PERANCANGAN SISTEM KOMUNIKASI KEYLESS PADA SEPEDA MOTOR BERBASIS ALGORITMA AES

DESIGN OF KEYLESS COMMUNICATION SYSTEM ON MOTORCYCLE BASED ON AES ALGORITHM

Eki Agung Nugroho[1], Sony Sumaryo[2], Porman Pangaribuan[3]
[1,2,3] Prodi S1 Teknik Elektro, Fakultas Teknik Elektro, Universitas Telkom
[1]nugrohoeki.agung@students.telkomuniversity.ac.id, [2] sonysumaryo@telkomuniversity.ac.id,
[3]porman@telkomuniversity.ac.id

Abstrak

Perkembangan teknologi sistem keamanan di kendaraan telah mendorong produsen kendaraan untuk menghasilkan sistem keamanan yang semakin ditingkatkan. Setelah dikembangkan di kendaraan roda empat, kini sistem keamanan ditingkatkan di kendaraan roda dua. Kebutuhan sistem keamanan pada sepeda motor mendorong produsen sepeda motor untuk meningkatkan sistem keamanan untuk produknya. Salah satu sistem kemanan yang dikembangkan adalah sistem penguncian dangan remote keyless.

Sistem remote keyless memerlukan komunikasi pada aplikasinya agar dapat digunakan secra wireless menggunakan modul NRF24L01 dan Arduino. Data yang akan dikirim secara wireless antara remote dengan modul receiver terlebih dahulu dienkripsi dengan algoritma AES untuk mengamankan informasi data pada modul tersebut yang dikirim dalam bentuk cipher, dan kemudian bagian penerima (receiver) akan menerima cipher dan merubahnya kembali dengan proses dekripsi ke dalam bentuk data asli yang sama pada modul kunci.

Hasil pengujian yang didapat dalam pengujian, remote keyless dengan menggunakan NRF24L01 dapat diimplementasikan pada jarak pada 1 meter hingga jarak 4 meter, data asli berhasil dikirim dalam bentuk cipher dan berhasil diubah menjadi data asli melalui proses dekripsi. Berdasarkan pengujian sistem, sistem remote keyless yang dibuat bekerja sesuai dengan yang diharapkan yaitu sepeda motor dapat diaktifkan jika Plain, Key, dan ID sesuai antara remote dan sepeda motor.

Kata Kunci: Keyless, remote, enkripsi, dekripsi.

Abstract

The development of technology in vehicle security system has encouraged manufacturers to produce vehicle security system that is increasingly enhanced. After being developed in four-wheeled vehicles, now improved security system at two-wheeled vehicle. Needs a security system on motorcycle motorbike manufacturers are pushing to improve the security system for its products. One of the security systems that are developed are locking system with remote keyless remote keyless system.

Keyless System need communications on the application so that it can be used in wireless using NRF24L01 module and Arduino. The data to be sent in wireless remote receiver module with between first encrypted with AES algorithms to secure data on the module information is sent in the form of cipher, and then the receiver (receiver) will receive the cipher and change it back to the process of decrypting the original data into the form on the same key modules.

The test results obtained in testing, remote keyless using NRF24L01 can be implemented at a distance of 1 meter for up to distance 4 meters, the original data is successfully sent in the form of cipher and successfully transformed into the original data through the process of decryption. Based on the test system, remote keyless systems made to work as expected, namely motorcycles can be activated if the Plain, Key, and ID match between the remote and the motorbike.Keywords: Keyless, remote, encryption, decryption.

Keywords : Keyless, remote, encryption, decryption.

---

1. Pendahuluan

Perkembangan dunia otomotif dapat diamati dengan munculnya berbagai inovasi yang diaplikasikan pada sebuah kendaraan. Produsen kendaraan terus mengembangkan inovasi untuk semakin meningkatkan kualitas produk kendaraan yang ditawarkannya dalam berbagai aspek yang diimplementasikan sehingga dapat menjadi nilai tambah dibanding dengan produk lainnya. Tak hanya produsen mobil saja yang meningkatkan inovasi, produsen sepeda motor pun kini telah bersaing untuk mengembangkan inovasi pada produknya. Salah satu fitur yang selalu ditingkatkan adalah fitur keamanan dan kepraktisan pada sepeda motor. Saat ini sistem penguncian pada sepeda motor secara umum masih menggunakan kunci konvensional yang dalam praktiknya masih terdapat kekurangan dalam hal keamanan. Hal ini menyebabkan mudahnya penjahat mengetahui celah keamanan pada penggunaan kunci konvensional.

Sistem remote keyless ini dipilih oleh penulis sebagai solusi untuk kemudahan dan keamanan kendaraan dibandingkan dengan menggunakan kunci konvensional. Sistem remote keyless ini merupakan sistem yang menggunakan modul kunci berupa remote yang memiliki transmitter dengan kunci digital unik untuk berkomunikasi dengan reciever mengirimkan data rahasisa, serta receiver pada modul penerima untuk mengolah data rahasia. Penggunaan sistem remote keyless ini akan memberikan kemudahan bagi pengendara untuk menyalakan dan mematikan sepeda motor. Dengan sistem ini pengendara tidak perlu lagi menggunakan kunci konvensional untuk menyalakan sepeda motor. Pengendara cukup mengantongi remote yang dapat secara otomatis berkomunikasi dengan modul yang ada didalam motor dengan radius tertentu. Kemudian pengendara sudah dapat mengaktifkan sepeda motornya dengan memutar knobnya saja.

Untuk memberikan keamanan, sistem penguncian dengan remote keyless ini tidak dapat diaktifkan jika remote dan sepeda motor tidak terdapat dalam radius tertentu [1], serta diperlukan suatu proses enkripsi pada data yang dikirimkan, dan proses dekripsi pada bagian penerima untuk mengubah kembali data yang sudah di terima. Pola enkripsi ini juga bertujuan agar data rahasia yang dikirimkan ke reciever di dalam motor tidak dapat diketahui dengan mudah, serta menghindari terjadinya kesalahan tertukarnya data oleh modul disetiap kendaraan jika terdapat beberapa sepeda motor dengan jenis dan merek yang sama.

2. Dasar Teori

2.1. Sistem *Remote Keyless*

Sistem Remote keyless merupakan modul kunci yang dipegang oleh pemilik sepeda motor selalu mentransmisikan gelombang pada frekuensi tertentu dan transceiver sepeda motor yang bertanggung jawab untuk menyalakan sepeda motor [2]. Jika seseorang membawa modul kuncinya mendekati sepeda motor dalam radius tertentu yang terjangkau oleh modul sistem yang terdapat di dalam sepeda motor, maka data yang ditransmisikan oleh modul kunci akan dapat diterima oleh modul di sepeda motor sehingga pengendara dapat langsung membuka kunci stang dan menyalakan sepeda motor. Sebaliknya, jika pemilik sepeda motor meninggalkan sepeda motor, maka pada radius jarak tertentu pemilik beserta modul kuncinya menjauhi sepeda motornya, sepeda motor tidak dapat dihidupkan.

2.2. Mikrokontroler

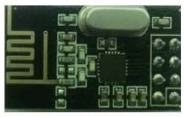
Mikrokontroler merupakan sistem komputer dalam bentuk *chip* IC (*Integrated Circuit*) yang berfungsi untuk memperoses atau ngengendalikan rangkaian elektronik dalam bentuk program yang dapat di tulis dan di hapus. Mikrokontroler pada umumnya terdiri dari CPU (*Central Processing Unit*), I/O yang dapat di program, memori. Mikrokontroler akan memperoses input berupa data atau input dari sensor yang kemudian digunakan untuk mengendalikan output berupa aktuator atau pun berupa data.

Gambar 1 RobotDyn Nano V3

Mikrokontroler yang digunakan adalah Nano V3 yang merupakan papan pengembangan dari RobotDyn dengan *bootloader* untuk Arduino IDE. Nano V3 merupakan mikrokontroler dengan *chip* IC ATmega 328p dengan ukuran yang kecil. Secara fungsional Arduino Nano dengan RobotDyn tidak berbeda , namun perbedaan terletak pada *jack power* DC dan penggunaan konektor *micro* USB. Nano V3 ini memiliki 14 pin input/output digital dan 8 pin input/output analog. Untuk pemrograman mikrokontroler ini menggunakan software Arduino IDE.

2.3. NRF24L01

Modul NRF24L01 merupakan modul transceiver frekuensi radio yang dapat berfungsi sebgai transmitter ataupun reciever. Transmitter terdiri dari sumber data, sinyal coder, pemancar, dan antena, dan untuk reciever terdiri dari antena, penerima sinyal encoder dan data interface [6]. Modul NRF24L01 digunakan untuk berkomunikasi secara wireless yang memanfaatkan gelombang radio pada frekuensi 2,4 GHz ISM (Industrial, Scientific, and Medical).

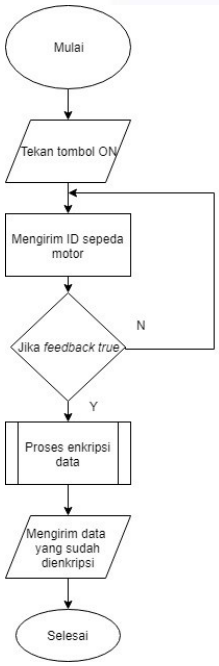


Gambar 2. NRF24L01

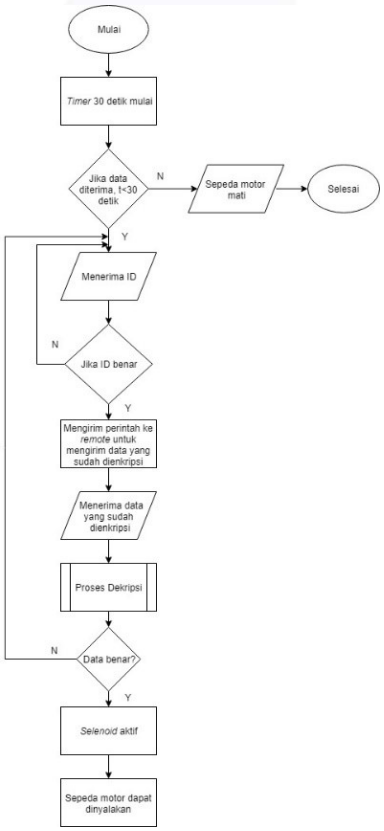
2.4. AES (Advanced Encryption Standard)

AES merupakan jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat proses enkripsi dan proses dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. AES mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit[10]. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan proses dekripsi. Berikut adalah perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan. Untuk proses enkripsi dan dekripsi Blok-blok data masukan dan kunci dioperasikan dalam bentuk array. Setiap anggota array sebelum menghasilkan keluaran ciphertext dinamakan dengan state terdiri dari baris byte. Dalam etiap state akan mengalami proses yang secara garis besar terdiri dari empat tahap yaitu, AddRoundKey, SubBytes, ShiftRows, dan MixColumns. Kecuali tahap MixColumns, ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap MixColumns tidak akan dilakukan pada tahap terakhir. Proses dekripsi adalah kebalikkan dari enkripsi yaitu chipertext dirubah menjadi data state.

2.4. Diagram Alir

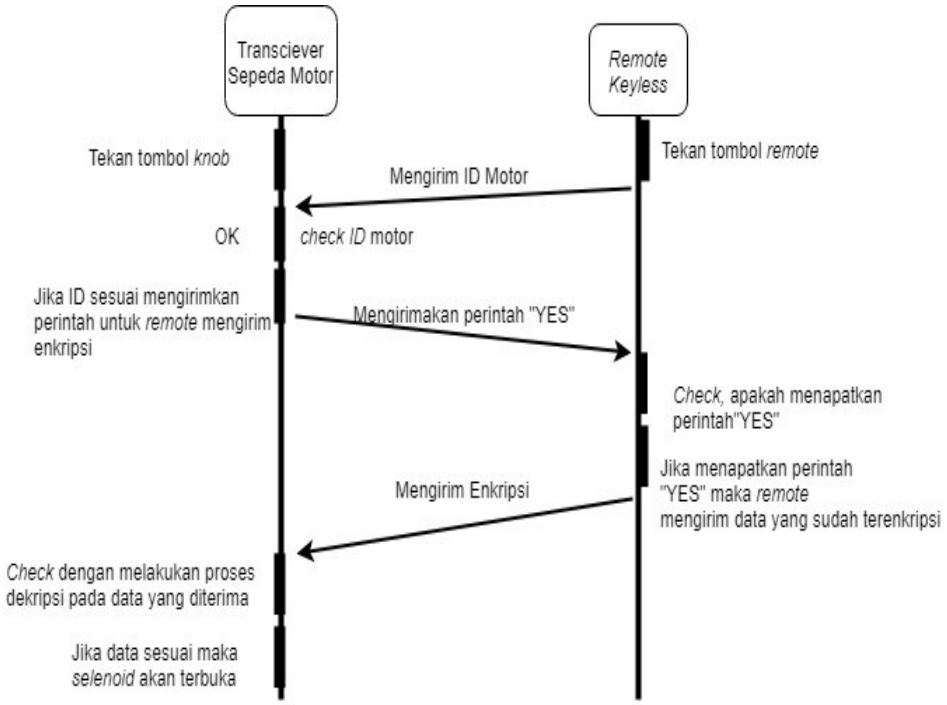


Gambar 3. Diagram *Remote Keyless*



Gambar 4. Diagram Modul Elektronik Kunci Kontak

2.5. Cara Kerja Sistem



Gambar 5. Proses Komunikasi Antara *Transceiver* Sepeda Motor dan *Remote Keyless*

3. Hasil Percobaan dan Analisa

3.1. Pengujian Waktu Untuk Proses Enkripsi dan Dekripsi

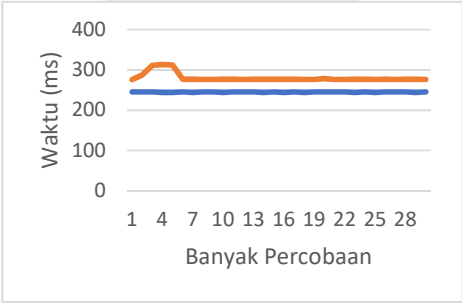
Tujuan : Untuk mengetahui waktu proses enkripsi dan dekripsi pada saat menyalakan sepeda motor.

Untuk melakukan proses enkripsi dan dekripsi digunakan:

Plain : 00112233445566778899aabbccddeeff

Key : 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f

Hasil Pengujian :



Gambar 6. Pengujian Waktu Enkripsi Dan Dekripsi

- Waktu Enkripsi = $\frac{\sum Waktu\ enkripsi}{\sum Banyaknya\ pengujian} = \frac{7340}{30} = 244{,}6667$ ms
- Waktu Dekripsi = $\frac{\sum Waktu\ dekripsi}{\sum Banyaknya\ pengujian} = \frac{8415}{30} = 280{,}5$ ms

Analisis:

Berdasarkan pengujian waktu dari proses enkripsi dan dekripsi sebanyak 30 kali dapat dilihat waktu untuk setiap proses enkripsi dan dekripsi data yang dikirim dan yang diterima diapat rata-rata hasil pengujian enkripsi sebesar 244,6667 ms dan untuk proses dekripsi 280,5 ms, sehingga rata-rata waktu yang dibutuhkan untuk proses algoritma AES adalah 525,1667 ms.

3.2. Pengujian Pengaruh Jarak Terhadap Keberhasilan Penerimaan Data

Tujuan : Pengujian ini bertujuan untuk mengetahui jarak komunikasi antara remote keyless dan modul elektronik kontak keyless, dengan hasil yang diharapkan modul dapat menerima data yang dikirim oleh remote dengan benar sehingga dapat menyalakan sepeda motor.

Hasil Pengujian :

Gambar 7. Pengujian Pengaruh Jarak Terhadap Keberhasilan Penerimaan Data

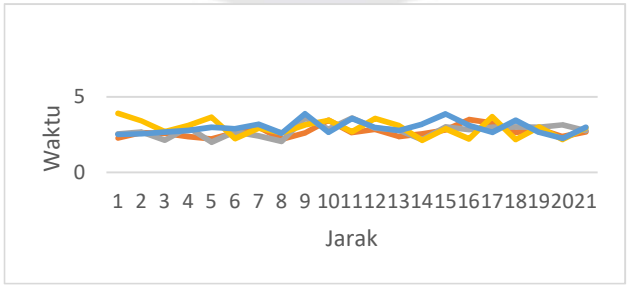
Analisis:

Berdasarkan hasil pengujian yang telah di lakukan, maka didapatkan hasil pengaruh jarak terhadap keberhasilan penerimaan data. Tingkat keberhasilan penerimaan data yang paling tinggi terdapat pada jarak 1 – 4 m dengan tingkat keberhasilan 100 % dari 20 kali pengiriman data. tingkat keberhasilan penerimaan data mulai menurun pada jarak lebih dari 4 m. Semakin jauh jarak antara *remote* dan sepeda motor maka tingkat keberhasilan modul elektronik pada sepeda motor menerima data semakin berkurang, hal ini dikarenakan modul elektronik sepeda motor tidak dapat menerima data secara sempurna.

3.3. Pengujian Pengaruh Waktu Terhadap Jarak

Tujuan :Pengujian ini bertujuan untuk mengetahui berapa waktu yang dibutuhkan untuk mengaktifkan solenoid. Pada pengujian ini jarak *remote* dan sepeda motor akan diubah-ubah. Perubahan jarak ini dilakukan untuk mengetahui apakah terjadi pengaruh antara jarak dan waktu untuk mengaktifkan solenoid. Parameter jarak uji yang akan diujikan berdasarkan pengujian pengaruh jarak terhadap keberhasilan penerimaan data, karena dalam pengujian ini akan dicari nilai waktu rata-rata dari setiap jarak.

Hasil Pengujian :



Gambar 8. Pengujian Pengaruh Waktu Terhadap Jarak Untuk Mengaktifkan Solenoid

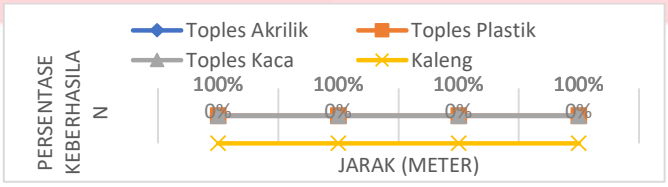
Analisis:

Hasil pengujian waktu terhadap jarak untuk mengaktifkan sepeda motor dipengaruhi oleh jarak sepeda motor dan *remote.* Semakin jauh letak posisi sepeda moror maka semakin lama waktu untuk menyalakan sepeda motor, namun perubahan selisih rata-rata waktu tiap jarak hanya sedikit. Untuk menyalakan sepeda motor pada jarak 1 meter didapatkan waktu rata-rata 2.694 s, pada jarak 2 meter didapatkan waktu rata-rata sebesar 2.7745 s, pada jarak 3 meter didapatkan waktu rata-rata sebesar 2.9425 s, pada jarak 4 meter didapatkan waktu rata-rata sebesar 2.986842s. Jarak 4 meter tersebut merupakan jarak optimal sepeda motor dan *remote* dapat saling berkomunikasi, selebihnya dari jarak tersebut sepeda motor dan *remote* tidak dapat berkomunikasi secara optimal.

3.4. Pengujian Pengaruh Medium Penghalang Terhadap Jarak Komunikasi

Tujuan **:**Pengujian jarak dengan penghalang dilakukan dengan memasukan *remote* yang dimasukan kedalam medium penghalang yang akan diujikan. Pengujian ini dilakukan untuk mengetahui apakah *remote* dapat teridentifikasi oleh modul elektronik pada sepeda motor jika *remote* tersebut dihalangi medium tertentu. Pengujian ini menggunakan beberapa media penghalang yaitu, toples akrilik, toples plastik, toples kaca, dan kaleng.

Hasil Pengujian:



Gambar 9. Pengujian Pengaruh Medium Penghalang Terhadap Jarak Komuniaksi

Analisis:

Terlihat pada grafik yang ditunjukan oleh gambar IV-4, bahwa modul elektronik kontak *keyless* tidak dapat menerima data jika *remote* dimasukan kedalam kaleng, namun pada medium kaca, plastik, dan akrilik, modul elektronik kontak *keyless* dapat menerima data dengan baik.

3.5. Pengujian Pengiriman dan Penerimaan Data

Tujuan **:** Tujuan dari pengujian sistem remote keyless adalah untuk menguji keamanan sistem remote keyless, apakah penggunaan ID , plain, dan key dapat berpengaruh terhadap keamanan sistem.

Tabel 2. Pengujian ID, *Plain*, dan *Key*

No	ID	*Plain*	*Key*	Keterangan
1	Sama	Sama	Sama	Berhasil
2	Beda	Sama	Sama	Tidak Berhasil
3	Sama	Beda	Sama	Tidak Berhasil
4	Sama	Sama	Beda	Tidak Berhasil
5	Beda	Beda	Sama	Tidak Berhasil
6	Beda	Sama	Beda	Tidak Berhasil
7	Sama	Beda	Beda	Tidak Berhasil
8	Beda	Beda	Beda	Tidak Berhasil

Analisis:

Berdasarkan hasil pengujian solenoid hanya dapat aktif jika ID, *plain,*dan kunci sesuai, jika ada salah satu komponen tersebut kurang maka, system tidak akan menyalakn *solenoid* sehingga sedikitpun perbedaan pada tiga komponen tersebut tidak sesuai maka sepeda motor tidak dapat dinyalakan.

4. Kesimpulan dan Saran

4.1.Kesimpulan

Berdasarkan hasil percobaan yang dilakukan dapat disimpulkan bahwa sistem yang diusulkan telah berhasil menjawab tujuan dari penelitian, karena:

1. Proses waktu enkripsi dan dekripsi dengan menggunakan plain dan key yang penulis gunakan memiliki waktu rata-rata enkripsi selama 244.6667 ms dan waktu rata-rata dekripsi selama 280.5 ms, sehingga waktu yang dibutuhkan dalam 1 kali proses enkripsi dan dekripsi adalah 525,1667.
2. Jarak terjauh antara remote dan sepeda motor agar modul elektronik dapat menerima data dengan keberhasilan 100% adalah 4 meter.
3. Waktu yang digunakan untuk menyalakan sepeda motor bergantung pada jarak antara sepeda motor dan *remote keyless*, dan waktu rata-rata yang didapat pada jarak 1 meter adalah 2.694 s dan pada jarak modul pada sepeda motor dapat menerima data dengan stabil pada jarak 4 meter dengan waktu rata-rata 2.986842s.
4. Berdasarkan pengujian sistem keamanan, sistem berhasil membaca seluruh data, jika data yang dikrimkan oleh remote sesuai dengan data yang terdapat pada sepeda motor maka, sepeda motor data dinyalakan, jika tidak sepeda motor tidak dapat dinyalakan.

4.2.Saran

Beberapa saran untuk mengembangkan penelitian ini antara lain:

1. Untuk meningkatkan kemanan dalam pengiriman data dengan menggunakan algoritma AES, dapat ditingkatkan dengan mengimplementasikan random peudeo number untuk tiap kali remote dinyalakan sehingga data yang dikirimkan akan berubah-ubah setiap remote dimatikan kemudian dinyalakan kembali.
2. Untuk mengurangi jarak pancar yang jauh, dapat diimplementasikan 2 jenis rf pada remote, satu rf dengan frekuensi kecil agar komunikasi kedua kendaraan lebih dekat, dan satu modul rf dengan frekuensi yang lebih besar untuk proses pertukaran data.

Daftar Pustaka

[1] B. M. D. Adiwidya, "Algoritma AES (Advanced Encryption Standard) dan Penggunaannya dalam Penyandian Pengompresian Data".

[2] Federal Information Processing Standards Publication 197, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," 2001.

[3] M. Ir. Yusuf Kurniawan, KRIPTOGRAFI KEamanan Internet dan Jaringan Komunikasi, BAndung: Informatika Bandung, 2004.

[4] P. Herdiansyah, "Analisis Keamanan dan Penerapan Kriptografi pada Sistem Keyless Entry Mobil," 2007.

[5] T. Glocker, T. Mantere and M. Elmusrati, "A Protocol for a Secure Remote Keyless Entry System Applicable in Vehicles using Symmetric-Key Cryptography," *8th International Conference on Information and Communication Systems (ICICS),* 2017.

[6] X. Lv and L. Xu, "AES Encryption Algorithm Keyless Entry System".

[7] A. M. K. Wardhana, D. A. . S. Asijah, MT and S. S. , "PERANCANGAN SISTEM KOMUNIKASI *WIRELESS* PADA KAPAL (MCST1- SHIP AUTOPILOT) DENGAN MEDIA KOMUNIKASI RF UNTUK MENDUKUNG SISTEM AUTOPILOT," 2012.

[8] K. N. D. Nofanti, . A. Rusdinar ST, MT, PhD and R. Nugraha S.Pd., MT., "PERANCANGAN DAN IMPLEMENTASI SISTEM KOMUNIKASI DAN KONTROL FORMASI PADA SWARM BOAT," *e-Proceeding of Engineering ,* vol. 4, p. 1580, 2017.

[9] F. Ellinger, Radio Frequency Integrated Circuits And Technologies, Zurich: Spinger, 2007.

[10] U. Jamil Shobrina, R. Primananda and . R. Maulana, "Analisis Kinerja Pengiriman Data Modul Transceiver NRF24l01, Xbee dan Wifi ESP8266 Pada *Wireless* Sensor Network," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer ,* vol. 2, pp. 1510-1517 , 2018.

[11] S. Kromodimoeljo, TEORI & APLIKASI KRIPTOGRAFI, SPK IT Consulting, 2009.

[12] Sugiyanto and R. K. Hapsari , "Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere," *ULTIMATICS,* vol. VIII, pp. 131-138, 2016.

[13] H. Pramaditya, "BRUTE FORCE PASSWORD CRACKING DENGAN MENGGUNAKAN GRAPHIC PROCESSING POWER," vol. 2, 2016.

[14] [Online]. Available: https://www.nayuki.io/page/aes-cipher-internals-in-excel. [Diakses 27 Agustus 2018].