnya variasi *plaintext* yang diuji. Faktor yang memengaruhi kenaikan ini antara lain jumlah karakter pada kunci serta kompleksitas pencocokan selama proses dekripsi.



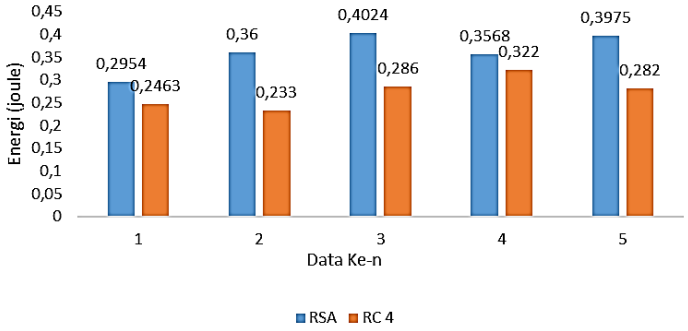

Gambar 8. Grafik Hasil Pengujian *Brute Force* RC 4 terhadap Pesan Terenkripsi dan Variasi Kunci

Seluruh percobaan *brute force* pada RC4 berhasil menemukan kunci dan mendekripsi pesan dengan benar. Hasil ini menunjukkan bahwa, pada implementasi dengan panjang kunci terbatas, RC4 memiliki

ketahanan yang rendah terhadap serangan *brute force*. Oleh karena itu, tingkat keamanan RC4 sangat bergantung pada panjang dan kerandoman kunci yang digunakan. Semakin panjang dan acak kunci, semakin besar pula ruang kunci yang harus dieksplorasi, sehingga waktu *brute force* meningkat signifikan. Namun, pada pengujian ini, dengan panjang kunci yang terbatas, penyerang masih mampu menemukan kunci dalam rentang puluhan detik menggunakan perangkat komputasi standar.

### 3.2.4 Pengujian Penggunaan Energi

Pengujian ini mengevaluasi pengaruh algoritma RSA dan RC4 terhadap konsumsi energi perangkat. Eksperimen dilakukan dengan mengukur konsumsi energi saat masing-masing algoritma dijalankan menggunakan 3 baterai Li-Ion 18650 (2200 mAh) paralel. Rata-rata waktu enkripsi dan dekripsi RSA mencapai ±9 detik per iterasi, dengan konsumsi energi 0.3568–0.4024 joule dan perubahan kapasitas baterai 0.0027–0.0036 Ah. Beban komputasi tinggi RSA menyebabkan penggunaan energi lebih besar, meskipun tegangan relatif stabil. Hal ini menunjukkan RSA kurang efisien untuk perangkat IoT yang sensitif terhadap konsumsi daya. Sedangkan RC4 (Rivest Cipher 4) waktu proses sangat singkat, hanya ±0.028 detik per iterasi, dengan konsumsi energi 0.2330–0.3220 joule dan perubahan kapasitas baterai 0.0191–0.0264 Ah. Meskipun arus lebih tinggi karena proses cepat, total energi tetap lebih rendah dibanding RSA. Ini menjadikan RC4 lebih hemat energi dan cocok untuk aplikasi yang mengutamakan efisiensi daya.




Gambar 9. Grafik Perbandingan Konsumsi Energi RSA dan RC 4 pada Setiap Pengiriman Data

Bagian ini memaparkan perbandingan antara hasil pengujian yang diperoleh dengan harapan penulis terhadap performa sistem yang dirancang.

Tabel 1. Hasil Pengujian Sistem Kriptografi RSA dan RC4

| Kegiatan | Hasil yang diharapkan | Hasil pengujian | Hasil | |
|---|---|---|---|---|
| | | | Berhasil | Tidak Berhasil |
| Keberhasilan pengiriman dan penerimaan pesan terenkripsi | Pesan terenkripsi dapat dikirim oleh node pengirim dan diterima oleh node penerima, kemudian berhasil didekripsi menjadi pesan asli | RSA dan RC4 berhasil mengirim dan menerima data sensor serta string, seluruh hasil dekripsi identik dengan data asli | 5 pengujian (RC4)<br>5 pengujian (RSA) | - |
| Waktu enkripsi data sensor | Waktu enkripsi yang cepat pada kedua algoritma kriptografi | Rata-rata waktu enkripsi RSA: 0,0104 s; RC4: 0,1894 s | 5 pengujian (RC4)<br>5 pengujian (RSA) | - |
| Waktu dekripsi data sensor | Waktu dekripsi yang cepat pada kedua algoritma kriptografi | Rata-rata waktu dekripsi RC4: 0,1616 s; RSA: 9,1284 s (lebih dari target) | 5 pengujian (RC4)<br>5 pengujian (RSA) | - |
| Waktu enkripsi data string dengan variasi jumlah karakter, angka, dan simbol yang berbeda | Waktu enkripsi yang cepat pada kedua algoritma kriptografi | RC4: 0,027 ms (8 karakter) → 0,389 ms (100 karakter). RSA: 0,007 ms (8 karakter) → 0,092 ms (100 karakter). RSA lebih stabil, RC4 cenderung meningkat pada data panjang | 5 pengujian (RC4)<br>5 pengujian (RSA) | - |

| Kegiatan | Hasil yang diharapkan | Hasil pengujian | Hasil | |
|---|---|---|---|---|
| | | | Berhasil | Tidak Berhasil |
| Waktu dekripsi data string dengan variasi jumlah karakter, | Waktu dekripsi yang cepat pada kedua algoritma kriptografi | RC4: 0,058 ms (8 karakter) → 0,167 ms (100 karakter). RSA: 5,250 ms (8 karakter) → | 5 pengujian (RC4) | - |
| angka, dan simbol yang berbeda | | 54,190 ms (100 karakter). RC4 jauh lebih cepat dan stabil dibanding RSA | 5 pengujian (RSA) | |
| Keamanan terhadap brute force (RSA) | Tidak dapat ditemukan kunci privat selama waktu pengujian | Semua percobaan brute force RSA gagal menemukan kunci (waktu 952,871 – 1001,652 s) | 5 pengujian | - |
| Keamanan terhadap brute force (RC4) | Mampu menolak intrusi kunci salah | Semua percobaan brute force RC4 berhasil menemukan kunci (waktu 52,871 – 85,983 s) | - | 5 pengujian |
| Efisiensi konsumsi energi | Konsumsi energi rendah untuk pengiriman data | Konsumsi energi RC4: 0,233 – 0,322 J; RSA: 0,2954 – 0,4024J | 5 pengujian (RC4)<br>5 pengujian (RSA) | - |

## 4. KESIMPULAN

Penelitian ini mengimplementasikan algoritma kriptografi RSA dan RC4 pada jaringan *Wireless Sensor Network* (WSN) menggunakan modul LoRa E220-400T22D sebagai media komunikasi antar node. Sistem terdiri dari tiga node utama, yaitu Node *Transceiver* sebagai pengirim data, Node *Receiver* sebagai penerima data, dan Node *Attacker* sebagai penyadap untuk serangan *brute force*.

Pengujian data yang dilakukan ada 2 yaitu data sensor yang terdiri dari suhu, kelembapan, tegangan, arus, serta string identitas "polinema" dan data string dengan variasi jumlah karakter, angka, dan simbol yang berbeda. Hasil pengujian menunjukkan bahwa kedua algoritma mampu melakukan proses enkripsi dan dekripsi secara utuh dengan tingkat keberhasilan 100% pada seluruh iterasi. Dari sisi kinerja, RSA memiliki waktu enkripsi lebih cepat (0,0104 detik) dibanding RC4 (0,1894 detik), namun jauh lebih lambat pada proses dekripsi (9,1284 detik) dibanding RC4 yang hanya memerlukan 0,1616 detik. Pada pengujian variasi panjang pesan, RC4 menunjukkan stabilitas dekripsi yang baik meskipun waktu enkripsi meningkat pada pesan di atas 40 karakter, sedangkan RSA mengalami lonjakan signifikan pada waktu dekripsi untuk pesan panjang.

Dari aspek keamanan, RC4 dengan kunci pendek berhasil diretas melalui brute force dalam rentang 52,871–85,983 detik (±0,88–1,43 menit), sedangkan seluruh upaya *brute force* terhadap RSA gagal menemukan kunci privat meskipun waktu pengujian mencapai 952,871–1001,652 detik (±15 16 menit). Hal ini membuktikan bahwa RSA memiliki ketahanan yang tinggi terhadap serangan brute force berkat ruang kunci yang sangat besar. Dari sisi konsumsi energi, RSA membutuhkan daya lebih besar (0,2954–0,4024 joule per siklus) dibanding RC4 (0,233–0,322 joule per siklus) akibat waktu proses yang lebih panjang.

Dengan demikian, RSA lebih unggul untuk sistem yang mengutamakan keamanan tinggi dan kecepatan enkripsi, sementara RC4 lebih sesuai untuk aplikasi yang memprioritaskan kecepatan dekripsi dan efisiensi energi pada perangkat dengan keterbatasan daya, seperti node sensor berbasis *Wireless Sensor Network* (WSN).

## 5. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Politeknik Negeri Malang, Jurusan Teknik Elektro atas dukungan fasilitas penelitian, serta kepada pihak-pihak yang turut membantu dalam proses perancangan dan pengujian sistem.

## 6. DAFTAR PUSTAKA

[1] N. Noprianto, R. F. Pratama, H. E. Dien, M. H. Ratsanjani, dan M. A. Hendrawan, "Pengembangan Mesh Network Sebagai Ekspansi Protokol LoRaWAN di Politeknik Negeri Malang," *JTIM : Jurnal Teknologi*
[2] *Informasi dan Multimedia*, vol. 6, no. 3, pp. 296–306, Okt. 2024.
[3] F. Hamid, E. Ratuloli, A. Setia Budi, dan A. Bhawiyuga, "Implementasi Skema Anti Collision Menggunakan Metode TDMA dan TPSN pada Sistem WSN Berbasis LoRa," *J-PTIIK : Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 5, no.1, pp. 283-290, Jan. 2021.
[4] N. H. Motlagh, M. Mohammadrezaei, J. Hunt, dan B. Zakeri, "Internet of things (IoT) and the energy sector," *Energies*, vol. 13, no. 2, pp. 494, Jan. 2020.

[5] K. K. Bhardwaj, A. Khanna, D. K. Sharma, dan A. Chhabra, "Designing Energy Efficient IoT Based Intelligent Transport System: Need, Architecture, Characteristics, Challenges, and Applications," Springer, vol. 206, pp. 209–233. Mei. 2019.

[6] H. Andre, B. A. Sugara, B. Baharuddin, R. Fernandez, dan R. W. Pratama, "Analisis Komunikasi Data Jaringan Nirkabel Berdaya Rendah Menggunakan Teknologi Long Range (LoRa) di Daerah Hijau Universitas

[7] Andalas," *Jurnal Ecotipe (Electronic, Control, Telecommunication, Information, and Power Engineering)*, vol. 9, no. 1, pp. 1–7, Okt. 2021.

[8] F. Muhammad, A. Bhawiyuga, dan D. P. Kartikasari, "Analisis Kinerja Protokol LoRaWAN untuk Transmisi Data pada Skenario Urban Area," *J-PTIIK : Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no.9, pp. 9054-9060, Sept. 2019.

[9] R. I. . Lestari, V. Suryani, dan A. A. Wardhana, "Digital Signature Method to Overcome Sniffing Attacks on LoRaWAN Network", *IJECES*, vol. 13, no. 7, pp. 533-539, Sept. 2022.

[10] Y. Adrian, C. Friscilla, N. Suardiman, A. Wijaya, dan Sudimanto, "Analisis Perbandingan Waktu Enkripsi dan Dekripsi Pada Algoritma ECC dan RSA," *Media Informatika*, vol.21, no.2, pp. 124-132, Okt. 2022.

[11] Suroso, "Studi Perbandingan Kriptograpi Menggunakan Metode DES, Triple DES Dan RSA," *SIGMA – Jurnal Teknologi Pelita Bangsa*, vol. 8, no. 1, Mar. 2018.

[12] Z. Arif dan A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi," *JTSI : Jurnal Teknologi Sistem Informasi*, vol. 4, no.2, pp.294-406, Sept. 2023.

[13] M. A. Bhaskara, M. P. A. Ariawan, I. B. A. Peling, dan I. P. A. Prayudha, "Studi Literatur: Analisa Perbandingan Teori Tentang Tingkat Keamanan Antar Algoritma Simetris," *Jurnal Bangkit Indonesia*, vol. 13, no. 1, pp. 40-45, Mar. 2024.

[14] H. Aspriyono, N. Saputra, dan E. P. Rohmawan, "Penerapan Wireless Sensor Network Untuk Deteksi Suhu, Kelembapan dan Gas Amonia Pada Kandang Sapi," *Jurnal Amplifier : Jurnal Ilmiah Bidang Teknik Elektro dan Komputer*, vol. 14, no. 1, pp. 89–94, Mei. 2024.

[15] Rahayu, A. P. Ardana, C. Pramudhita, D. Syafitri, dan R. Z. Sirega, "Perbandingan Algoritma RSA dengan Algoritma Blowfish Pada Perancangan Aplikasi Keamanan Data," *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, vol. 7, no. 1, pp. 203–207, Feb. 2024.

[16] M. R. D. Kasili, H. Dalai, W. Yunus, dan Zohrahatay, "Perbandingan Kinerja Algoritma RSA dan Algoritma RC4 dalam Mengenkripsi dan Dekripsi Data File Berbasis Android," *Jurnal Ilmiah Ilmu Komputer Banthayo Lo Komputer*, vol. 4, no. 1, pp. 51–57, 2025.

[17] F. K. Wardhana, A. Kurniawan, B. R. Seto, dan I. A. Saputro, "Analisis Perbandingan Kinerja Enkripsi Algoritma RC4 dan AES," *Seminar Nasional AMIKOM Surakarta (SEMNASA)*, pp. 124–134, Nov. 2023.

[18] A. Seputra dan G. A. J. Saskara, "Kriptografi simetris RC4 pada transaksi online booking engine system," *Jurnal Pendidikan Teknologi dan Kejuruan*, vol. 17, no. 2, pp. 286–295, Jul. 2020.