# Perancangan Sistem Keamanan Komunikasi Data pada Jaringan LoRA Menggunakan Algoritme PRESENT

Eka Hero Ramadhani[#1], Asri Wulandari[#2], Alfin Hikmaturokhman*[3]

[#]*Program Studi Teknik Elektro, Politeknik Negeri Jakarta*
*Jl. Prof. DR. G.A. Siwabessy, Kampus Universitas Indonesia, Depok, Indonesia*
[1]eka.hero.ramadhani.te23@stu.pnj.ac.id
[2]asri.wulandari@elektro.pnj.ac.id

[#]*Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara*
*Jl. Raya H. Usa, Putat Nutug, Ciseeng, Bogor, Indonesia*
[1]eka.hero@poltekssn.ac.id

**Department of Electrical Engineering, Telkom University*
*Jl. DI Panjaitan No.128, Karangreja, Purwokerto, Indonesia*
[3]alfinh@telkomuniversity.ac.id

***Abstract*— *LoRa is a low-power wireless communication technology capable of transmitting data over long distances. LoRa is widely used in embedded systems and the Internet of Things (IoT) in various sectors, such as agriculture, fisheries, industry, transportation, and smart cities. However, the data transmitted through LoRa is not encrypted, so the confidentiality of the data is not guaranteed because the data can be intercepted and read by hackers at the same frequency. Therefore, data encryption techniques are needed in the LoRa system to maintain data confidentiality when transmitted. In this research, a LoRa system is designed, and an analysis of the lightweight PRESENT block cipher algorithm is carried out to secure data communication on the LoRa system. This research uses a LoRa RFM95W module with a 915 MHz frequency and an ATmega328P microcontroller. This research method consists of the stages of literature study, design, implementation, testing, and analysis. After the design and implementation stages, the LoRa system was tested with data transmission test scenarios with test vectors and data communication interception tests. This research shows that the PRESENT algorithm was successfully implemented on the LoRa communication system, and hackers could not read the data sent from LoRa Tx and Rx. The test results also show that implementing the PRESENT algorithm on the LoRa system does not affect data communication performance based on RSSI values. The results of this research can be used in further research in various fields, such as IoT security in agriculture, fisheries, transportation, industry, and smart cities.***

***Keywords*— *PRESENT algorithm, LoRa, RFM95W, ATmega328P, data communications security***

***Abstrak*— LoRa merupakan teknologi komunikasi nirkabel yang berdaya rendah dan mampu mentransmisikan data jarak jauh. Saat ini LoRa banyak digunakan pada sistem tertanam dan *Internet of Things* (IoT) di berbagai sektor, seperti bidang pertanian, perikanan, industri, transportasi, dan kota pintar. Namun, data yang dikirimkan melalui LoRa tidak terenkripsi sehingga kerahasiaan data tidak terjamin keamanannya karena data dapat disadap dan dibaca oleh peretas pada frekuensi yang sama. Oleh sebab itu, perlu teknik enkripsi data pada sistem LoRa untuk menjaga kerahasiaan data saat ditransmisikan. Pada penelitian ini dirancang sistem LoRa dan dilakukan analisis algoritme PRESENT *block cipher* ringan untuk mengamankan komunikasi data pada sistem LoRa. Pada penelitian ini digunakan modul LoRa RFM95W frekuensi 915 MHz dan mikrokontroler ATmega328P. Metode penelitian ini terdiri dari tahapan studi literatur, desain, implementasi, pengujian, dan analisis. Setelah tahap desain dan implementasi, dilakukan pengujian terhadap sistem LoRa dengan skenario uji transmisi data dengan vektor uji dan uji penyadapan komunikasi data. Hasil penelitian ini menunjukkan bahwa algoritme PRESENT berhasil diimplementasikan pada sistem komunikasi LoRa dan data yang dikirimkan dari LoRa Tx dan Rx tidak dapat dibaca oleh peretas. Hasil uji juga menunjukkan bahwa implementasi algoritme PRESENT pada sistem LoRa tidak memengaruhi performa komunikasi data berdasarkan nilai RSSI. Hasil penelitian ini dapat digunakan pada penelitian selanjutnya untuk berbagai bidang, misalnya untuk keamanan IoT pada pertanian, perikanan, transportasi, industri, dan kota pintar.***

***Kata Kunci*— algoritme PRESENT, LoRa, RFM95W, ATmega328P, keamanan komunikasi data**

## I. PENDAHULUAN

LoRa sebagai konektivitas nirkabel rendah daya saat ini populer dikembangkan dan dioperasikan pada sistem tertanam [1]. LoRa merupakan teknologi komunikasi nirkabel modern yang dapat berkomunikasi jarak jauh dengan konsumsi daya yang rendah [2]. LoRa dapat mentransmisikan data hingga jarak 3 Km pada *Free Space Path Loss* (FSPL) [3]. LoRa mampu mengirimkan data hingga jarak 15 Km dalam kondisi *Line of Sight* (LOS) [4]. LoRa adalah teknologi lapisan fisik jaringan yang menggunakan modulasi *Chirp Spread Spectrum* (CSS) dengan frekuensi 915, 868, dan 433 MHz [5]. Saat ini LoRa telah banyak digunakan di berbagai bidang, seperti pertanian [6], [7]; perikanan [8]; industri [9]; transportasi [10], [11]; kota pintar [12]; dan pada IoT [13]. Namun, LoRa memiliki kerentanan keamanan pada transmisi data yang memungkinkan data dapat disadap oleh pihak yang tidak berkepentingan di frekuensi yang sama [14]. Hal itu disebabkan karena data yang dikirimkan melalui LoRa tidak

terenkripsi sehingga dapat disadap dan dibaca oleh peretas [15]. Oleh karena itu, penting untuk menerapkan kriptografi berupa teknik enkripsi pada sistem LoRa guna mengamankan kerahasiaan data saat ditransmisikan.

*Advanced Encryption Standard* (AES) adalah algoritme kriptografi standar yang diterbitkan oleh *National Institute of Standards and Technology* (NIST) untuk enkripsi data [16]. AES merupakan *block cipher* yang telah diimplementasikan dan diteliti oleh Amelia dan Fahmi untuk mengamankan transmisi data pada sistem LoRa [17]. Hasil penelitian Windya dkk. menunjukkan bahwa AES dapat mengamankan kerahasiaan data yang dikirimkan melalui LoRa [18], namun AES memiliki kompleksitas komputasi yang besar dan konsumsi daya yang tinggi berdasarkan hasil penelitian dari Zhang dkk. [19], sedangkan rangkaian sistem LoRa biasanya merupakan perangkat keras dengan sumber daya komputasi yang terbatas, misalnya sistem LoRa dengan mikrokontroler ATmega328P. ATmega328P adalah mikrokontroler 8-bit berdaya rendah [20]. Oleh sebab itu, perlu algoritme kriptografi yang ringan (*lightweight*) untuk dapat diterapkan pada perangkat keras rangkaian sistem LoRa yang memiliki sumber daya komputasi rendah dan terbatas seperti rangkaian sistem LoRa dengan mikrokontroler ATmega328P.

PRESENT merupakan algoritme kriptografi *block cipher* ultra ringan yang distandarkan dalam ISO/IEC 29192-2:2019 [21]. Algoritme PRESENT memiliki kinerja yang lebih baik dibandingkan AES pada perangkat keras dengan sumber daya komputasi rendah [22]. Dalam penelitian ini akan dilakukan desain, implementasi, dan analisis algoritme PRESENT pada sistem LoRa dengan mikrokontroler ATmega328P dan modul LoRa RFM95W di frekuensi 915 MHz untuk mengamankan komunikasi data pada LoRa. Kemudian menganalisis hasil implementasi dengan pengujian vektor uji dan uji sadap pada rangkaian sistem komunikasi LoRa sebelum dan sesudah diimplementasikan algoritme PRESENT.

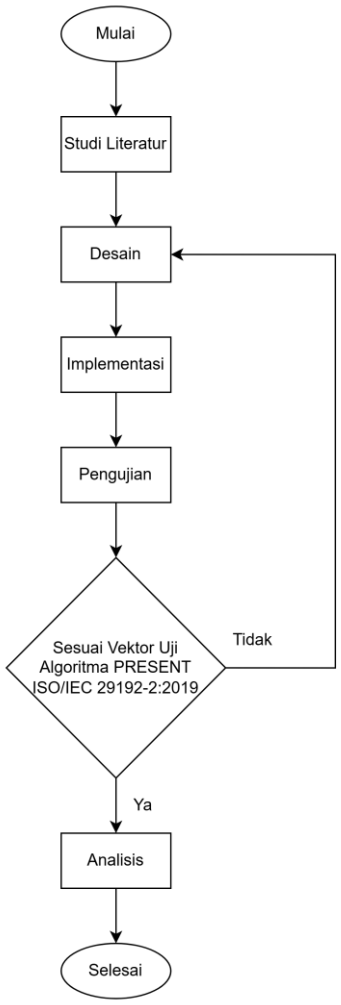
## II. METODOLOGI

Metode penelitian menjelaskan secara rinci tahapan bagaimana memulai, melakukan, dan menyelesaikan penelitian [23]. Metode penelitian dalam penelitian ini terdiri dari tahapan studi literatur, desain, implementasi, pengujian, dan analisis. Diagram tahapan penelitian ini disajikan pada Gambar 1.

### *A. Studi Literatur*

Pada tahap studi literatur, dilakukan pencarian literatur terkait LoRa, algoritme kriptografi, dan implementasi pemrograman pada mikrokontroler. Pada penelitian ini kami menggunakan modul LoRa RFM95W dan mikrokontroler ATmega328P. Penelitian ini fokus mempelajari algoritme PRESENT untuk mengamankan komunikasi data pada LoRa RFM95W dengan mikrokontroler ATmega328P.

RFM95W merupakan modul LoRa yang dipatenkan oleh Hope RF dengan menggunakan teknik modulasi LoRa TM yang tahan interferensi, komunikasi spektrum jarak jauh dengan sensitivitas lebih dari -148 dBm, dan konsumsi daya rendah [24]. Modul RFM95W LoRa mendukung mode modulasi standar, seperti *Frequency Shift Keying* (FSK), *Gaussian Frequency Shift Keying* (GFSK), *Gaussian Minimum Shift Keying* (GMSK), dan *On Off Keying* (OOK) sehingga memungkinkan untuk kompatibel dengan sistem atau standar seperti WMBus dan IEEE 802.15 .4g. *Bandwidth* LoRa RFM95W adalah 7,8–500 kHz dengan rentang frekuensi 868–915 MHz. Panjang *payload* modul LoRa RFM95W adalah 64 byte. Papan sirkuit modul LoRa RFM95W ditunjukkan pada Gambar 2 dan struktur paket modulasi LoRa TM disajikan pada Gambar 3.



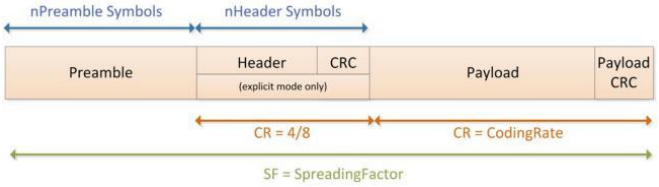

Gambar 1 Diagram tahapan penelitian

Gambar 2 Papan sirkuit modul LoRa RFM95W [24]

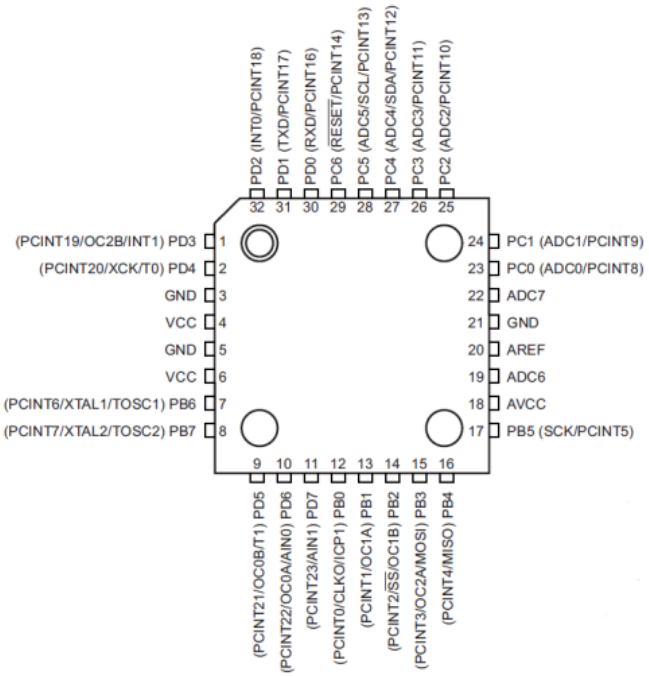
ATmega328P merupakan mikrokontroler *Complementary Metal Oxide Semiconductor* (CMOS) 8-bit berdaya rendah dengan arsitektur *Advanced Virtual RISC* (AVR) [20].

Terdapat 32 KB memori program yang dapat diprogram dalam sistem, 2 KB SRAM internal, 1 KB EEPROM, dan 10.000 flash/100.000 siklus tulis/hapus EEPROM. Pada mikrokontroler ATmega328P terdapat 23 jalur I/O yang dapat diprogram, 32 lead TQFP, dan 32 pad QFN/MLF. Konfigurasi pin *Integrated Circuit* (IC) mikrokontroler ATmega328P disajikan pada Gambar 4. Tegangan operasi ATmega328P adalah 2,7–5,5 V. Konsumsi daya ATmega328P rendah yaitu 1,5 mA pada 3V. ATmega328P mengeksekusi instruksi dalam satu siklus *clock*, sehingga dapat mencapai *throughput* mendekati 1 MIPS per MHz, memungkinkan perancang sistem untuk mengoptimalkan konsumsi daya versus kecepatan pemrosesan. Terdapat 32 x 8 register untuk keperluan performa umum, dan memiliki *throughput* hingga 16 MIPS pada 16 MHz.

ATmega328P dapat ditemukan dan diprogram pada Arduino Nano. Mikrokontroler inti Arduino Nano adalah ATmega328P yang memiliki *clock* pada frekuensi 16 MHz dengan 20 pin I/O digital, 8 pin analog, dan *port* Mini USB [25]. Papan Arduino Nano ditunjukkan pada Gambar 5.




Gambar 3 Struktur paket modulasi LoRaiee TM [24]

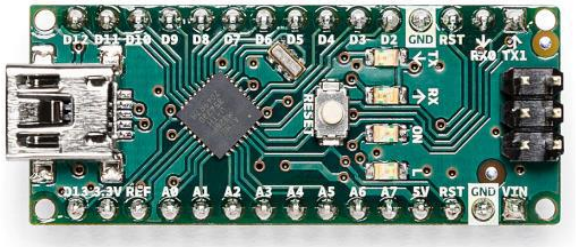



Gambar 4 Konfigurasi pin IC mikrokontroler ATmega328P [20]

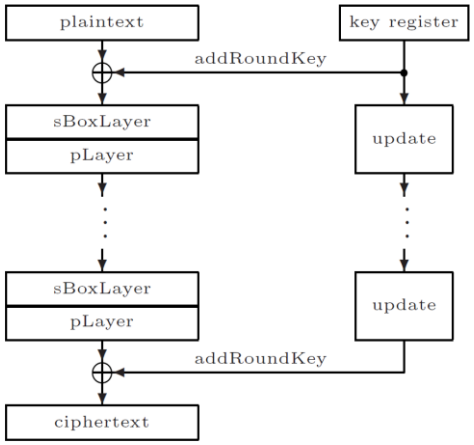
Algoritme PRESENT merupakan *block cipher* yang ringan dengan spesifikasi ukuran blok pemrosesan 64-bit dan panjang ukuran kunci 80 atau 128 bit [21]. PRESENT merupakan algoritme kriptografi dengan menggunakan teknik *Substitution Permutation Network* (SPN) dengan 31 putaran [26]. Implementasi PRESENT memerlukan 32 siklus *clock* untuk mengenkripsi teks biasa 64-bit dengan kunci 80-bit, menggunakan 1570 *Gate Equivalents* (GE), dan memiliki konsumsi daya simulasi sebesar 5µW. Skema algoritme PRESENT disajikan pada Gambar 6 dan skema operasi SPN disajikan pada Gambar 7. Vektor uji untuk memastikan implementasi algoritme PRESENT benar dengan kunci 80-bit dalam notasi heksadesimal disajikan pada Tabel I.

## *B. Desain*

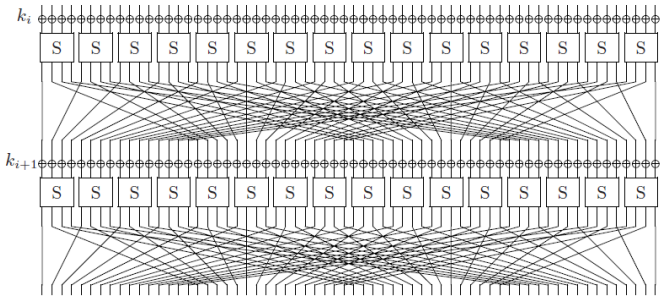
Setelah memperoleh pengetahuan dari tahap studi literatur, tahapan desain penelitian ini dikerjakan yang terdiri dari kegiatan menentukan ruang lingkup penelitian, menyiapkan perangkat keras dan perangkat lunak yang diperlukan, meran-




Gambar 5 Papan Arduino Nano dengan mikrokontroler ATmega328P [25]




Gambar 6 Skema algoritme PRESENT [26]




Gambar 7 Skema operasi SPN [26]

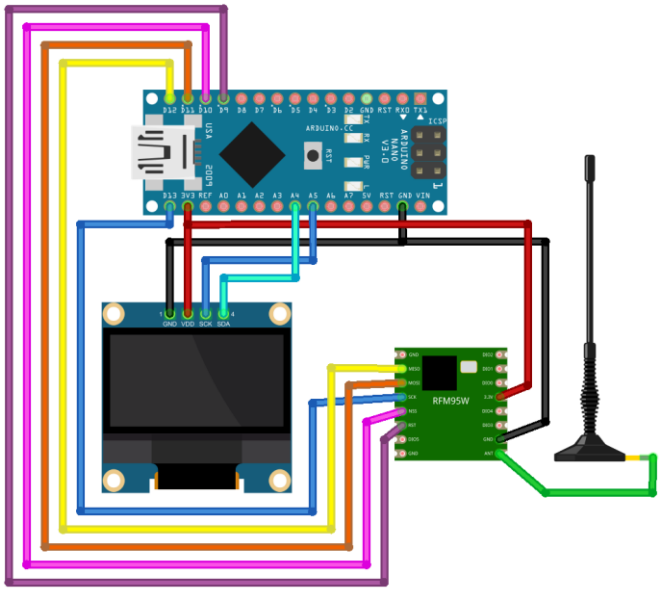
cang perakitan perangkat keras, dan merancang implementasi program. Ruang lingkup penelitian ini adalah mendesain implementasi algoritme PRESENT untuk mengamankan komunikasi LoRa pada frekuensi 915 MHz dan menganalisis keamanan komunikasi data pada LoRa yang telah diimplementasikan algoritme PRESENT. Perangkat keras yang digunakan berupa seperangkat komputer untuk pemrograman mikrokontroler, modul LoRa RFM95W, Arduino Nano dengan mikrokontroler ATmega328P, kabel Mini USB, modul OLED, *Breadboard*, dan kabel *jumper*. Desain rangkaian perangkat keras ditunjukkan pada Gambar 8. Perangkat lunak yang digunakan adalah Fritzing untuk merancang diagram rangkaian dan Arduino IDE untuk menyusun program ke dalam mikrokontroler. Bahasa pemrograman yang digunakan untuk implementasi dalam penelitian ini menggunakan C++. Setelah program ditulis dalam skrip menggunakan bahasa C++, kemudian dikompilasi pada mikrokontroler menggunakan Arduino IDE. Diagram alir desain implementasi program disajikan pada Gambar 9.

### *C. Implementasi*

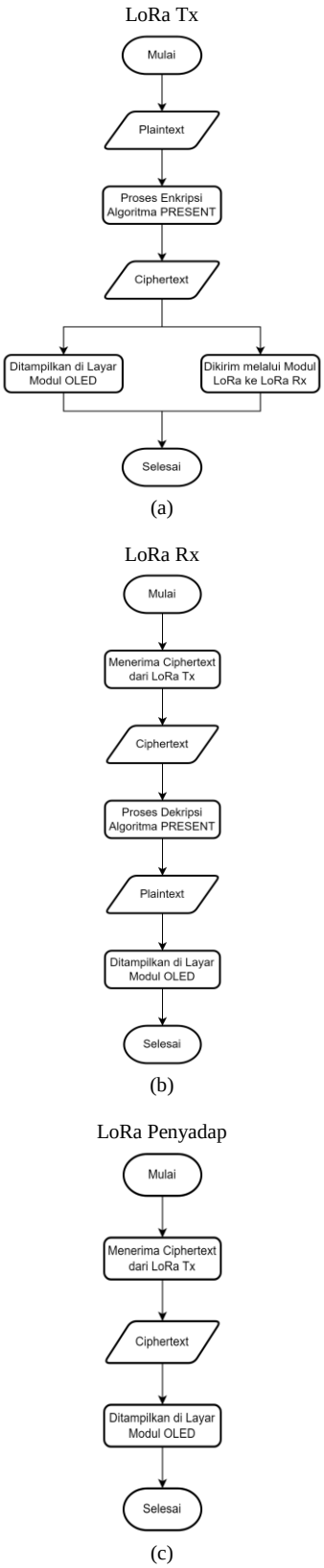
Tahapan implementasi terdiri dari perakitan perangkat keras, penulisan sketsa skrip kode program, dan kompilasi program ke dalam mikrokontroler. Implementasi sesuai de-

TABEL I
VEKTOR UJI UNTUK IMPLEMENTASI ALGORITME PRESENT DENGAN PANJANG KUNCI 80-BIT

| ***Plaintext*** | **Kunci** | ***Ciphertext*** |
|---|---|---|
| 0000000000000000 | 00000000000000000000 | 5579C1387B228445 |
| 0000000000000000 | FFFFFFFFFFFFFFFFFFFF | E72C46C0F5945049 |
| FFFFFFFFFFFFFFFF | 00000000000000000000 | A112FFC72F68417B |
| FFFFFFFFFFFFFFFF | FFFFFFFFFFFFFFFFFFFF | 3333DCD3213210D2 |




Gambar 8 Desain rangkaian perangkat keras

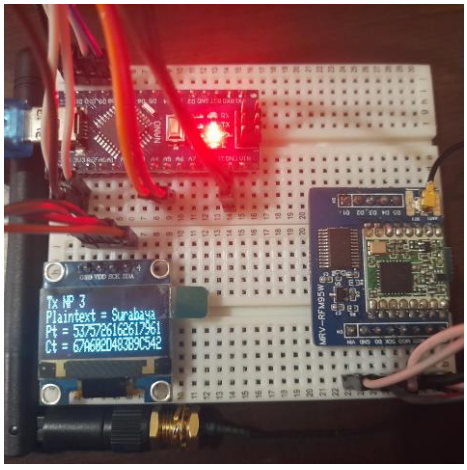



Gambar 9 Diagram alir desain implementasi program (a) LoRa Tx, (b) LoRa Rx, dan (c) LoRa Penyadap

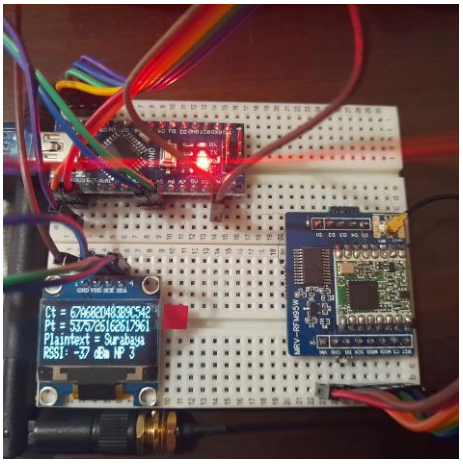
ngan desain dalam tahapan penelitian ini. Ada tiga perangkat sistem LoRa yang dirakit yaitu LoRa Tx, Rx, dan Penyadap. Perangkat keras sistem LoRa yang dikembangkan dalam penelitian ini telah dirakit sesuai dengan desain disajikan pada Gambar 10 untuk LoRa Tx, Gambar 11 untuk LoRa Rx, dan Gambar 12 untuk LoRa Penyadap.

### *D. Pengujian*

Pada tahapan pengujian, dilakukan uji coba pengaktifan perangkat LoRa untuk komunikasi data dari perangkat LoRa Tx dan Rx guna memastikan sistem LoRa yang dikembangkan pada penelitian ini dapat bekerja. Terdapat dua skenario pengujian yang terdiri dari uji vektor algoritme PRESENT dan uji penyadapan komunikasi data. Pengujian dengan uji vektor algoritme PRESENT untuk memastikan implementasi algoritme PRESENT pada sistem LoRa pada penelitian ini telah sesuai dengan standar dan teori dari algoritme PRESENT. Skenario uji penyadapan komunikasi antara LoRa Tx dan Rx menggunakan LoRa Penyadap untuk mengetahui hasil penerapan algoritme PRESENT dalam mengamankan komunikasi data LoRa pada penelitian ini. Ilustrasi skenario uji sadap disajikan pada Gambar 13.




Gambar 10 Perangkat keras LoRa Tx



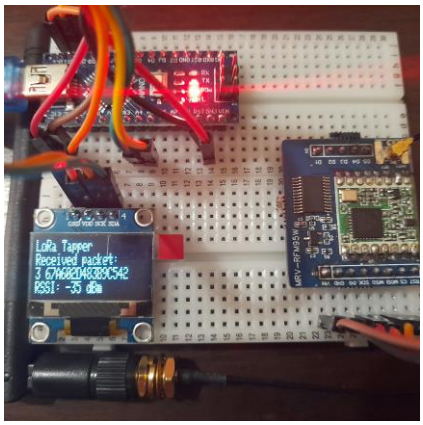

Gambar 11 Perangkat keras LoRa Rx

### *E. Analisis*

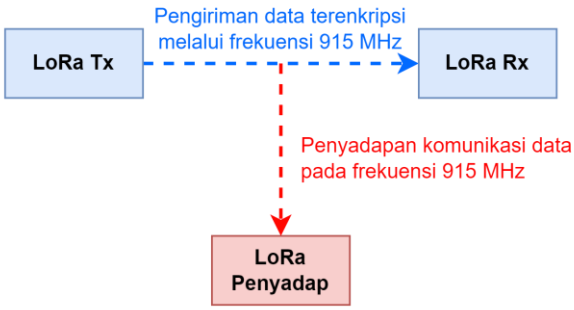
Pada tahapan analisis, pertama dilakukan analisis hasil implementasi algoritme PRESENT pada sistem LoRa dengan vektor uji algoritme PRESENT. Jika hasil vektor uji sesuai, maka implementasi algoritme PRESENT pada sistem LoRa yang dikembangkan pada penelitian ini berhasil dan sesuai dengan standar dan teori algoritme PRESENT. Setelah itu dilakukan analisis terhadap hasil skenario uji penyadapan komunikasi data untuk membuktikan bahwa sistem LoRa hasil penelitian ini dapat mengamankan kerahasiaan data yang dikirimkan secara nirkabel pada frekuensi 915 MHz. Kedua, dilakukan analisis terhadap nilai RSSI komunikasi data antara LoRa Tx dan Rx sebelum dan sesudah implementasi algoritme PRESENT untuk mengetahui performa transmisi datanya. Pengukuran nilai RSSI komunikasi data sistem LoRa dalam penelitian ini dengan 10 titik uji yaitu pada jarak 100, 200, 300, 400, 500, 600, 700, 800, 900, dan 1000 meter pada kondisi *Non Line Of Sight* (NLOS) antara gedung tempat perangkat LoRa Tx (perangkat berada di lantai 5) dengan perangkat LoRa Rx yang berada pada permukaan tanah. Ilustrasi pengukuran nilai RSSI disajikan pada Gambar 14. Pada Gambar 15 disajikan peta lokasi uji komunikasi data antara perangkat LoRa Tx dengan Rx.

## III. HASIL DAN PEMBAHASAN

Setelah sistem LoRa pada penelitian ini dirancang, diimplementasikan, dan diuji, maka hasil dalam tahapan pengujian dianalisis. Hasil pengujian sistem LoRa dengan



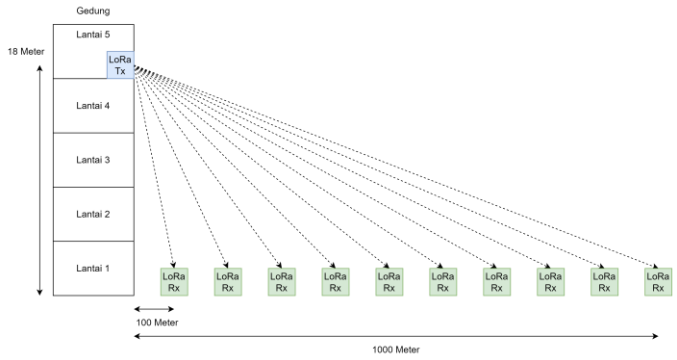

Gambar 12 Perangkat keras LoRa Penyadap




Gambar 13 Ilustrasi skenario uji penyadapan

vektor uji algoritme PRESENT menunjukkan bahwa sistem LoRa yang dikembangkan dalam penelitian ini berhasil diimplementasikan algoritme PRESENT dengan nilai data keluaran sesuai dengan vektor uji algoritme PRESENT yang disajikan pada Tabel II. Hasil pengujian sistem LoRa dengan vektor uji algoritme PRESENT ditunjukkan pada Gambar 16.

Pada skenario pengujian penyadapan komunikasi data pada frekuensi 915 MHz, digunakan karakter 64-bit sebagai *plaintext* yang akan dienkripsi dan dikirimkan dari LoRa Tx




Gambar 14 Ilustrasi pengukuran nilai RSSI antara perangkat LoRa Tx dengan Rx

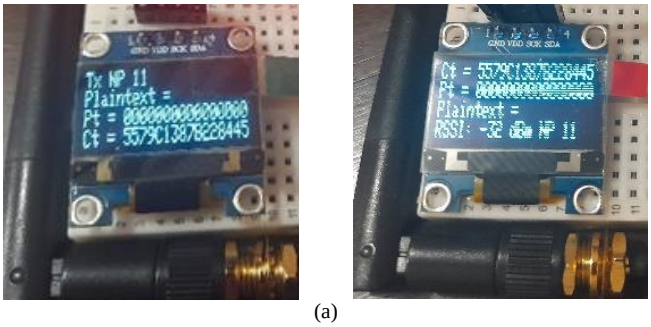

Gambar 15 Peta lokasi uji komunikasi data antara perangkat LoRa Tx dengan Rx

TABEL III
HASIL UJI MENGGUNAKAN VEKTOR UJI ALGORITME PRESENT DENGAN PANJANG KUNCI 80-BIT

| Plaintext | Kunci | Ciphertext |
|---|---|---|
| 0000000000000000 | 00000000000000000000 | 5579C1387B228445 |
| 0000000000000000 | FFFFFFFFFFFFFFFFFFFF | E72C46C0F5945049 |
| FFFFFFFFFFFFFFFF | 00000000000000000000 | A112FFC72F68417B |
| FFFFFFFFFFFFFFFF | FFFFFFFFFFFFFFFFFFFF | 3333DCD3213210D2 |

Test Vector Row 1
Ciphertext = 5579C1387B228445

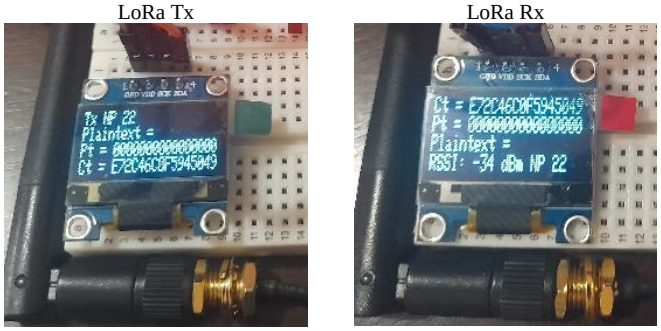
LoRa Tx | LoRa Rx




(a)

Test Vector Row 2
Ciphertext = E72C46C0F5945049

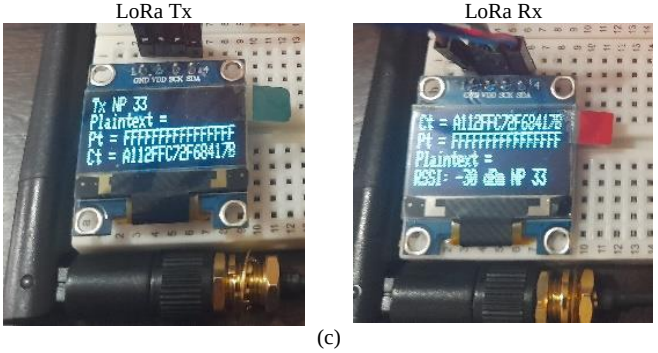
LoRa Tx | LoRa Rx




(b)

Test Vector Row 3
Ciphertext = A112FFC72F68417B

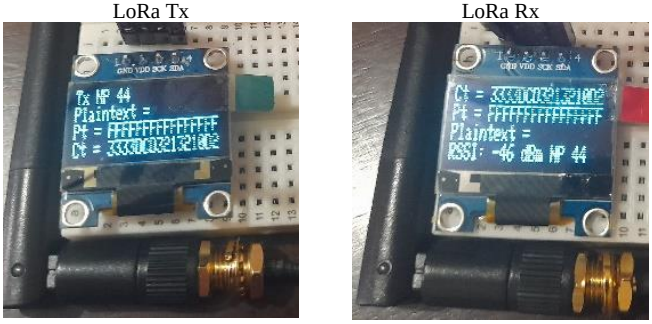
LoRa Tx | LoRa Rx




(c)

Test Vector Row 4
Ciphertext = 3333DCD3213210D2

LoRa Tx | LoRa Rx



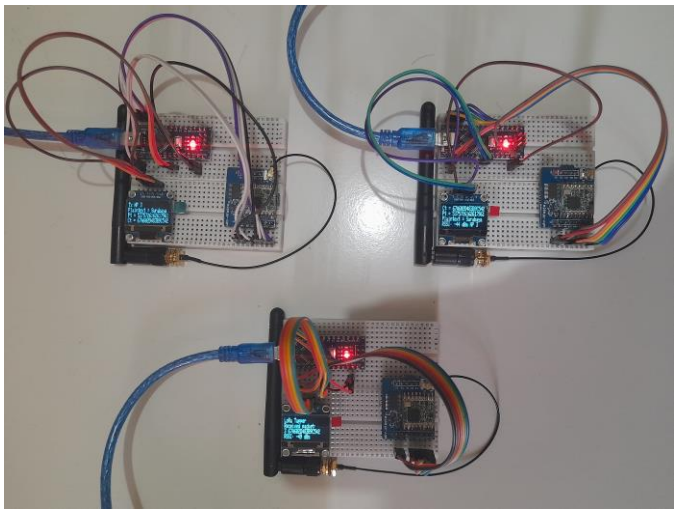

(d)

Gambar 16. Hasil pengujian sistem LoRa dengan vektor uji algoritme PRESENT pada penelitian ini: (a) Vektor Uji Baris 1, (b) Vektor Uji Baris 2, (c) Vektor Uji Baris 3, dan (d) Vektor Uji Baris 4

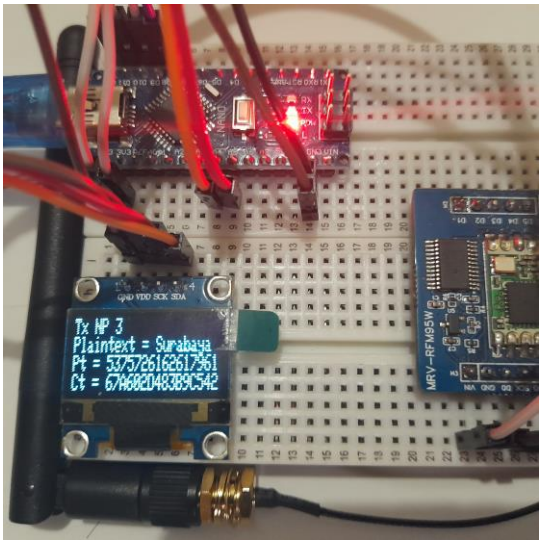
ke Rx. Data 64-bit sama dengan *plaintext* yang berupa 8 karakter. *Plaintext* pada skenario uji sadap ini adalah *string* “Surabaya”. Kunci untuk enkripsi dan dekripsi pada algoritme PRESENT adalah 80 bit atau sama dengan 10 karakter. Kunci enkripsi dan dekripsi yang digunakan pada sistem LoRa pada skenario uji sadap penelitian ini adalah *string* “udon'tKn0w”. *Ciphertext* yang dihasilkan dari enkripsi berupa *string* “67A602D483B9C542” berupa nilai heksadesimal data sebanyak 64 bit. Uji penyadapan komunikasi data ditunjukkan pada Gambar 17.

Hasil pengujian penyadapan komunikasi data pada sistem LoRa yang dikembangkan dalam penelitian ini menunjukkan bahwa algoritme PRESENT berhasil diimplementasikan untuk mengamankan kerahasiaan data yang dikirimkan dari LoRa Tx ke Rx. Hasil pengujian penyadapan komunikasi data ditunjukkan pada Gambar 18 untuk LoRa Tx, Gambar 19 untuk LoRa Rx, dan Gambar 20 untuk LoRa Penyadap. LoRa Penyadap hanya menerima paket LoRa dalam bentuk *ciphertext* saja. Jika peretas coba mengubah *ciphertext* (nilai heksadesimal) menjadi karakter, maka mereka tidak akan mendapatkan *plaintext* nya. Pada pengujian penyadapan ini, *ciphertext* “67A602D483B9C542” diubah menjadi karakter, sehingga hasilnya adalah “g¦Ô*f*¹ÅB”. Data atau pesan yang dikirimkan melalui sistem LoRa yang telah diterapkan dengan algoritme PRESENT dijamin dan terjaga kerahasiaannya.

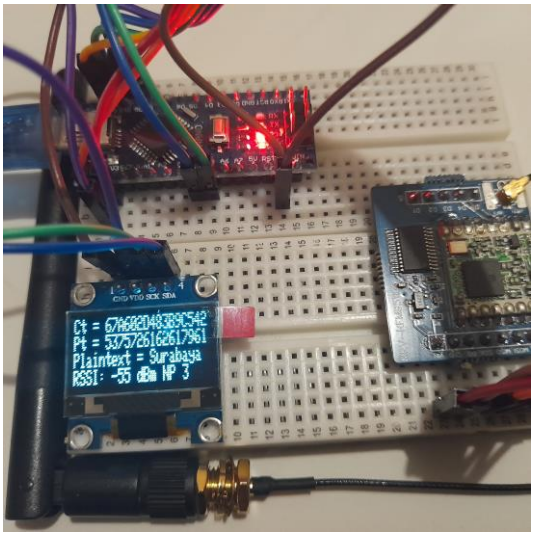
Setelah perangkat LoRa berhasil dikembangkan dan diuji di dalam laboratorium, selanjutnya dilakukan pengujian performa komunikasi data LoRa berdasarkan nilai RSSI pada kondisi lingkungan di luar ruangan. Untuk mengukur jarak komunikasi data antara perangkat LoRa Tx dan Rx digunakan teorema *Pythagoras* dengan nilai posisi perangkat LoRa Tx berada di ketinggian 18 meter di atas permukaan tanah dan perangkat LoRa Rx berada di permukaan tanah dengan jarak sejauh n dengan posisi gedung yang telah diilustrasikan pada Gambar 14. Notasi rumus teorema *Pythagoras* untuk mengukur jarak komunikasi data antar LoRa Tx dan Rx dalam penelitian ini disajikan pada Persamaan (1) dan Gambar 21. Pada Tabel III disajikan perhitungan jarak uji komunikasi data antara LoRa Tx dan Rx dalam penelitian ini.



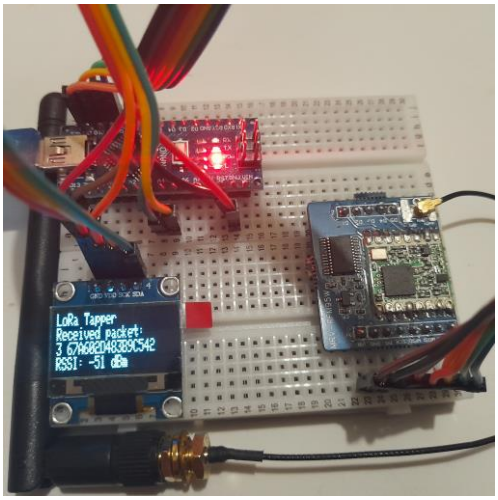
Gambar 17 Skenario uji penyadapan komunikasi data




Gambar 18 Perangkat LoRa Tx pada uji penyadapan




Gambar 19 Perangkat LoRa Rx pada uji penyadapan

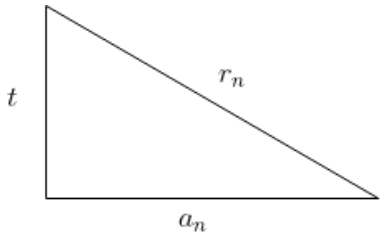



Gambar 20 Perangkat LoRa Penyadap pada uji penyadapan

$$r_n = \sqrt{t^2 + a_n^2} \quad (1)$$

$r_n$ adalah jarak antara perangkat LoRa Tx ke Rx di titik uji n, $t$ adalah nilai ketinggian posisi perangkat LoRa Tx; dan $\alpha_n$ adalah jarak uji antara perangkat LoRa Rx dengan gedung;

Pengujian komunikasi data antara perangkat LoRa Tx dengan Rx pada lingkungan luar ruangan secara NLOS karena terdapat perumahan dan pepohonan yang menghalangi. Proses pengujian tanpa adanya perbedaan ketinggian pada perangkat LoRa Rx dan tanpa skenario gangguan transmisi sinyal. Hasil pengujian komunikasi data LoRa sebanyak 10 kali pada lingkungan luar ruang menunjukkan bahwa perangkat LoRa yang dikembangkan dalam penelitian ini 100% berhasil mampu mengirimkan data sebesar 64-bit hingga jarak 1 Km secara NLOS. Hasil pengukuran nilai RSSI komunikasi data antara perangkat LoRa Tx dengan Rx dalam penelitian ini




Gambar 21 Ilustrasi jarak pengujian nilai RSSI perangkat LoRa Tx dan Rx

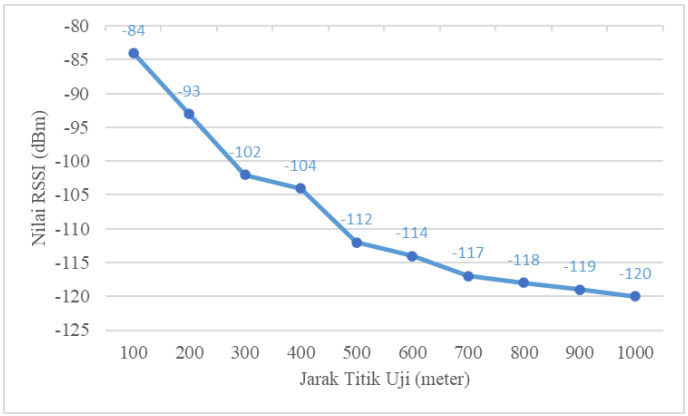
TABEL IIII
PERHITUNGAN JARAK UJI KOMUNIKASI DATA ANTARA PERANGKAT LORA TX DENGAN RX

| n | $\alpha_n$ (meter) | t (meter) | $r_n$ (meter) |
|---|---|---|---|
| 1 | 100 | 18 | 101,6 |
| 2 | 200 | 18 | 200,8 |
| 3 | 300 | 18 | 300,5 |
| 4 | 400 | 18 | 400,4 |
| 5 | 500 | 18 | 500,3 |
| 6 | 600 | 18 | 600,3 |
| 7 | 700 | 18 | 700,2 |
| 8 | 800 | 18 | 800,2 |
| 9 | 900 | 18 | 900,2 |
| 10 | 1000 | 18 | 1000,2 |

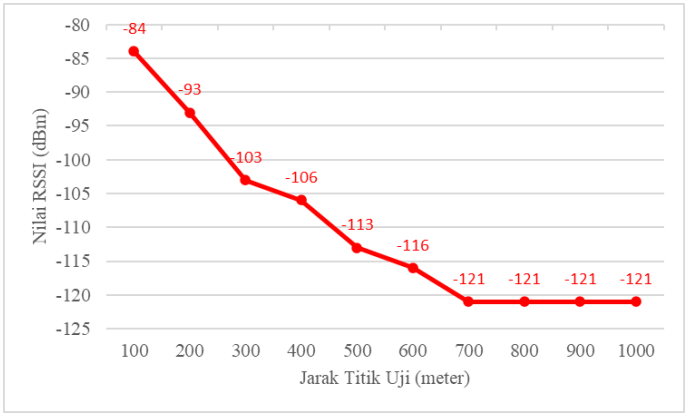
TABEL IV
NILAI RSSI HASIL UJI KOMUNIKASI DATA ANTARA PERANGKAT LORA TX DENGAN RX

| n | $\alpha_n$ (meter) | $r_n$ (meter) | Nilai RSSI (dBm) Sebelum Implementasi Algoritme PRESENT | Nilai RSSI (dBm) Sesudah Implementasi Algoritme PRESENT |
|---|---|---|---|---|
| 1 | 100 | 101,6 | -84 | -84 |
| 2 | 200 | 200,8 | -93 | -93 |
| 3 | 300 | 300,5 | -102 | -103 |
| 4 | 400 | 400,4 | -104 | -106 |
| 5 | 500 | 500,3 | -112 | -113 |
| 6 | 600 | 600,3 | -114 | -116 |
| 7 | 700 | 700,2 | -117 | -121 |
| 8 | 800 | 800,2 | -118 | -121 |
| 9 | 900 | 900,2 | -119 | -121 |
| 10 | 1000 | 1000,2 | -120 | -121 |

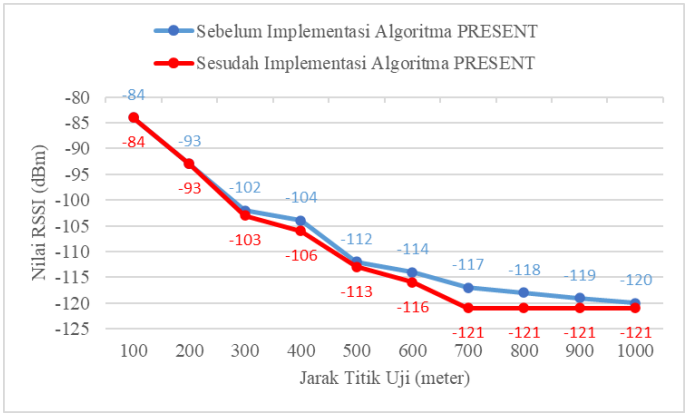
sebelum dan sesudah diimplementasikan algoritme PRESENT disajikan pada Tabel IV. Grafik visualisasi korelasi nilai RSSI dengan jarah titik uji komunikasi data LoRa hasil pengujian sebelum implementasi algoritme PRESENT disajikan pada Gambar 22. Grafik visualisasi korelasi nilai RSSI dengan jarah titik uji komunikasi data LoRa hasil pengujian sesudah implementasi algoritme PRESENT disajikan pada Gambar 23. Grafik komparasi nilai RSSI hasil pengujian komunikasi data LoRa disajikan pada Gambar 24.




Gambar 22 Grafik nilai RSSI dengan jarah titik uji komunikasi data LoRa sebelum implementasi algoritme PRESENT




Gambar 23 Grafik nilai RSSI dengan jarah titik uji komunikasi data LoRa sesudah implementasi algoritme PRESENT




Gambar 24 Grafik komparasi nilai RSSI hasil uji komunikasi data LoRa sebelum dan sesudah implementasi algoritme PRESENT

Data yang disajikan pada grafik komparasi nilai RSSI hasil uji komunikasi data perangkat LoRa Tx dan Rx sebelum dan sesudah implementasi algoritme PRESENT menunjukkan bahwa tidak terdapat pengaruh signifikan implementasi algoritme PRESENT terhadap performa komunikasi data berdasarkan nilai RSSI karena selisih nilai RSSI sebelum dan sesudah implementasi algoritme PRESENT rata-rata sebesar 2. Performa komunikasi data perangkat LoRa Tx dan Rx sebelum dan sesudah implementasi algoritme PRESENT relatif sama kekuatan sinyalnya dengan nilai jarak komunikasi perangkat sama. Pada titik uji 100 dan 200 meter, nilai RSSI komunikasi data perangkat LoRa Tx dan Rx memiliki nilai RSSI yang sama yaitu -84 dan -93 dBm. Hasil pengujian komunikasi data perangkat LoRa Tx dengan Rx menunjukkan bahwa semakin jauh posisi jarak komunikasi perangkat maka semakin kecil nilai RSSI atau semakin kecil kekuatan sinyalnya. Selain itu, nilai RSSI juga dipengaruhi kondisi lingkungan posisi komunikasi data antara perangkat LoRa Tx dengan Rx, misalnya dalam keadaan NLOS dengan penghalang perumahan dan pepohonan.

## IV. SIMPULAN

Hasil penelitian ini berupa perangkat sistem LoRa dengan implementasi algoritme PRESENT untuk mengamankan komunikasi data pada frekuensi 915 MHz. Pada penelitian ini, sistem LoRa yang dibangun dan dikembangkan menggunakan mikrokontroler ATmega328P dan modul LoRa RFM95W. Hasil analisis penelitian ini menunjukkan bahwa sistem LoRa yang dikembangkan dapat mengamankan kerahasiaan data yang dikirimkan dari LoRa Tx ke Rx pada frekuensi 915 MHz setelah dilakukan uji penyadapan menggunakan perangkat LoRa pada frekuensi yang sama, dan nilai keluaran dari sistem LoRa sudah sesuai dengan vektor uji algoritme PRESENT. Selanjutnya, hasil analisis dari uji komunikasi data secara NLOS antara perangkat LoRa Tx dengan Rx sebelum dan sesudah implementasi algoritme PRESENT menunjukkan bahwa tidak terdapat pengaruh signifikan terhadap performa komunikasi data LoRa. Hal itu ditunjukkan dengan nilai RSSI yang relatif sama pada saat pengujian komunikasi pada titik uji yang telah ditentukan karena selisih nilai RSSI sebelum dan sesudah implementasi algoritme PRESENT rata-rata sebesar 2 dBm dalam 10 kali percobaan. Pada titik uji 100 dan 200 meter, nilai RSSI komunikasi data perangkat LoRa Tx dan Rx memiliki nilai RSSI yang sama yaitu -84 dan -93 dBm. Hasil penelitian ini dapat digunakan untuk penelitian lebih lanjut dan pada penelitian selanjutnya untuk berbagai bidang, misalnya untuk keamanan IoT pada pertanian, perikanan, transportasi, industri, dan kota pintar.

## UCAPAN TERIMA-KASIH

Kami mengucapkan terima kasih kepada Politeknik Negeri Jakarta (PNJ) yang telah mendanai dan memfasilitasi penelitian ini. Kami juga mengucapkan terima kasih kepada Alfin Hikmaturokhman selaku penulis koresponden atas bantuan, dukungan, dan rekomendasinya dalam penelitian ini.

## DAFTAR REFERENSI

[1] A. Kusyanti, R. Primananda, F. A. Bakhtiar, N. Santoso, dan D. A. Rini, "Implementation of lightweight block cipher for IOT Communication Module," *7th International Conference on Sustainable Information Engineering and Technology 2022, Nov. 2022*. doi:10.1145/3568231.3568263

[2] C. Bouras, A. Gkamas, dan S. A. Salgado, "Energy efficient mechanism for lora networks," *Internet of Things*, vol. 13, hlm. 100360, 2021. doi:10.1016/j.iot.2021.100360

[3] P. Dani Prasetyo Adi dan A. Kitagawa, "A performance of radio frequency and signal strength of LoRa with BME280 sensor," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 2, hlm. 649, Apr. 2020. doi:10.12928/telkomnika.v18i2.14843

[4] P. D. Adi dan Y. Wahyu, "The error rate analyze and parameter measurement on Lora Communication for Health Monitoring," *Microprocessors and Microsystems*, vol. 98, hlm. 104820, 2023. doi:10.1016/j.micpro.2023.104820

[5] A. R. Askhedkar, dkk., "Lora communication using TVWS frequencies: Range and data rate," *Future Internet*, vol. 15, no. 8, hlm. 270, 2023. doi:10.3390/fi15080270

[6] F. Deng, P. Zuo, K. Wen, dan X. Wu, "Novel soil environment monitoring system based on RFID sensor and Lora," *Computers and Electronics in Agriculture*, vol. 169, hlm. 105169, 2020. doi:10.1016/j.compag.2019.105169

[7] L. Moiroux-Arvis, C. Cariou, dan J.-P. Chanet, "Evaluation of lora technology in 433-MHz and 868-mhz for underground to aboveground data transmission," *Computers and Electronics in Agriculture*, vol. 194, hlm. 106770, 2022. doi:10.1016/j.compag.2022.106770

[8] W. Hassan, M. Føre, J. B. Ulvund, dan J. A. Alfredsen, "Internet of fish: Integration of acoustic telemetry with LPWAN for efficient real-time monitoring of fish in Marine Farms," *Computers and Electronics in Agriculture*, vol. 163, hlm. 104850, 2019. doi:10.1016/j.compag.2019.06.005

[9] Nur-A-Alam, M. Ahsan, Md. A. Based, J. Haider, dan E. M. Rodrigues, "Smart Monitoring and controlling of appliances using Lora based IOT System," *Designs*, vol. 5, no. 1, hlm. 17, 2021. doi:10.3390/designs5010017

[10] F. M. Ortiz, T. T. de Almeida, A. E. Ferreira, dan L. H. M.K. Costa, "Experimental vs. Simulation Analysis of lora for vehicular communications," *Computer Communications*, vol. 160, hlm. 299–310, 2020. doi:10.1016/j.comcom.2020.06.006

[11] H. Desai, M. Nardello, D. Brunelli, dan B. Lucia, "Camaroptera: A long-range image sensor with local inference for Remote Sensing Applications," *ACM Transactions on Embedded Computing Systems*, vol. 21, no. 3, hlm. 1–25, 2022. doi:10.1145/3510850

[12] R. O. Andrade dan S. G. Yoo, "A comprehensive study of the use of Lora in the development of Smart Cities," *Applied Sciences*, vol. 9, no. 22, hlm. 4753, 2019. doi:10.3390/app9224753

[13] J. C. Liando, A. Gamage, A. W. Tengourtius, dan M. Li, "Known and unknown facts of Lora," *ACM Transactions on Sensor Networks*, vol. 15, no. 2, hlm. 1–35, 2019. doi:10.1145/3293534

[14] F. B. Limas, A. Kusyanti, dan R. Primananda, "The implementaion of Mickey cipher in securing constrained devices based on LoRa," *Proceedings of the 8th International Conference on Sustainable Information Engineering and Technology*, Okt. 2023. doi:10.1145/3626641.3627018

[15] E. Erkan, H. Oğraş, dan Ş. Fidan, "Application of a secure data transmission with an effective timing algorithm based on Lora Modulation and Chaos," *Microprocessors and Microsystems*, vol. 99, hlm. 104829, 2023. doi:10.1016/j.micpro.2023.104829

[16] M. J. Dworkin, "Advanced encryption standard (AES)," *NIST FIPS 197*, 2023. doi:10.6028/nist.fips.197-upd1

[17] F. Amelia dan M. F. Ramadhani, "LoRa-based asset tracking system with data encryption using AES-256 algorithm," *2022 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*, 2022. doi:10.1109/icramet56917.2022.9991210

[18] P. A. Windya, V. Suryani, dan A. A. Wardana, "Sniffing prevention in Lora network using combination of Advanced Encryption Standard (AES) and message authentication code (MAC)," *2021 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS)*, 2021. doi:10.1109/icadeis52521.2021.9702081

[19] C. Zhang, J. Yue, L. Jiao, J. Shi, dan S. Wang, "A novel physical layer encryption algorithm for Lora," *IEEE Communications Letters*, vol. 25, no. 8, hlm. 2512–2516, 2021. doi:10.1109/lcomm.2021.3078669
[20] Atmel Corporation, "ATmega328P Datasheet," *Atmel Corporation*
[21] ISO/IEC, "ISO/IEC 29192-2:2019 Information security — Lightweight cryptography — Part 2: Block ciphers," *International Standard*, 2019
[22] G. Sravya, Manchalla. O. V. P. Kumar, Y. Sudarsana Reddy, K. Jamal, dan K. Mannem, "The ideal block ciphers - correlation of AES and present in cryptography," *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 2020. doi:10.1109/iciss49785.2020.9315883
[23] C. G. Thomas, *Research Methodology and Scientific Writing*, 2021. doi:10.1007/978-3-030-64865-7
[24] Hope Microelectronics, "RFM95/96/97/98(W) Datasheet – Low Power Long Range Transceiver Module V1.0," *Hoperf Electronic*
[25] Arduino, "Product Reference Manual Arduino Nano Datasheet", *Arduino Nano*, 2023
[26] A. Bogdanov, dkk., "Present: An ultra-lightweight block cipher," *Cryptographic Hardware and Embedded Systems - CHES 2007 Springer*, hlm. 450–466, 2007. doi:10.1007/978-3-540-74735-2_31

**Eka Hero Ramadhani**, pengembang teknologi pembelajaran pada Politeknik Siber dan Sandi Negara (Poltek SSN). Saat ini aktif sebagai peneliti di bidang rekayasa perangkat keras kriptografi. Bidang minat keilmuan pada topik keamanan IoT.

**Asri Wulandari**, menyelesaikan gelar sarjana di Universitas Brawijaya Malang dan Program Magister di Universitas Indonesia pada bidang teknik telekomunikasi. Saat ini menjadi staf pengajar di Politeknik Negeri Jakarta dan menjadi asesor pada LSP Politeknik Negeri Jakarta. Riset dan penelitian yang dilakukan adalah pada teknologi jaringan seluler, *networking*, dan pengembangan terkait kedua bidang tersebut.

**Alfin Hikmaturokhman**, Dosen di Telkom University Purwokerto. Alfin memegang gelar sarjana dalam bidang teknik elektro dari UGM dan meraih gelar magister dari Telkom University dan doktor dalam bidang yang sama dari Universitas Indonesia.