Rancang Bangun Perangkat Keamanan Data *End-to-End Encryption* pada Komunikasi Radio Menggunakan NRF24L01 PA LNA

Muhammad Daniel Firdaus, Oktario, Kiki Kananda, Swadexi Istiqphara

Program Studi Teknik Elektro, Jurusan Teknologi Produksi, Industri dan Informasi, Institut Teknologi Sumatera
Email : muhammad.13115003@student.itera.ac.id, oktario.13116072@student.itera.ac.id, kiki.kananda@el.itera,ac,id, swadexi.istiqphara@el.itera.ac.id

***Abstract*— Komunikasi radio merupakan salah satu teknologi komunikasi nirkabel yang memanfaatkan gelombang radio sebagai media. Komunikasi radio menggunakan gelombang radio untuk mengirim informasi dari pemancar menuju penerima. Proses pengiriman informasi tersebut dirambatkan melalui udara yang memungkinkan adanya pelacakan dan pengumpulan data secara tersembunyi oleh penyadap. Fakta bahwa kanal komunikasi nirkabel dianggap sebagai kanal yang rentan terhadap berbagai macam serangan maka aspek keamanan merupakan salah satu hal penting dalam komunikasi nirkabel.**

Diperlukan sebuah metode untuk melindungi informasi yang dikirim melalui komunikasi radio dari serangan atau penyadapan yang menyebabkan perubahan, kerusakan, dan kebocoran informasi. Kriptografi dapat digunakan sebagai metode untuk melindungi informasi. Pada penelitian sebelumnya dilakukan analisis tentang keamanan dari sistem komunikasi nirkabel seperti interkoneksi *Internet of Thing* (IoT) dan pengiriman surat elektronik dengan beberapa metode kriptografi untuk mengamankan data-data yang dikirimkan melalui komunikasi nirkabel. Maka penelitian ini dilakukan perancangan dan pembuatan perangkat keamanan data pada komunikasi radio dengan metode penelitian mengirimkan data *plaintext* sebesar 2 *bytes* sampai 16 *bytes* dari perangkat pemancar ke penerima. Perangkat ini menggunakan metode kriptografi *Corrected Block Tiny Encryption Algorithm* (XXTEA) yang ditanamkan pada mikrokontroler Arduino Nano.

Hasil pengujian didapatkan bahwa CRYPTOBLE berhasil melakukan proses enkripsi/dekripsi data dengan parameter penelitian, yaitu rata-rata kecepatan proses enkripsi dari 1622,893 sampai 1800,4 mikrodetik, rata-rata kecepatan pengiriman didapatkan sebesar 183,90 sampai 788,90 mikrodetik, rata-rata kecepatan proses dekripsi dari 2167,890 sampai 3027,6 mikrodetik, dan presentase data hilang sebesar 0%. Maksimal *baudrate* yang dapat digunakan adalah 74880 bps dan maksimal jarak adalah 100 meter. Menggunakan perangkat CRYPTOBLE data yang dikirimkan melalui komunikasi radio lebih aman.

***Keywords*—Komunikasi radio, keamanan, kriptografi, *Corrected Block Tiny Encryption Algorithm*, XXTEA.**

I. PENDAHULUAN

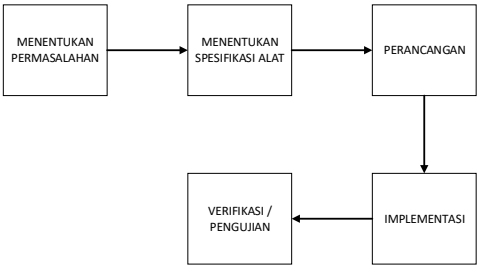
Sistem keamanan dalam komunikasi nirkabel merupakan salah satu hal penting yang harus diperhatikan. Kanal komunikasi nirkabel dianggap sebagai kanal yang rentan terhadap berbagai macam serangan. Pada sistem komunikasi nirkabel, informasi dirambatkan menggunakan gelombang radio melalui udara terbuka. Proses pengiriman tersebut memungkinkan terjadinya pelacakan dan pengumpulan data secara tersembunyi oleh penyadap [1]. Salah satu contoh terdapat 22 juta ancaman terhadap *Internet of Things* (IoT) *smartcity* yang lebih tepatnya adalah penyerangan CCTV di kota Libanon pada tahun 2017 [2]. Para penyadap atau peretas melakukan *cyberattack* dengan cara menanamkan sebuah *malware* dan mendeteksi lokasi melalui perangkat yang telah tersadap [3]. Menurut laporan Kapersky Lab bahwa terdapat 120.000 lebih *malware* yang menyerang IoT selama tahun 2018, statistik menunjukkan bahwa propagasi *malware* IoT yang paling populer masih berusaha secara paksa membobol kata sandi atau yang dikenal dengan *brute force, brute force* ini telah terdeteksi sebanyak 93% [4]. Contoh kejahatan *cyberattack* tersebut dapat terjadi pada saat pengiriman maupun penerimaan pada jaringan komunikasi elektronik seperti telemetri atau IoT [5].

Diperlukan sebuah metode untuk melindungi informasi yang dikirim melalui komunikasi radio dari serangan atau penyadapan yang menyebabkan perubahan, kerusakan, dan kebocoran informasi. Kriptografi adalah ilmu dan seni untuk menjaga kemanan pesan. Kriptografi dapat digunakan sebagai metode untuk melindungi informasi. Pada penelitian sebelumnya dilakukan analisis tentang keamanan dari sistem komunikasi nirkabel seperti interkoneksi *Internet of Thing* (IoT) dan pengiriman surat elektronik dengan beberapa metode kriptografi untuk mengamankan data-data yang dikirimkan melalui komunikasi nirkabel. Parameter yang diteliti, yaitu keberhasilan enkripsi data dan kecepatan proses enkripsi serta kecepatan pengiriman. Maka penelitian ini dilakukan perancangan dan pembuatan perangkat keamanan data pada komunikasi radio dengan metode penelitian mengirimkan data *plaintext* sebesar 2 *bytes* sampai 16 *bytes* dari perangkat pemancar ke penerima. Parameter yang diteliti adalah hasil engkripsi, kecepatan enkripsi, kecepatan pengiriman, hasil dekripsi, kecepatan dekripsi, dan presentase data hilang saat pengiriman. Perangkat ini menggunakan metode kriptografi *Corrected Block Tiny Encryption Algorithm* (XXTEA) yang ditanamkan pada mikrokontroler Arduino Nano. Perangkat ini juga dilengkapi dengan aplikasi berbasis Windows yang berfungsi sebagai antarmuka pengguna untuk melakukan

konfigurasi perangkat, yaitu konfigurasi waktu, *baudrate*, kunci, dan alamat radio.

II. METODE PENELITIAN

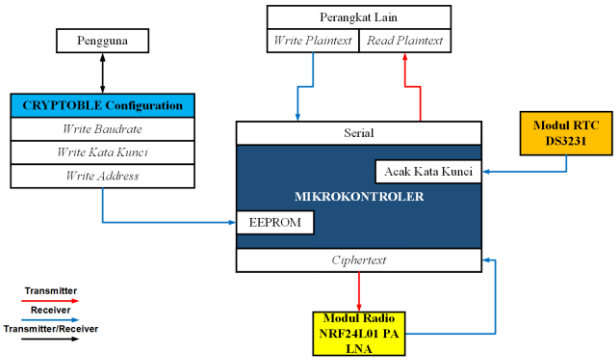
Metode penelitian yang digunakan memiliki lima tahapan yang ditunjukkan pada Gambar 1.



Gambar 1. Metode Penelitian yang digunakan

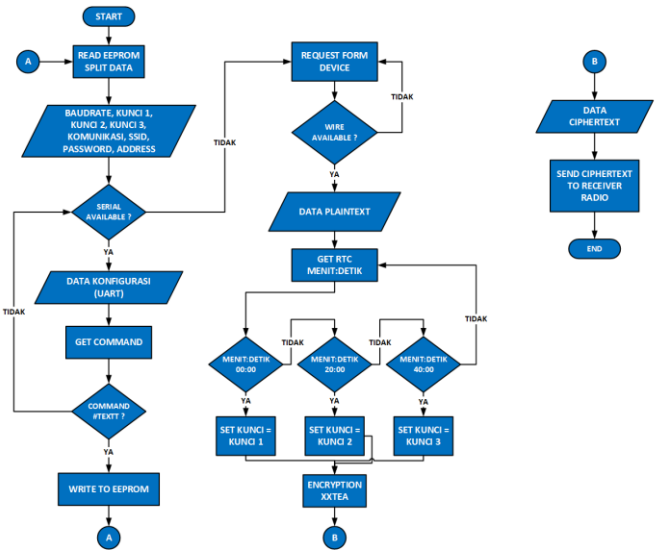
III. PERANCANGAN DAN IMPLEMENTASI

A. *Diagram Blok*

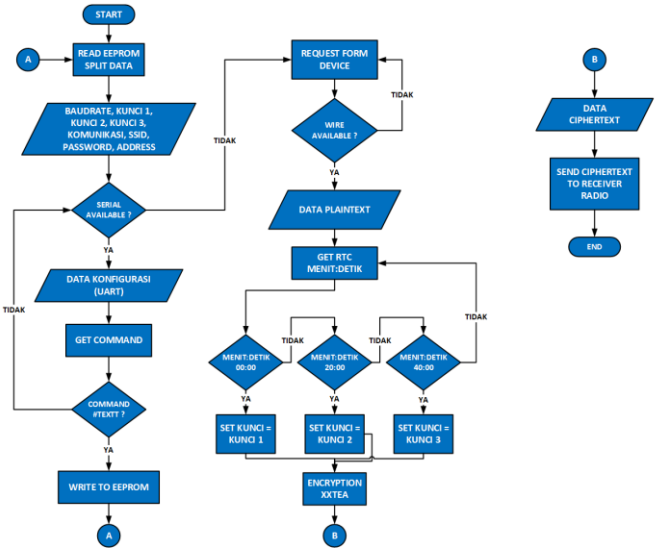


Gambar 2. Diagram Blok Sistem

B. *Flowchart* Perangkat



Gambar 3. *Flowchart* Perangkat Pemncar



Gambar 4. *Flowchart* Perangkat Penerima

C. *Kebutuhan hardware*

1. Mikrokontroler Arduino Nano
   Arduino Nano merupakan mikrokontroler *open-source* yang sudah dirangkai lengkap dengan sistem minimum. Arduino Nano ini merupakan mikrokontroler yang memiliki fungsi sebagai otak dari perangkat atau sistem yang dirancang. Menggunakan *chip* ATmega328 dilengkapi dengan 32 KB *flash memory*, 1 KB EEPROM, 16 MHz *clock speed*, dan memiliki 20 pin I/O [6].
2. Modul Radio NRF24L01 PA LNA
   Modul NRF24l01 PA LNA digunakan untuk komunikasi jarak jauh dengan menggunakan frekuensi gelombang radio sebesar 2,4 – 2,5 GHz *Industrial*, *Scientific*, *and Medical* (ISM). Modul *wireless* NRF24L01 PA LNA memiliki kecepatan hingga 2 Mbps dengan beberapa opsi *date rate* 250 Kbps, 1 Mbps dan 2 Mbps. Modul ini bisa digunakan sebagai *transmitter* dan *receiver* yang terdiri dari *synthesizer* frekuensi terintegrasi, kekuatan *amplifier*, osilator kristal, *demodulator*, *modulator*, dan *enhanced Shockburst*™ mesin protocol. Pada bagian *output* daya, saluran frekuensi, dan *setup protocol* yang mudah dieksekusi program melalui antarmuka *Serial Peripheral Interface* (SPI). Konsumsi arus yang digunakan sangat rendah, hanya sebesar 0,9 mA pada daya *output* sebesar −6 dBm dan 12.3 mA dalam *mode* RX atau mode *receiver* [7][8].
3. Modul *Realtime Clock* DS3231
   Modul RTC DS3231 adalah *Realtime Clock* (RTC) dengan kompensasi suhu kristal osilator yang terintegrasi (TCX0). TCX0 ini menyediakan sebuah *clock* referensi yang stabil, akurat, dan memelihara akurasi RTX sekitar ±2 menit pertahun. Modul DS3231 menyediakan waktu dan kalender dengan dua waktu alarm dalam satu hari dan keluaran gelombang persegi yang dapat diprogram. Waktu dan kalender memberikan informasi tentang detik, menit, jam, hari, tanggal, bulan, dan tahun yang terdapat ada register

internal dan dapat diakses menggunakan komunikasi *Inter Integrated Circuit* (I2C) [9].

D. *Kebutuhan software*

1. Arduino IDE
   Software ini merupakan *software* pengembangan dari produk Arduino untuk *mengompile* dan mengunggah *source code* yang telah dibuat menggunakan Bahasa Arduino ke mikrokontroler Arduino.
2. Visual Studio
   Visual Studio merupakan *tools development* dari Windows, yaitu Visual Studio. Visual Studio menggunakan bahasa *C#*.

E. *Hasil Implementasi*

Hasil Implementasi perangkat CRYPTOBLE dalam bentuk cetak PCB dan *packaging* perangkat ditunjukkan pada Gambar 5.

Gambar 5. Hasil Implementasi Perangkat CRYPTOBLE

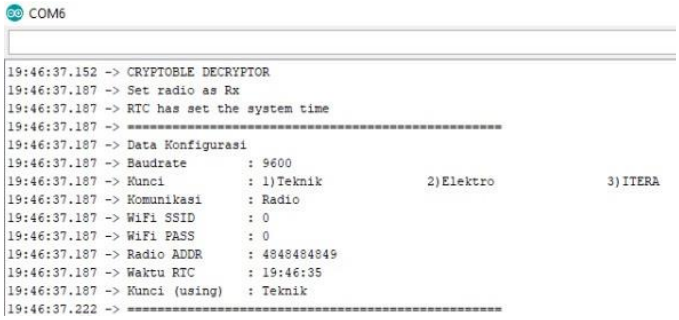
IV. PENGUJIAN

A. *Pengujian Aplikasi CRYPTOBLE Configuration*

Pengujian terhadap aplikasi CRYPTOBLE Configuration dilakukan untuk mengetahui kinerja dari aplikasi sehingga dapat digunakan dengan baik sebagai aplikasi untuk pengaturan atau konfigurasi dari perangkat CRYPTOBLE. Pengujian dilakukan dengan menjalankan aplikasi dan mengirim data konfigurasi. Pengujian tersebut ditunjukkan pada Gambar 6.

Gambar 6. Pengujian CRYPTOBLE Configuration

Pengujian tersebut dilakukan dengan mengisi data konfigurasi dan mengirim data tersebut ke perangkat CRYPTOBLE. Pemeriksaan dengan melihat data yang tersimpan pada CRYPTOBLE melalui serial monitor. Hasil pengujian data konfigurasi ditunjukkan pada Gambar 7.



Gambar 7. Hasil Pengujian Kesesuaian Data Konfigurasi

B. *Pengujian Perangkat CRYPTOBLE*

Pengujian terhadap perangkat CRYPTOBLE dilakukan untuk mengetahui kinerja dari perangkat sehingga dapat digunakan dengan baik sebagai perangkat keamanan data. Pengujian dilakukan dengan mengirim teks. Hasil pengujian pengiriman data teks ditunjukkan pada Gambar 8 dan Gambar 9.

```
17:12:04.126 -> ================================================
17:12:05.088 -> Data sensor     : ITERA
17:12:05.088 -> Waktu           : 144 uS
17:12:05.088 ->
17:12:05.088 -> Kunci           : Teknik
17:12:05.088 -> Cipher          : B0E97D396585BF2A
17:12:05.088 -> Waktu           : 1652 uS
17:12:05.088 ->
17:12:05.088 -> Checking CRC
17:12:05.088 -> XOR (16x)       : □ 8 } D s 7 □ = □ > □ 3 q 7 □ D
17:12:05.124 -> CRC             : D
17:12:05.124 ->
17:12:05.124 -> Data sent to radio
17:12:05.124 -> ================================================
```

Gambar 8. Hasil Pengujian Perangkat Pemancar

```
19:46:37.496 -> ================================================
19:46:37.564 -> Data radio      : B0E97D396585BF2A:D
19:46:37.598 -> Waktu           : 184 uS
19:46:37.598 ->
19:46:37.598 -> Checking CRC
19:46:37.598 -> XOR (16x)       : □ 8 } D s 7 □ = □ > □ 3 q 7 □ D
19:46:37.598 -> CRC             : Valid
19:46:37.598 ->
19:46:37.598 -> Kunci           : Teknik
19:46:37.598 -> Plaintext       : ITERA
19:46:37.598 -> Waktu           : 2432 uS
19:46:37.598 ->
19:46:37.598 -> Data sent to device
19:46:37.598 -> ================================================
```

Gambar 9. Hasil Pengujian Perangkat Penerima

Dari pengujian tersebut didapat data yang ditunjukkan pada Tabel 1 dan Tabel 2.

Tabel 1. Data Pengujian Perangkat Pemancar CRYPTOBLE 10 meter

No.	Data	Panjang data	Waktu enkripsi	Hasil enkripsi (ciphertext)

		(byte)	(microsecond)	
1	Hi	2	287,6	48690D00
2	INA	3	284,8	494E410D
3	2020	4	1646	D060A942857B83A6
4	ITERA	5	1666,8	B0E97D396585BF2A
5	Teknik	6	1666,8	1C1545A035CE21B8
6	Elektro	7	1677,2	DAF048CB1CD03CA5
7	INSTITUT	8	1805,2	059237FD59D69A9D0CAFEA7A
8	TEKNOLOGI	9	1798,8	AAD174AA34A4EDEB554AAF6C
9	HelloWorld	10	1800,8	EB622B2668F464CA29813D18
10	Kriptografi	11	1800,4	A5D5B4DC976F06D43FBDE79D
11	Arduino Nano	12	1987,6	BEB3341CCB6ABCD801A58544EAF3A060
12	Bandarlampung	13	1998,8	BBEC95E9E007F318FA101C031342920A
13	Teknik Elektro	14	2010	533779184360EC5ABA52395ED5F2C4F
14	Sumatera BagSel	15	2005,2	A3CA43F13DEE4D982043762D3E1A92AE
15	correctedblokTEA	16	2007,6	451B9E1CB31E801554D10B103E883AE8
	Rata-rata		1629,573	

Tabel 2. Data Pengujian Perangkat Penerima CRYPTOBLE 10 meter

No.	Data	Waktu pengiriman (microsecond)	Hasil dekripsi (plaintext)	Waktu dekripsi (microsecond)	Data hilang sensor (%)	Data hilang radio (%)
1	Hi	184,4	Hi	602,2	0	0
2	INA	184	INA	598	0	0
3	2020	184,4	2020	2388,8	0	0
4	ITERA	185,2	ITERA	2430,4	0	0
5	Teknik	184	Teknik	2388,8	0	0
6	Elektro	185,2	Elektro	2395,2	0	0
7	INSTITUT	184,8	INSTITUT	3024,8	0	0
8	TEKNOLOGI	184	TEKNOLOGI	3018,8	0	0
9	HelloWorld	183,2	HelloWorld	3027,6	0	0
10	Kriptografi	185,2	Kriptografi	3022,4	0	0
11	Arduino Nano	oversize	oversize	oversize	0	5,882
12	Bandarlampung	oversize	oversize	oversize	0	5,882
13	Teknik Elektro	oversize	oversize	oversize	0	5,882
14	Sumatera BagSel	oversize	oversize	oversize	0	5,882
15	correctedblokTEA	oversize	oversize	oversize	0	5,882
	Rata-rata	184,213		2289,7	0	1,961

Data pengujian menunjukkan bahwa CRYTOBLE sudah dapat mengirim data dan melakukan proses enkripsi dan dekripsi. Namun pada data teks dengan panjang 12 *bytes* sampai 16 *bytes* mengalami masalah, yaitu kapasitas dari maksimal data yang dapat ditampung pada perangkat penerima sehingga tidak dapat dienkripsi karena tidak berhasil memeriksa keaslian data melalui CRC. Didapatkan kecepatan rata-rata enkripsi sebesar 1629,573 mikrodetik, kecepatan rata-rata dekripsi sebesar 2289,7 mikrodetik, dan rata-rata data hilang pada pengiriman radio sebesar 1,961%.

Pengujian kedua dilakukan pada jarak 100 meter dengan data teks yang sama. Data yang diambil data kecepatan, hasil enkripsi, hasil dekripsi, data hilang pada pemancar, dan data hilang pada penerima. Hasil pengujian perangkat CRYPTOBLE pada jarak 100 meter dapat ditunjukkan pada Tabel 3 dan Tabel 4.

Tabel 3. Data Pengujian Perangkat Pemancar CRYPTOBLE 100 meter

No.	Data	Panjang data (byte)	Waktu enkripsi (microsecond)	Hasil enkripsi (ciphertext)
1	Hi	2	287,6	48690D00
2	INA	3	284,8	494E410D
3	2020	4	1646	D060A942857B83A6
4	ITERA	5	1666,8	B0E97D396585BF2A
5	Teknik	6	1666,8	1C1545A035CE21B8
6	Elektro	7	1677,2	DAF048CB1CD03CA5
7	INSTITUT	8	1805,2	059237FD59D69A9D0CAFEA7A
8	TEKNOLOGI	9	1798,8	AAD174AA34A4EDEB554AAF6C
9	HelloWorld	10	1800,8	EB622B2668F464CA29813D18
10	Kriptografi	11	1800,4	A5D5B4DC976F06D43FBDE79D
11	Arduino Nano	12	1987,6	BEB3341CCB6ABCD801A58544EAF3A060
12	Bandarlampung	13	1998,8	BBEC95E9E007F318FA101C031342920A
13	Teknik Elektro	14	2010	533779184360EC5ABA52395ED5F2C4F
14	Sumatera BagSel	15	2005,2	A3CA43F13DEE4D982043762D3E1A92AE
15	correctedblokTEA	16	2007,6	451B9E1CB31E801554D10B103E883AE8
	Rata-rata		1629,573	

Tabel 4. Data Pengujian Perangkat Penerima CRYPTOBLE 100 meter

No.	Data	Waktu pengiriman (microsecond)	Hasil dekripsi (plaintext)	Waktu dekripsi (microsecond)	Data hilang sensor (%)	Data hilang radio (%)
1	Hi	184,4	Hi	632,8	0	0
2	INA	184	INA	626	0	0
3	2020	184,4	2020	2385,2	0	0
4	ITERA	185,2	ITERA	2448,8	0	0
5	Teknik	184	Teknik	2443,2	0	0
6	Elektro	185,2	Elektro	2440	0	0
7	INSTITUT	184,8	INSTITUT	2964	0	0
8	TEKNOLOGI	184	TEKNOLOGI	3031,2	0	0

9	HelloWorld	183,2	HelloWorld	2969,2	0	0
10	Kriptografi	185,2	Kriptografi	2960,8	0	0
11	Arduino Nano	oversize	oversize	oversize	0	5,882
12	Bandarlampung	oversize	oversize	oversize	0	5,882
13	Teknik Elektro	oversize	oversize	oversize	0	5,882
14	Sumatera BagSel	oversize	oversize	oversize	0	5,882
15	correctedblokTEA	oversize	oversize	oversize	0	5,882
	Rata-rata	184,440		2290,12	0	1,961

Data pengujian kedua menunjukkan bahwa CRYTOBLE sudah dapat mengirim data dan melakukan proses enkripsi dan dekripsi. Namun pada data teks dengan panjang 12 *bytes* sampai 16 *bytes* mengalami masalah, yaitu kapasitas dari maksimal data yang dapat ditampung pada perangkat penerima sehingga tidak dapat dienkripsi karena tidak berhasil memeriksa keaslian data melalui CRC. Didapatkan kecepatan rata-rata enkripsi sebesar 1629,573 mikrodetik, kecepatan rata-rata dekripsi sebesar 2290,12 mikrodetik, dan rata-rata data hilang pada pengiriman radio sebesar 1,961%.

Pengujian ketiga dilakukan pada jarak 200 meter dengan data teks yang sama. Data yang diambil data kecepatan, hasil enkripsi, hasil dekripsi, data hilang pada pemancar, dan data hilang pada penerima. Hasil pengujian perangkat CRYPTOBLE pada jarak 200 meter dapat ditunjukkan pada Tabel 5 dan Tabel 6.

Tabel 5. Data Pengujian Perangkat Pemancar CRYPTOBLE 200 meter

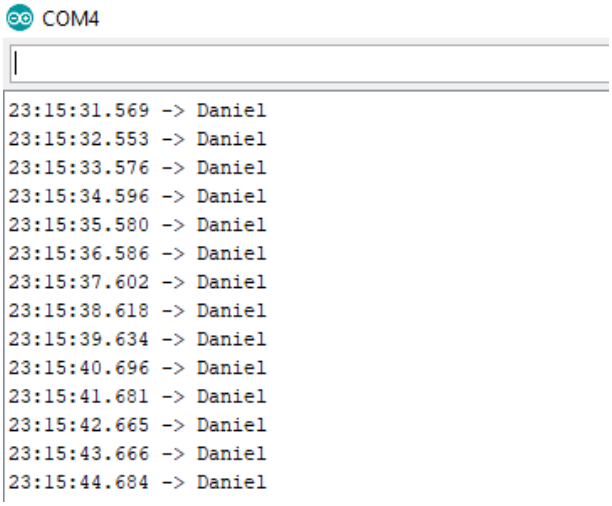
No.	Data	Panjang data (byte)	Waktu enkripsi (microsecond)	Hasil enkripsi (ciphertext)
1	Hi	2	287,6	48690D00
2	INA	3	284,8	494E410D
3	2020	4	1646	D060A942857B83A6
4	ITERA	5	1666,8	B0E97D396585BF2A
5	Teknik	6	1666,8	1C1545A035CE21B8
6	Elektro	7	1677,2	DAF048CB1CD03CA5
7	INSTITUT	8	1805,2	059237FD59D69A9D0CAFEA7A
8	TEKNOLOGI	9	1798,8	AAD174AA34A4EDEB554AAF6C
9	HelloWorld	10	1800,8	EB622B2668F464CA29813D18
10	Kriptografi	11	1800,4	A5D5B4DC976F06D43FBDE79D
11	Arduino Nano	12	1987,6	BEB3341CCB6ABCD801A58544EAF3A060
12	Bandarlampung	13	1998,8	BBEC95E9E007F318FA101C031342920A
13	Teknik Elektro	14	2010	53377918E4360EC5ABA52395ED5F2C4F
14	Sumatera BagSel	15	2005,2	A3CA43F13DEE4D982043762D3E1A92AE
15	correctedblokTEA	16	2007,6	451B9E1CB31E801554D10B103E883AE8
	Rata-rata		1629,573	

Tabel 6. Data Pengujian Perangkat Penerima CRYPTOBLE 200 meter

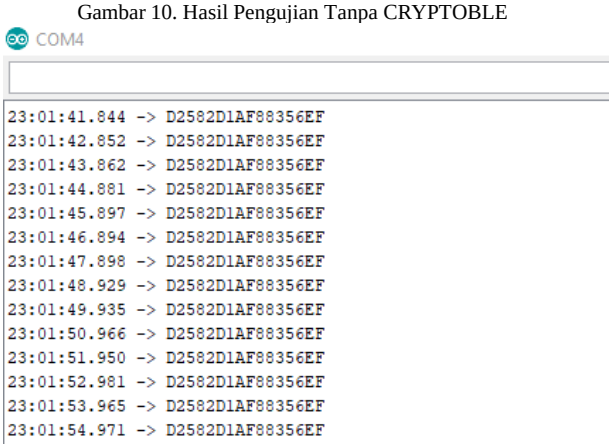
No.	Data	Waktu pengiriman (microsecond)	Hasil dekripsi (plaintext)	Waktu dekripsi (microsecond)	Data hilang sensor (%)	Data hilang radio (%)
1	Hi	650	Hi	596,8	0	0
2	INA	680	INA	600	0	0
3	2020	710	2020	2319,2	0	0
4	ITERA	770	ITERA	2389,2	0	0
5	Teknik	740	Teknik	2436,4	0	0
6	Elektro	800	Elektro	2436,8	0	0
7	INSTITUT	860	INSTITUT	2777	0	40
8	TEKNOLOGI	869	TEKNOLOGI	2891,1	0	10
9	HelloWorld	830	HelloWorld	2952,9	0	10
10	Kriptografi	980	Kriptografi	2965	0	20
11	Arduino Nano	oversize	oversize	oversize	0	5,882
12	Bandarlampung	oversize	oversize	oversize	0	5,882
13	Teknik Elektro	oversize	oversize	oversize	0	5,882
14	Sumatera BagSel	oversize	oversize	oversize	0	5,882
15	correctedblokTEA	oversize	oversize	oversize	0	5,882
	Rata-rata	788,90		2236,44	0	7,294

Hasil pengujian CRYPTOBLE dengan jarak komunikasi 200 meter didapatkan bahwa data teks yang dikirim dari perangkat pemancar berhasil diterima oleh perangkat penerima. Proses enkripsi/dekripsi juga berhasil dilakukan dengan baik. Namun pada data teks dengan panjang 12 *bytes* sampai 16 *bytes* mengalami masalah yang sama dengan pengujian pertama, yaitu kapasitas dari maksimal data yang dapat ditampung pada perangkat penerima sehingga tidak dapat dienkripsi karena tidak berhasil memeriksa keaslian data melalui CRC. Didapatkan kecepatan rata-rata enkripsi sebesar 1629,573 mikrodetik, kecepatan rata-rata dekripsi sebesar 2236,44 mikrodetik, dan rata-rata data hilang pada pengiriman radio sebesar 7,294%. Selain itu terdapat data yang tidak diterima oleh CRYPTOBLE *decrytor*, yaitu data INSTITUT sebanyak 4 kali, TEKNOLOGI sebanyak 1 kali, HelloWorld sebanyak 1 kali, dan Kriptografi sebanyak 2 kali.

Pengujian selanjutnya *sniffing* untuk melihat data ketika terjadi penyadapan terhadap komunikasi radio. Penyadapan dapat terjadi ketika alamat dan kanal komunikasi radio telah diketahui penyadap. Data yang dikirim adalah kata “Daniel”. Dilakukan perbandingan antara pengiriman data tanpa menggunakan CRYPTOBLE dengan pengiriman data menggunakan CRYPTOBLE. Perbandingan tersebut ditunjukkan pada Gambar 10 dan Gambar 11.



Gambar 10. Hasil Pengujian Tanpa CRYPTOBLE



Gambar 11. Hasil Pengujian Dengan CRYPTOBLE

Pengiriman data tanpa menggunakan CRYPTOBLE berhasil di-*sniffing* oleh penyadap dan data dapat dibaca dengan jelas. Sedangkan pengiriman data menggunakan CRYPTOBLE berhasil di-*sniffing* namun data tidak dapat dibaca dengan jelas karena data sudah dalam bentuk *ciphertext*. Pengujian ini membuktikan bahwa CRYPTOBLE berhasil meningkatkan keamanan dengan mengenkripsi data sebelum dikirim melalui komunikasi radio.

V. Hasil dan Pembahasan

Aplikasi CRYPTOBLE Configuration berhasil mengirim data ke perangkat dan data tersebut tersimpan pada EEPROM dengan presentase data hilang sebesar 0%. Perangkat CRYPTOBLE berhasil mengamankan data untuk meningkatkan keamanan. Rata-rata kecepatan proses enkripsi dari 1622,893 sampai 1800,4 mikrodetik. Rata-rata kecepatan proses dekripsi dari 2167,890 sampai 3027,6 mikrodetik. Maksimal *baudrate* yang dapat digunakan adalah 74880 bps. Perangkat CRYPTOBLE berhasil melakukan pengiriman data *ciphertext* dari pemancar ke penerima. Rata-rata kecepatan yang didapatkan sebesar 183,90 sampai 788,90 mikrodetik. Pada jarak 10 dan 100 meter tidak terdapat kendala namum pada jarak 200 meter terdapat data yang hilang disebabkan dengan terdapat sedikit penghalang. Menggunakan perangkat CRYPTOBLE data yang dikirimkan melalui radio lebih aman sehingga tidak mudah untuk dipecahkan.

VI. Kesimpulan

Perangkat dibuat sesuai dengan spesifikasi perancangan. Perangkat dinamakan CRYPTOGRAPHY PORTABLE, disingkat CRYPTOBLE dapat meningkatkan keamanan data dengan mengenkripsi data sebelum dikirim. Pengguna dibantu dengan aplikasi CRYPTOBLE Configuration untuk melakukan konfigurasi perangkat. CRYPTOBLE dapat dijadikan salah satu penunjang sistem keamanan data pada perangkat-perangkat nirkabel.

Referensi

[1] Soebroto A., Tibyani, Syafiiuddin, "Penerapan Advanced Encryption Standard (AES) Pada Radio Frequency Indetification (RFID) Untuk Sistem Pembayaran Tol Otomatis," Malang, 2010.

[2] Admin, "Miliki Celah Keamanan, Internet of Things Berpotensi Jadi Target Hacker," Techno.okezone.com, 2018. https://techno.okezone.com/read/2018/09/05/207/1946596/miliki-celah-keamanan-internet-of-things-berpotensi-jadi-target-hacker.

[3] Admin, "Strategi Cybersecurity dalam menghadapi pesatnya perkembangan IoT dengan dukungan 5G tech," hukumonline.com, 2019. https://www.hukumonline.com/berita/baca/lt5d7c64650b340/strategi-cyber-security-dalam-pesatnya-perkembangan-iot-dengan-dukungan-5g-tech

[4] Admin, "FBI Ungkap Modus Hacker Retas Perangkat IoT dan Tips Menghindarinya," Infokomputer.grid.id, 2019. https://infokomputer.grid.id/read/12913328/fbi-ungkap-modus-hacker-retas-perangkat-iot-dan-tips-menghindarinya.

[5] Admin, "Begini Cara Hacker Bobol Perangkat Smarthome dengan Malware," Infokomputer.grid.id. 2019. https://infokomputer.grid.id/read/121251315/begini-cara-hacker-bobol-perangkat-smart-home-dengan-malware.

[6] Admin, "Store: Arduino Nano," Arduino. 2020. https://store.arduino.cc/usa/arduino-nano.

[7] Upik J., Rakhmadany P., Rizal M, "Analsis Kinerja Pengiriman Data Modul Transceiver NRF24L01, Xbee dan Wifi ESP8266 Pada Wireless Sensor Network," E-ISSN: 2548-964X, Vol. 2, No. 4, hlm. 1510-1517, 2018.

[8] Nordic Semiconductor, "Single Chip 2.4 GHz Transceiver nRF24L01," Nordic Semiconductor ASA, 2006.

[9] Maxim Intefrated, "DS321 datasheet," Maxim Integrated Product, Inc, 2015.