# Security Performance of Advanced Encryption Standard 128 for Long-Range Communication System

Isminarti[1, 3, a), e)], Syafaruddin[1, b)], Amil Ahmad Ilham[2, c)], and Ardiaty Arief[1, d)]

[1]*Department of Electrical Engineering, Universitas Hasanuddin*
*Jl. Poros Malino Km.6 Bontomarannu, 92127 Gowa South Sulawesi, Indonesia*
[2]*Department of Informatics, Universitas Hasanuddin*
*Jl. Poros Malino Km.6 Bontomarannu, 92127 Gowa South Sulawesi, Indonesia*
*3Department of Mechatronic Engineering, Politeknik Bosowa*
*Jl. Kapasa Raya No. 23 daya, 90241 Makassar, Indonesia*

[a)] *Corresponding author: isminarti20d@student.unhas.ac.id*
[b)] *syafaruddin@unhas.ac.id,* [c)] *amil@unhas.ac.id,* [d)] *ardiaty@eng.unhas.ac.id,* [e)] *isminarti@politeknikbosowa.ac.id*

**Abstract.** Despite having outstanding security characteristics, the Advanced Encryption Standard (AES) algorithm has lately become vulnerable due to the rise of cryptanalysts. Improving this algorithm's security is crucial due to the widespread commercial use of AES. This research creates a security system on a Long-Range (LoRa) communication system utilizing the AES 128 algorithm to achieve faster processing times in the encryption and decryption process of messages using MATLAB to enhance security performance. The AES-128 block encryption in this inquiry demonstrates that the messages were transmitted in layers with an average processing time of 0.74 milliseconds (ms) for each function. The duration for encryption and decryption is 5.89 ms.

## INTRODUCTION

The rapid rise of cloud-based data applications has made it essential to protect data during transmission. Specific cryptographic techniques and procedures were devised to provide confidentiality, data protection, communication, authorization, and non-repudiation. Mathematical methods are used in cryptography to turn data into confidential information that only authorized people can access. Cryptography can be divided into two categories: symmetric and asymmetric. Two keys are used in asymmetric cryptography: a public key for encryption and a private key for decryption. These algorithms include SSL, RSA, SSH, and DH. This study will develop encryption and decryption models by integrating symmetric cryptography of the AES-128 block cipher type into the LoRa transceiver modulation and demodulation process on communication systems.

Symmetric cryptography encrypts and decrypts the message using the same key. AES, CAS, RC6, TEA, IDEA, Serpent, Twofish, and other algorithms are included in this category (1–4).

The AES algorithm uses 128-bit sequences for input and output (digits with values of 0 or 1). These sequences are occasionally referred to as blocks, and the length is the number of bits they hold. A 128-bit string serves as the AES algorithm's Cipher Key. This standard's scope prohibits using other input, output, and Cipher Key lengths. Such sequences will have bits numbered from zero to one less than the length of the line (block length or key length). The number $i$ attached to a bit is known as its index and will be in one of the ranges $0 < i < 128$ (5). For wireless networks, AES is used to secure communication (6) (7).

The National Institute of Standards and Technology (NIST) of the United States government has standardized the symmetric encryption known as Advanced Encryption Standard. AES features keys that are 128 bits, 192 bits, and 256 bits long. The number of rounds in the encryption process depends on these key lengths: AES 128-bit, 192-bit, and 256-bit have 10, 12, and 14 rounds, respectively (8). The AES algorithm requires two inputs, like other kinds of encryption: plaintext and cipher key. To create ciphertext, a succession of AES encryption algorithms is applied to the plaintext using a cipher key. Using the AES-128 method, this research's contribution is to provide the fastest processing times possible for text files. This will increase data security during the encryption and decryption process.

The outline of the paper is organized as follows. The next section explains the related work about AES 128 security systems, including the encryption and decryption processes. The following section presents the result and discussion, and the last section is a conclusion of the best processing time of the works.

## RELATED WORK

Other studies concentrate on creating and examining the CBC (Cipher Block Chaining) mode implementation of the Mix Columns AES-128 algorithm. Parallelism in signal processing results in less virtual memory, logical components, and encryption time in the mix columns portion (9).

A researcher enhances the reliability of data security in IoT LoRaWAN-based applications that use unreliable network servers. Tests were run on a prototype IoT LoRaWAN system to compare outcomes with and without the security measure. The proposed payload format reduces the risks associated with using an unreliable network server by adding additional data security and integrity layers. When data includes 96 bytes, resulting in a payload format of 104, the overhead is at its highest and equals 31.2 seconds in duration (10).

Another researcher improved the security strength of the AES algorithm by showing the reasons for the loopholes in AES and provided a solution using a Symmetric Random Function Generator (SRFG). The use of randomness in the key generation process in block cipher is novel in this domain. They also compared their results with the original AES based on parameters such as nonlinearity, resiliency, balancedness, propagation characteristics, and immunity. The results suggest that, compared to the original AES, RK-AES has three times greater confusion qualities and a 53.7% better avalanche impact. The time required by the modified key expansion module, which forces a trade-off between security and time, is the constraint of their current work (11).

## Encryption Process

The widely used technology of encryption greatly aids data security. The AES algorithm encrypts data using a specific structure to offer the highest level of security. It uses several rounds to accomplish that, with four subprocesses in each round. To encrypt a 128-bit block, there are four steps in each cycle (12)(5). **FIGURE 1** presents the encryption stage consisting of three stages: SubstitutionBytes, ShiftRows, MixColumns, and AddRoundKey.

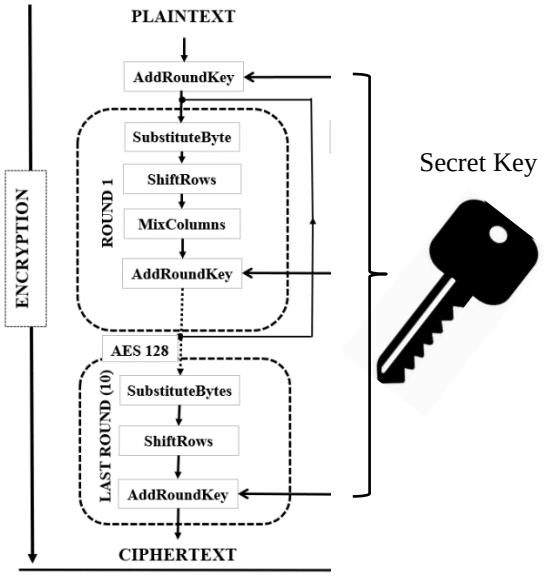


**FIGURE 1.** Encryption process in AES 128 security systems structure

The encryption process starts from plaintext/ message and then AddRoundKey (addresses the Round Key with an additional pointer). After this function, The SubBytes transformation uses a substitution table to perform a non-linear byte separately on each substitution box (S-box) byte. In the ShiftRows, the final three-line conditions' bytes in this function are cyclically shifted through the different numbers of bytes. The next function is processed column by column via the MixColumns transformation, which treats each column as a four-term polynomial.

## Decryption Process

Decryption is the procedure used to recover the encrypted data's original form. The key that was obtained from the data sender is the foundation of this procedure. The sender and the receiver need the same key to encrypt and decrypt data with an AES algorithm, and the decryption procedure is similar to the encryption process in reverse order. As shown in **FIGURE 2**, the final round of the decryption stage consists of three steps: InverseShiftRow, InverseSubByte, InverseMixColumn, and AddRoundKey.

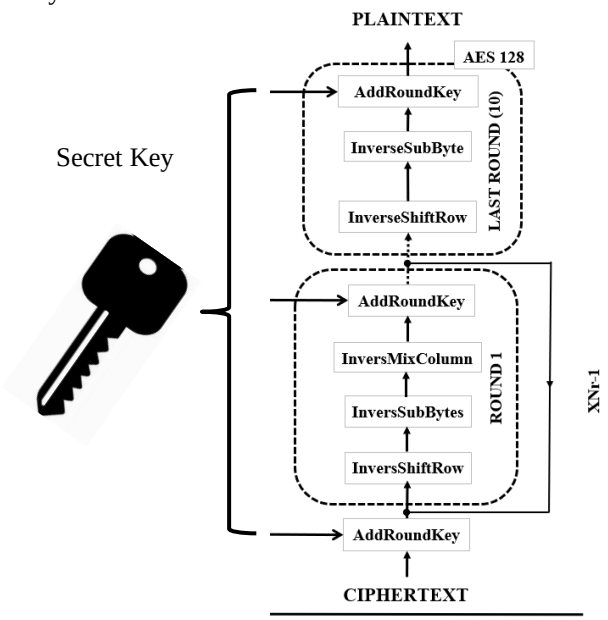


**FIGURE 2.** Decryption process in AES 128 security systems structure

Block ciphers offer security services using the Advanced Encryption Standard (AES) as a common algorithm. There are several variations of this technology available for network security. Strengthening the security of this algorithm is essential, given the use of AES in commercial applications. The AES structure's decryption operation is shown in **FIGURE 2.**

## RESULT AND DISCUSSION

The author describes AES 128 methods using 10 round keys in this study. **FIGURE 1** illustrates the AES algorithm's operation. The key in this cryptography process is "60000102030400e1f10f," while the plaintext utilized is the hexadecimal code "00112233445566778899aabbccddeeff." Ciphertext "8ea2b7ca516745bfeafc49904b496089" is the result of the encryption operation. **TABLE 1** shows the results of this investigation.

**TABLE 1.** Processing Time of AES 128.

| Function | | Processing Time (ms) | Step (times) |
|---|---|---|---|
| **Encryption** | **Decryption** | | |
| SubstituteByte | InverseSubByte | 0.55 | 30 |
| ShiftRow | InverseShiftRow | 0.21 | 10 |
| MixColumn | InversMixColumn | 1.7 | 9 |
| AddRoundKey | AddRoundKey | 0.48 | 11 |
| | **Average** | **0.74** | |

The plaintext is encoded to the same Hex code as the decryption output, which is as follows: "00112233445566778899aabbccddeeff."

This study used a logical XOR process to generate the Substitute Byte function for AES 128/128 bit/16 bytes. The results of this study show that an AES algorithm can create a faster processing time with a significant step, with an average processing time of 0.74 ms for each function. The duration for encryption and decryption is 5.89 ms.

## CONCLUSION

The Rijndael Mix Column model is one technique that can be built to enhance the performance of communication systems in terms of security and time, according to the AES algorithm. Time simulations of each operation function in the encryption and decryption process are carried out in this study using MATLAB. This research's contribution is to provide the fastest processing times possible for text files. This will increase data security during the encryption and decryption process. This study used a logical XOR process to generate the Substitute Byte function for AES 128. The results of this study show that an AES algorithm can create a faster processing time with a large step, with an average processing time of 0.74 ms for each function. The duration for encryption and decryption is 5.89 ms. In future work, we will optimize the authentication process on the transceiver.

## ACKNOWLEDGMENTS

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. Wahid NA, Ali A, Esparham B, Marwan M. A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. J Comput Sci Appl Inf Technol. 2018;3(2):1–7.

2. Mewada S. Classification of Efficient Symmetric Key Cryptography Algorithms. Int J Comput Sci Inf Secur. 2016;14(2):105–10.

3. Ramakrishnan S. Cryptographic and Information Security. Cryptographic and Information Security. books.google.com; 2018.

4. Ganguly D. Cryptography and Network Security. fourth. Network and Application Security. 2012. 31–46 p.

5. National Institute of Standards and Technology. 197: Announcing the advanced encryption standard (AES). Vol. 2009, … Technology Laboratory, National Institute of Standards …. 2001. 8–12 p.

6. Savolainen PT, Kyntäjä T, Vallant H, Marksteiner S, Aertgeerts A, Van HaleWeyck L, et al. Structured Overview of Communication Standards for Smart Grids. 2015;1–72.

7. Daemen J, Rijmen V. The Design of Rijndael. Vol. 1, New York. Printed in Germany: © Springer-Verlag Berlin Heidelberg 2002; 2002. 255 p.

8. Hayati N, Ramli K, Suryanegara M, Suryanto Y. Potential Development of AES 128-bit Key Generation for LoRaWAN Security. 2019 2nd Int Conf Commun Eng Technol ICCET 2019. 2019;57–61.

9. Barrera A, Cheng CW, Kumar S. Improved Mix Column Computation of Cryptographic AES. Proc - 2019 2nd Int Conf Data Intell Secur ICDIS 2019. 2019;229–32.

10. De Moraes P, Da Conceicao AF. Protecting LoRaWan data against untrusted network servers. In: Proceedings - 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, SmartD. IEEE; 2021. p. 99–106.

11. Saha R, Geetha G, Kumar G, Kim TH. RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys. Galdi C, editor. Secur Commun Networks. 2018;2018:9802475.

12. Muhammad Abdullah A, Muhamad Abdullah A. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. Eastern Mediterranean University; 2017.