elb-14-05-07.pdf

by

Submission date: 22-May-2023 03:12AM (UTC-0400)
Submission ID: 2099019875
File name: elb-14-05-07.pdf (1.09M)
Word count: 4888
Character count: 24549

ICIC Express Letters
Part B: Applications
Volume 14, Number 5, May 2023

ICIC International ©2023 ISSN 2185-2766
pp. 499–508

IMPROVED DATA SECURITY USING ADVANCED ENCRYPTION STANDARD ALGORITHM ON LONG-RANGE COMMUNICATION SYSTEM AT SMART GRID

Isminarti[1,2], Amil Ahmad Ilham[3,*], Ardiaty Arief[1] and Syafaruddin[1]

[1]Department of Electrical Engineering
[3]Department of Informatics
Universitas Hasanuddin
Jl. Poros Malino Km. 6, Bontomarannu, Gowa, Sulawesi Selatan 92171, Indonesia
isminarti20d@student.unhas.ac.id; ardiaty@eng.unhas.ac.id; syafaruddin@unhas.ac.id
*Corresponding author: amil@unhas.ac.id

[2]Department of Mechatronic Engineering
Politeknik Bosowa
Jl. Kapasa Raya No. 23, Makassar, Sulawesi Selatan 90245, Indonesia
isminarti@politeknikbosowa.ac.id

Received October 2022; accepted December 2022

Abstract. *Research on data security on smart grids is the main focus of this research. The long-range (LoRa) communication system has been developed and equipped with a capable security system. However, many obstacles in the field still cause the need to increase data security in this communication system. The advanced encryption standard (AES) algorithm improves data security on the sender and recipient sides through the encryption and decryption of messages. This research produces an encryption and decryption model using symmetric cryptographic block cipher type AES-256, which is then inserted into the modulation and demodulation process at the LoRa transmitter and receiver on the smart grid. The AES-256 block cipher in this study proves that the security messages sent are layered with a total text file processing time of 1.239 ms. The results of the occupied bandwidth simulation show that the bandwidth used is suitable for the ITU-R standard of 99%.*

Keywords: Security, AES, Ciphertext, Communication, Smart grid

1. **Introduction.** A smart grid is a two-way communication network where the role of information is very important in the process of energy transmission and distribution. The smart grid is a combination of ICT with computer processing capabilities and electrical systems to improve communication between users. Smart grid constraints are when exposed to various malicious cyber attacks that can destroy basic infrastructure and disruption of communication between networks and users [1]. Cyber security systems can be created on the smart grid by authenticating authenticated users. A researcher authenticates a two-way smart meter between a smart meter on the customer side and a server on the utility side. This study presents a key model (cryptography) with two-way authentication between smart meters and utility, and then examines the LPWAN protocol architecture to evaluate cyber attack behavior on smart grids [2]. Other researchers have also investigated security issues in smart grids on the customer and electricity provider side and proposed a methodology to improve secure communication wherein their research shows that, as the spurious factor increases, the detection time by the proposed algorithm increases [1]. A research community is also developing suitable analytical models that can play an important role in the study of smart grid technologies, and a mathematical model is proposed that accurately estimates the probability of success of LoRaWAN network

DOI: 10.24507/icicelb.14.05.499

packets on bidirectional traffic, i.e., uplink (UL) and downlink (DL) transmissions, and accounts for the most important features of LoRa chipsets and the LoRaWAN standard [3]. LoRa can measure the reliability of a communication system from network performance where failure can be divided into two factors, namely intrinsic factors (hardware, software, communication protocols, etc.) and extrinsic factors (weather conditions, malicious agents, terrorist attacks, etc.) [4]. A researcher using the collision-free low-latency multi-hop LoRa network protocol proposed a prototype LoRa node using the MultiTech mDot module. The results showed that the proposed protocol provides the following: high reliability, parallel transmission, minimized number of times and assigned slots for all links in the network [5]. Security research is also researched [6] by analyzing that LoRaWAN reduces communication power by setting different transmission latencies for different end devices, and AES does not take encryption strength into account, the AES encryption process results in lower power consumption of up to 26.2%. Other researchers also provide an overview of the AES algorithm and explain some of the important features of this algorithm in detail and demonstrate some previous research that has been done by comparing it with other algorithms such as DES, 3DES, and Blowfish. This research is not head to head because it compares with the old algorithm that since January 1997, the US National Institute of Standards and Technology (NIST) announced the start of an initiative to develop a new encryption standard namely AES and in 2002, its name was changed to advanced encryption standard (AES) and published by NIST. The new encryption standard will become the federal information processing standard (FIPS), replacing the old data encryption standard (DES) and triple-DES [7]. A researcher uses SX1278 to send data in the form of small packets based on wide-area radio technology where the main problem from LoRa technology revealed in the study is the average packet loss when sending data is almost 50%, i.e., there is a 0.5 chance that packets will not be received at the receiving side and to improve the reliability and security of the data sent, the researcher proposes a basic logic to make sending and receiving packets more reliable using the concept of packet serialization and securing it using the AES algorithm [8]. Other researchers discuss security risks in IoT LoRaWAN-based applications that aim to increase data security resilience using untrusted network servers and then set security measures. The payload format proposed in this study provides data confidentiality and an additional layer of integrity to reduce the risk of using untrusted network servers. The researcher uses the AES-128 encryption algorithm using the CBC (cipher block chaining) operating mode, which focuses on parallelization using FPGA [9]. Other research also improves data security resilience in IoT LoRaWAN-based applications that use untrusted network servers. The payload format proposed in this study provides an additional data confidentiality and integrity layer to reduce the risk of using untrusted network servers [10].

This study aims to produce encryption and decryption models using symmetric cryptography of the AES-256 block cipher type inserted into the LoRa transceiver modulation and demodulation process on the smart grid to increase the reliability of the LoRa communication system. This research will contribute to the solutions previously researched by [1-3,5,6,8]. [9] used AES-128 by modifying the payload and using an FPGA with parallel processing so that the time required for sending messages was faster than the sequential processing used in this study, but the FPGA datasheet was able to run the process up to us. Researchers have not received a research that uses AES-256, so the processing time value works very quickly. The contribution of this research is to produce a LoRa communication system transceiver model on a smart grid using the AES-256 algorithm to improve data security on the modulation and demodulation process with a total text file processing time of 1.239 ms which requires high constraints in maintaining data confidentiality.

The outline of the paper is organized as follows. Section 2 explains the data security systems, including the encryption and decryption processes and modulation and demodulation processes. Section 3 reviews the proposed method using encryption and decryption in the modulation and demodulation model on LoRa. Section 4 presented the simulation result and discussion. Section 5 concludes this paper and addresses our future studies.

2. Data Security Systems.

The data security system is the main thing in maintaining the information/messages/data that will be conveyed. The communication network on the smart grid requires data security that is difficult for profit-seeking parties to hack, so to maintain the security of data information conveyed by the transmitter to the receiver is safe against threats, a layered security level using cryptography is needed.

2.1. Encryption and decryption process.

Cryptography is a method to protect data (encrypt and decrypt information) from intruders or to prevent unauthorized access when transferring data over an open channel network. The decryption process must be known by the sender and recipient. There are 2 types of encryption in cryptography, namely symmetric key cryptography, and asymmetric key cryptography, and symmetric key cryptography will be discussed in this study. Symmetric key cryptography relies on a single key for the encryption and decryption of information. This key needs to be kept secret and the sender and recipient have the same key, which is different from asymmetric key cryptography which uses a different secret key so that it requires more processing time [11-13].

Encryption is the process of encoding data to prevent intruders from reading the original data easily. This stage can convert the original data (plaintext) into an unreadable format known as ciphertext. While decryption is the opposite of encryption. This is the process of converting ciphertext to original text without losing any words in the input text. The cryptographic process relies on mathematical calculations with substitutions and permutations with or without keys. Today, the network has an important role to transfer data accurately and quickly from source to destination. Data is not secure enough to be transferred strictly confidential. Information security has become one of the main challenges of sharing resources with data communication over computer networks.

DES (data encryption standard) and AES are both symmetric block ciphers. DES has a minor key size, making it less secure to beat triple DES but slower. The essential complexity between DES and AES is that in DES, the plaintext square is isolated into two halves before the main computation starts. In AES, the entire square is arranged to obtain the ciphertext. DES is a more established computation, and AES is computation driven, faster, and more secure than DES. AES (advanced encryption standard) is an encryption-decryption algorithm for data. AES supports keys with lengths of 128, 192, and 256 bits. This cryptographic key encrypts and decrypts data in blocks of 128, 192, and 256 bits. AES was developed based on algebraic operations and multiple encryption cycles for communication security which NIST nominated as an algorithm that is capable of high computational efficiency and can be used in various applications, especially in high-speed broadband links. Table 1 represents the features of AES.

AES consists of 3 block ciphers namely AES-128, AES-192 and AES-256 [14,15]. The basic structure of AES is shown in Figure 1.

Parameters, symbols, and algorithm functions as shown in Figure 1 are presented as follows.

1) The plaintext is input data or messages in the form of text to the cipher or output from the inverse cipher which will be sent from the transmitter through the encryption process and to the receiver through the decryption process so that the input data received is the same as the output data or plaintext.

TABLE 1. AES features [11]

Features	AES
Block size (bits)	128
Key size (bits)	128, 192, or 256
Matrix orientation	Input is mapped column-wise
Number of rounds	10, 12, or 14
Key expansion	Dedicated expansion algorithm
GF (28) polynomial	x8+x4+x3+x+1 (011B)
Origin of S-box	The multiplicative inverse in GF (28) plus affine transformation
Origin of round constants	Elements 2i of GF (28)
Diffusion layer	Left multiplication by 4×4 circular MDS matrix (2,3,1,1) – mix columns
Permutations	Shift rows

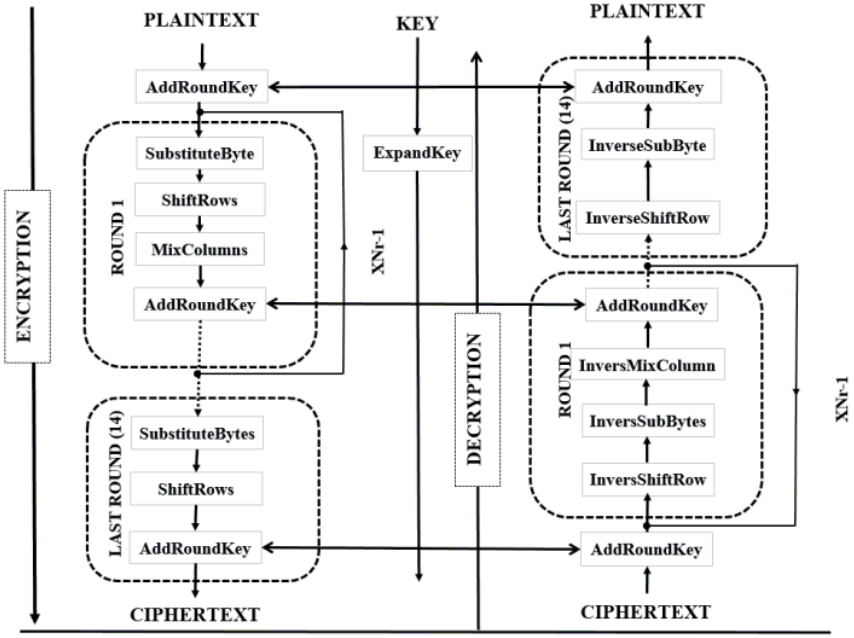


FIGURE 1. Basic structure of AES [16,17]

2) AddRoundKey() is a transformation in cipher in the encryption process and InverseCipher in the decryption process where RoundKey is added using XOR operation. The length of the RoundKey is equal to the size of the State, in this study we use the value Nb = 4 so that the length of the RoundKey is equal to 128 bits/16 bytes [15]. Nb is the number of columns (32-bit words). In this study, we used the AES-256 block cipher with Nk = 8, Nb = 4, and Nr = 14.
3) SubstituteByte() is a non-linear byte substitution that operates independently on each byte state using a substitution table (S-box). Table 2 presents substitution S-box tables, namely non-linear substitution tables used in several byte substitution transformations in encryption and decryption.

TABLE 2. Substitution table (S-Box) and inverse substitution table (Invers S-Box)

(a) Encryption process [12-14]

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(b) Decryption process

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

The byte substitution process is carried out to modify the data in a nonlinear way to hide the relationship between the original and the encrypted message.

4) ShiftRow() is the process of shifting rows from one another to increase the complexity of the algorithm, in this process, the first row is skipped, the second row is moved to one place, the third row is moved to two places and the last row is moved three places. ShiftRow is done in the encryption process while in the decryption process it is called InversShiftRows. Row shifting and column mixing will result in random data.
5) MixColumns() is a vertical random process so that with byte transposition, the encryption process is much more complicated so that the encryption results are very sophisticated and difficult to hack unless someone has a secret key.

AES algorithm is made using the FIBS-197 standard. This algorithm is not built for speed and does not hide text messages. The function executes AES-256 based on the key size. The function also does not check if the key or input size is the correct length and will error if it is not the correct size.

2.2. **Modulation and demodulation process.** Spread spectrum LoRa is a patented modulation developed by Semtech (https://www.semtech.com/) based on chirp spread spectrum (CSS) modulation. LoRa modulation is often referred to as "chirp modulation" [18]. LoRa (Long Range) provides long-distance and low power consumption, low data rate, and data transmission security. On public, private, or hybrid networks, LoRa can be used to achieve more comprehensive coverage than cellular networks. LoRa technology can easily integrate with existing networks and enable low-power battery-operated Internet of Things (IoT) applications. LoRa uses radio signals where these signals carry no information other than a transmitter that is constantly on. The signal must be modified in some way to convey information. Several ways can be done; two of the most popular methods are to alter the amplitude and the frequency [19]. CSS was developed for radar applications in the 1940s and used in military and aerospace communications. LoRa offers a trade-off between sensitivity and data rate while operating on fixed bandwidth channels of 125 kHz (for uplink channels) and 500 kHz (for downlink channels). In addition, LoRa uses an orthogonal dispersion factor. This higher spread factor provides increased processing gain and higher reception sensitivity [8].

In the demodulation process resampling can be done to balance the data, that is, draw a sample from some of the available data. Sampling is divided into two, namely undersampling and oversampling. The oversampling technique takes the minority class so that the proportion in the sample is greater than the original proportion.

3. **Proposed Method.** In this study, we insert an encryption process at the LoRa transmitter to improve data security at the transmitter and also the decryption process at the receiver side. The method used in this study is experimental, namely testing the speed

and the security of the encryption and decryption of messages in the modulation and demodulation process using AES-256 security to improve data security with a high level of reliability. In this study, the researcher encrypts the message "MODELING AND SIMULATION OF LONG RANGE (LORA) COMMUNICATION SYSTEM ON SMART GRID" using a plaintext transposition cipher. The number of columns in plaintext is 79, so it uses a 4×4 matrix. The text will be filled in the row first using five 4×4 matrices, as presented in Figure 2.

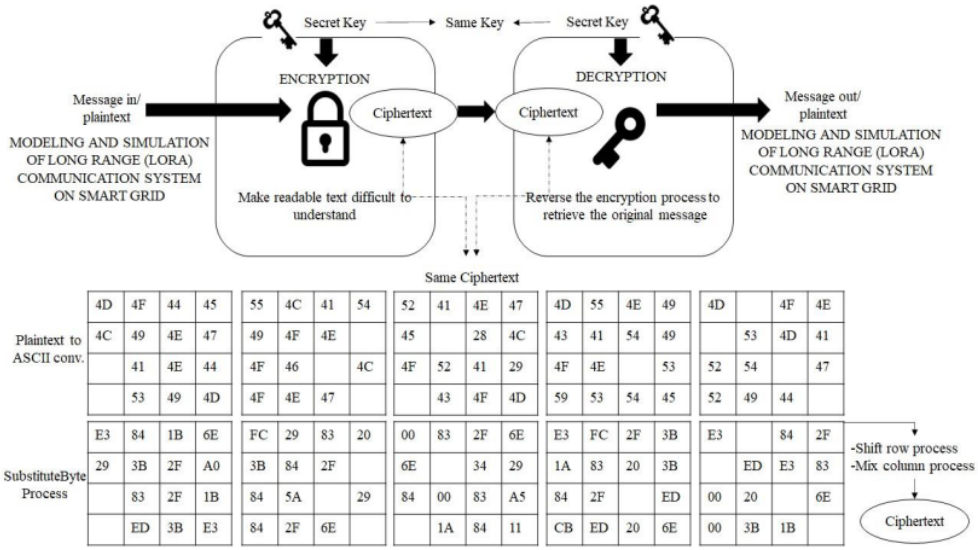
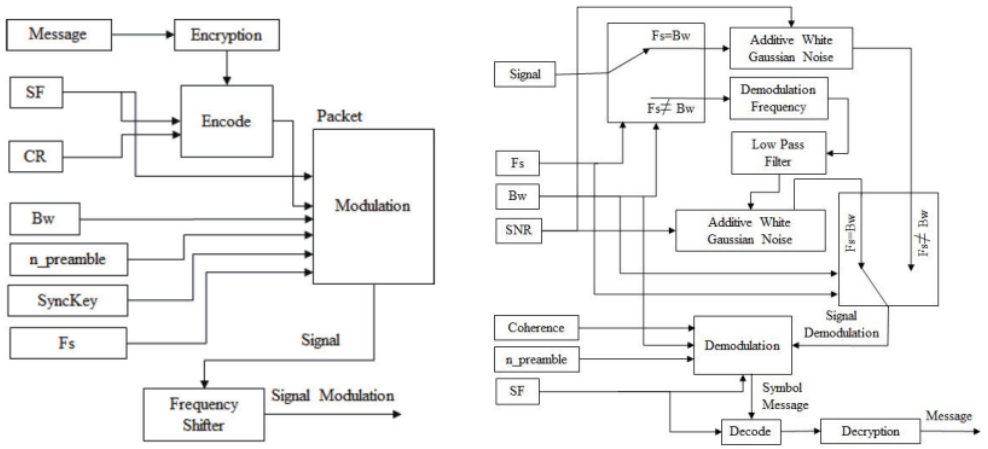


FIGURE 2. Encryption and decryption process on symmetric keys cryptography

After the first stage, converting plaintext into ASCII code as shown in the picture, the next stage is to substitute byte, shift row, mix column, and then add round key up to 14 rounds. This process then produces ciphertext which is processed at the transmitter and then the ciphertext "aa33decbb022ca90b73b7d74ec82c7112e5e4024bbb0f6529c85e91104213c8ae36a7c39699e5fb2da0775447545b51d0ad48a0e78f1c7eaa60236f292b22832f4076e1bca430d2c480868898bb3f3" and secret key "01213243546576879 8a90a1b2c3d0e0f102342132435465768798a0b1c2d3e4f" received at the receiver are processed at the receiver until it produces the same plaintext as the message. The transmit power in this study is 14 dBm with 158 columns of encrypted messages. The encryption and decryption processes at the transmitter and receiver are presented in Figure 3.

The block diagram above Figure 3(a) is a signal modulation process using encryption with 6 parameter values, namely SF = 10, CR = 1, Bw = 125 kHz, n_preamble, SyncKey, and Fs = 10 MHz. The encode block encodes the encrypted message, and in this process, the SF and CR parameters are also used. The modulation block receives packets from the encrypted message to produce a signal that is then sent to the frequency shifter to produce a modulation signal.

In Figure 3(b), the signal modulation will receive in the transmitter. If the value of Fs = Bw, then the process will be carried out on AWGN; if not, it will be forwarded to the frequency modulation process using MFSK and filtered using LPF. Signal interference or interference in overlapping bands distorts so that AWGN processes the following procedure. This study tested the sending of data messages with several iterations to see the system's reliability [20]. Either unlicensed spectrum causes AWGN and fading interference. Radio spectrum congestion is correlated with population density, and it is



(a) Modulation on LoRa transmitter (b) Demodulation on LoRa receiver

FIGURE 3. Secure data signal

essential to measure it, especially in urban environments. It has also been demonstrated that spectrum availability varies spatially and temporally [21].

Thus, the impact of interference cannot be abstracted into a single parameter but needs to be modeled statistically or can be regenerated based on empirical measurements. The emulated LoRa frames are then linearly summed with the collected measurements. LoRa demodulated its signal below 19.5 dB of the noise floor. In contrast, LoRa utilizes an unlicensed spectrum to cause the noise as one of the significant channel disturbances. Therefore, the impact of interference cannot simply be abstracted into a single parameter such as an average but needs to be modeled statistically or regenerated based on empirical measurements. Thus, the SDR is configured to capture the radio spectrum near the expected gateway location. Supposedly there is significant interference variability throughout the day. In that case, it is essential to collect interference measurements and sample this variability over different periods, then run the emulator during those periods. In the demodulation process, the symbol message is decoded and decrypted on the receiving side, producing a message according to the initial information. The testing and validation results using Matlab prove that the data sent is the same as the information received.

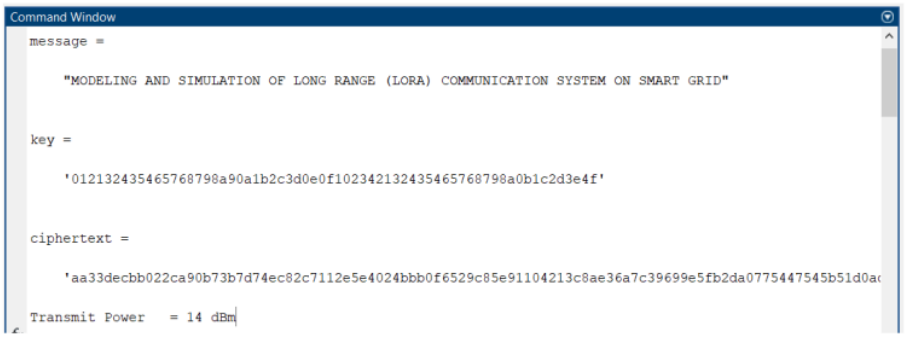
4. **Simulation Results and Discussion.** This research produces a simulation of sending data packets by encrypting and decrypting messages authenticated with a secret key. Figure 4 shows that this study succeeded in simulating messages with a high level of security.

As an illustration in Figure 4, the simulation results describe the process of sending and receiving messages. The result of the processing time of the AES-256 function presents in Table 3.

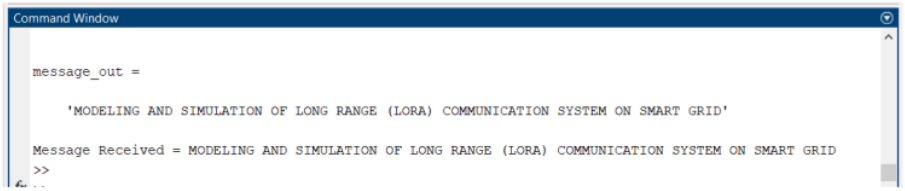
In this study, AES-256/256 bit/32 bytes using a microcontroller, the SubstituteByte function produces an average processing time of 0.303 ms with a substitution process of 83 times, ShiftRow = 0.031 ms with a shift process of 70 times, MixColumn = 0.877 ms with a substitution process by 65 times and AddRoundKey = 0.028 ms with a logical XOR process of 75 times.

In Figure 5, the difference in spectrogram time is getting closer, indicating that the data sent is very long because it goes through a layered authentication process so it takes twice as long as the transmission process without encryption. The LoRa packet

transmission spectrogram with 14 dBm of power and 99% occupied bandwidth indicates that the bandwidth used has complied with ITU-R standards [22].



(a) Simulation of the encryption process

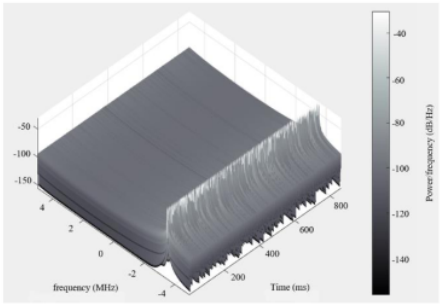


(b) Simulation of the decryption process

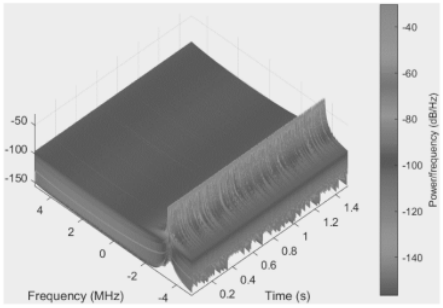
FIGURE 4. Simulation results of encryption and decryption of messages

TABLE 3. Processing time of AES-256

AES-256 using microcontroller	
Function	**Processing time (ms)**
SubstituteByte	0.303
ShiftRow	0.031
MixColumn	0.877
AddRoundKey	0.028
Total	**1.239**



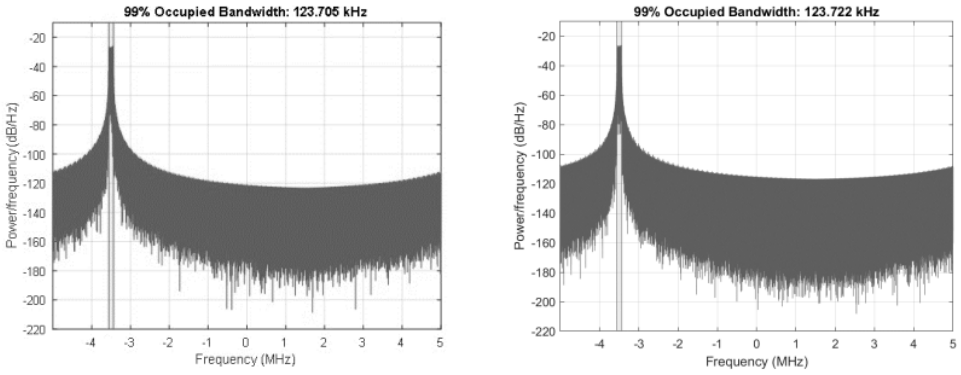
(a) Without security



(b) With AES-256 security

FIGURE 5. (color online) The spectrogram on LoRa packet transmission with 14 dBm power

In Figure 6 the width of the occupied bandwidth is also under the standards set for equipment in several areas, such as Japan and the United States. Here ITU-R defines it as the maximum bandwidth, excluding emissions that do not exceed a certain percentage of total emissions.



(a) Without security (b) With security

FIGURE 6. Width of occupied bandwidth

5. **Conclusions.** This study has investigated the capability of an AES-256 block cipher in the LoRa communication network to send messages with layered security and a total text file processing time of 1.239 ms. The message sending process with and without security remains the same on the occupied bandwidth with 99% accuracy. The LoRa packet spectrogram indicates a longer access speed because this AES algorithm is not made to generate speed and text messages. The input message in the LoRa packet can also be displayed because it is not hidden, nor does it check whether the key or input size is long or short. In addition, the data message is secure and safe as long as the secret key is not detected. In the process of sending messages with and without protection, the message is well received, but the time it takes is a little longer. Finally, we will discuss our future study to calculate the error rate in the data by comparing analytical and numerical calculations to produce higher computations in LoRa communication systems.

Acknowledgment. This research is a part of the doctoral dissertation and granted with the research scheme of Penelitian Disertasi Doktor (PDD) 2022 sponsored by the Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia.

REFERENCES

[1] T. Chen, X. Yin and G. Wang, Securing communications between smart grids and real users; providing a methodology based on user authentication, *Energy Reports*, vol.7, pp.8042-8050, 2021.

[2] A. Panagi, *Exploring Communication Features and Security Vulnerabilities of Long-Range (LoRa) Networks*, Bachelor Thesis, Cyprus University of Technology, 2021.

[3] M. Capuzzo, D. Magrin and A. Zanella, Mathematical modeling of LoRa WAN performance with bi-directional traffic, *2018 IEEE Global Communications Conference (GLOBECOM)*, pp.206-212, 2018.

[4] J. P. Astudillo Leon and L. J. de la Cruz Llopis, Emergency aware congestion control for smart grid neighborhood area networks, *Ad Hoc Networks*, vol.93, 101898, 2019.

[5] D. L. Mai and M. K. Kim, Multi-hop LoRa network protocol with minimized latency, *Energies*, vol.13, no.6, 1368, 2020.

[6] K. L. Tsai, Y. L. Huang, F. Y. Leu, I. You, Y. L. Huang and C. H. Tsai, AES-128 based secure low power communication for LoRaWAN IoT environments, *IEEE Access*, vol.6, pp.45325-45334, 2018.

[7] J. Daemen and V. Rijmen, *The Design of Rijndael*, Springer-Verlag, Berlin, Heidelberg, 2002.
[8] A. Madaan, S. Bansal, A. Sahu and F. Kidwai, Peer to peer communication in GUI interface using LoRa technology, *Procedia Computer Science, ICITETM2020*, vol.173, no.2019, pp.299-304, 2020.
[9] A. Barrera, C. W. Cheng and S. Kumar, Improved mix column computation of cryptographic AES, *Proc. of the 2nd International Conference on Data Intelligence and Security*, pp.229-232, 2019.
[10] P. De Moraes and A. F. Da Conceicao, Protecting LoRaWAN data against untrusted network servers, *Proc. of IEEE Congress on Cybermatics: 2021 IEEE International Conferences on Internet of Things (iThings 2021), IEEE Green Computing and Communications (GreenCom 2021), IEEE Cyber, Physical and Social Computing (CPSCom 2021) and IEEE Smart Data*, pp.99-106, 2021.
[11] N. Mavrogiannopoulos, *Secure Communications Protocols and the Protection of Cryptographic Keys*, Ph.D. Thesis, Katholieke Universiteit Leuven, 2013.
[12] W. Stallings, *Cryptography and Network Security*, 4th Edition, Prentice Hall Pub, 2005.
[13] H. Y. Chang, J. J. Wang, C. H. Chen and C. Y. Lin, Efficient authentication steganographic systems based on a client-server model with random-like codes, *International Journal of Innovative Computing, Information and Control*, vol.18, no.2, pp.633-644, 2022.
[14] V. S. Aparna, A. Rajan, I. Jairaj, B. Nandita, P. Madhusoodanan and A. A. S. Remya, Implementation of AES algorithm on text and image, *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI 2019)*, pp.1279-1283, 2019.
[15] National Institute of Standards and Technology, *FIPS 197: Announcing the Advanced Encryption Standard (AES)*, 2001.
[16] A. Singh, P. Agarwal and M. Chand, Analysis of development of dynamic S-Box generation, *Computer Science and Information Technology*, vol.5, no.5, pp.154-163, 2017.
[17] A. M. Abdullah, Advanced encryption standard (AES) algorithm to encrypt and decrypt data, *Cryptogr. Netw. Secur.*, 2017.
[18] L. Vangelista, Frequency shift chirp modulation: The LoRa modulation, *IEEE Signal Processing Letters*, vol.24, no.12, pp.1818-1821, 2017.
[19] P. Seneviratne, *Begining LoRa Radio Networks with Arduino*, Apress Berkeley, CA, 2019.
[20] U. Noreen, A. Bounceur and L. Clavier, A study of LoRa low power and wide area network technology, *The 3rd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP 2017)*, 2017.
[21] B. Al Homssi, K. Dakic, S. Maselli, H. Wolf, S. Kandeepan and A. Al-Hourani, IoT network design using open-source LoRa coverage emulator, *IEEE Access*, vol.9, pp.53636-53646, 2021.
[22] I. Sm, *Recommendation ITU-R SM.328-10 Spectra and Bandwidth of Emissions*, 1999.

elb-14-05-07.pdf

ORIGINALITY REPORT

12%	8%	10%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	link.springer.com Internet Source	2%
2	dokumen.pub Internet Source	1%
3	www.icicelb.org Internet Source	1%
4	joyslab.files.wordpress.com Internet Source	1%
5	Poliana De Moraes, Arlindo Flavio Da Conceicao. "Protecting LoRaWan data against untrusted network servers", 2021 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), 2021 Publication	1%
6	Submitted to ECPI College of Technology Student Paper	1%

7	telegra.ph Internet Source	1 %
8	Dinh Loc Mai, Myung Kyun Kim. "Multi-Hop LoRa Network Protocol with Minimized Latency", Energies, 2020 Publication	1 %
9	Submitted to Gitam University Student Paper	1 %
10	M. Somasundara Rao, K. Venkata Rao, M. H. M. Krishna Prasad. "Hybrid Security Approach for Database Security using Diffusion based cryptography and Diffie-Hellman key exchange Algorithm", 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021 Publication	1 %
11	sunnypapers.com Internet Source	1 %

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	On		