Increased AES 128 Security to AES 256 for Long-Range Communication System Reliability

Isminarti*, Syafaruddin, Amil Ahmad Ilham and Ardiaty Arief
Department of Electrical Engineering,
Universitas Hasanuddin
Jl. Poros Malino Km.6 Bontomarannu, 92127, Gowa, Sulawesi Selatan, Indonesia
Department of Mechatronic Engineering
Politeknik Bosowa
Makassar, Indonesia
*isminarti20d@student.unhas.ac.id; isminarti@politeknikbosowa.ac.id.

Abstract – The AES algorithm has excellent security features, but recently, with the increasing number of cryptanalysts. The popularity of AES in commercial use makes it essential to strengthen the security of this algorithm. This study builds a security system on a Long-Range (LoRa) communication system using the AES algorithm by comparing AES 128 and AES 256 to produce faster processing times in the encryption and decryption process of messages using MATLAB to improve system reliability. This research develops a modulation and demodulation model for data at the LoRa transmitter and receiver using the symmetric cryptographic block cipher type AES. The use of the block ciphers AES-128 and AES-256 in this investigation shows that the messages were sent in layers, taking a total amount of time to parse a text file of 5.89 milliseconds for AES 128 and 5.70 milliseconds for AES 256.

Index Terms – AES, LoRa, symmetric, cryptographic block cipher, processing times

I. INTRODUCTION

It has become crucial to protect data during transmission due to the rapid development of cloud-based data applications. Specific cryptographic techniques and procedures had developed to offer confidentiality, data protection, communication, authorization, and non-repudiation. Cryptography processes employ mathematics to transform data into private information only authorized persons can read. There are two categories of cryptography: symmetric and asymmetric.

The message is encrypted and decrypted using the same key in symmetric cryptography. This category includes algorithms like Blowfish, DES, 3DES, AES, CAS, RC6, TEA, IDEA, Serpent, Twofish, and others [1]–[3].

Asymmetric cryptography employs two keys: a public key for encryption and a private key for decryption. This group of algorithms includes DH, SSH, RSA, and SSL. This study will create encryption and decryption models that integrate symmetric cryptography of the AES-256 block cipher type into the LoRa transceiver modulation and demodulation process on the smart grid.

There are two categories of network performance: intrinsic variables (hardware, software, communication protocols, etc.) and extrinsic factors (weather conditions, malicious agents, terrorist attacks, etc.) [4].

II. RELATED WORK

A researcher has identified the cause of the AES gap and offered a remedy by utilizing a symmetric random function generator (SRFG). When using randomness for key generation in block ciphers, the nonlinearity, resilience, balance, propagation properties, and immunity of the original AES and SRFG are compared [5]. Other researchers focus on the development and analysis of the implementation of the Mix Columns AES-128 algorithm using CBC (Cipher Block Chaining) mode. In terms of encryption time and delay in the mix columns section, parallelism in signal processing produces less delay time, logical elements, and virtual memory [6]. A researcher examines unique features using on-fly keys instead of pre-computed key algorithms in related research. The pre-computed algorithm spends more time during different encryption iterations using the AES 128/192/256 comparison, implemented using the fly key generation module in the architectural design. Encryption achieves maximum throughput for AES 256, so the architectural approach is more efficient than the algorithmic in AES design [7].

This study compares AES 128 and 256 to produce optimal processing time using MATLAB in the encryption and decryption process. To improve the processing time of AES 256, the researchers compared the processes that occurred in AES 128 and developed the iteration process to get faster processing times.

III. RESULT AND DISCUSSION

Block ciphers use the Advanced Encryption Standard (AES) as a standard algorithm to provide security services. In network security, this method is accessible in numerous versions. This algorithm has excellent security features. However, it was also recently deciphered by the cryptanalysis procedure. The popularity of AES in commercial use makes it imperative to strengthen this algorithm's security. Fig. 1 presents the process of encryption and decryption in the AES structure.

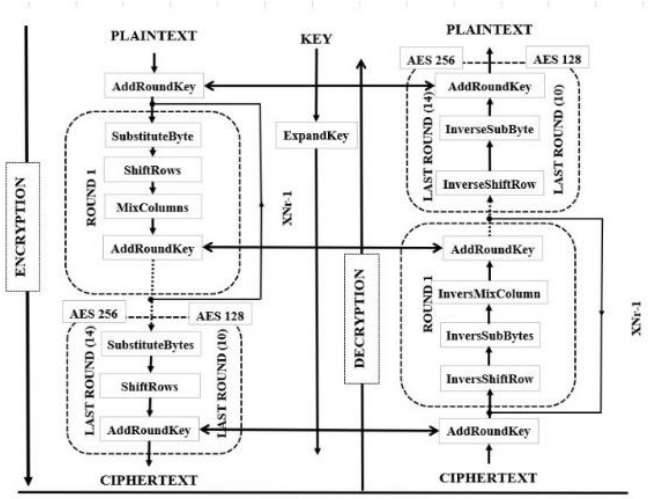

Fig. 1. AES Structure [8]–[10]

Fig. 1 describes the process of the AES algorithm; in the picture, the author describes two algorithms, namely AES 128 with 10 round keys and 14 round keys for AES 256. In this cryptography process, the plaintext used is in the form of hexa code '00112233445566778899aabbccddeeff' and the key used is '000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f' for AES 256 and '60000102030400e1f10f. The encryption process produces Ciphertext '8ea2b7ca516745bfeafc49904b496089' and the decryption output produces the same hexa code as the plaintext as follow '00112233445566778899aabbccddeeff'. The results of this study can be seen in TABLE 1 as follows.

TABLE 1. COMPARING PROCESSING TIME OF AES 128 AND AES 256

Function	AES 128		AES 256	
	Processing Time (ms)	Step (times)	Processing Time (ms)	Step (times)
SubstituteByte	0.55	30	0.48	40
ShiftRow	0.21	10	0.20	14
MixColumn	1.70	9	2.10	13
AddRoundKey	0.48	11	0.06	15
Total	**5.89**		**5.70**	

In this study, AES 128/128 bit/16 byte and AES 256/256 bit/32 bytes have Substitute Byte function produces an average processing time of 0.07 ms difference, ShiftRow = 0.01 ms, MixColumn = 0.4 ms and AddRoundKey = 0.42 ms with a logical XOR process. The results of this study prove that with a long step, an AES algorithm can produce a faster processing time where the average time required for each function is 0.74 ms for AES 128 and 0.71 ms for AES 256. The encryption and decryption process is 5.89 ms on AES 128 and 5.70 ms on AES 256.

IV. 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.

V. REFERENCES

[1] N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention," *J. Comput. Sci. Appl. Inf. Technol.*, vol. 3, no. 2, pp. 1–7, 2018.

[2] S. Mewada, "Classification of Efficient Symmetric Key Cryptography Algorithms," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 2, pp. 105–110, 2016.

[3] D. Ganguly, *Cryptography and Network Security*, Fourth. 2012.

[4] L. C. Hwang, C. S. Chen, T. T. Ku, and W. C. Shyu, "A bridge between the smart grid and the Internet of Things: Theoretical and practical roles of LoRa," *Int. J. Electr. Power Energy Syst.*, vol. 113, pp. 971–981, 2019.

[5] R. Saha, G. Geetha, G. Kumar, and T. H. Kim, "RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys," *Secur. Commun. Networks*, vol. 2018, p. 9802475, 2018.

[6] A. Barrera, C. W. Cheng, and S. Kumar, "Improved Mix Column Computation of Cryptographic AES," *Proc. - 2019 2nd Int. Conf. Data Intell. Secur. ICDIS 2019*, pp. 229–232, 2019.

[7] A. D. Report, M. O. F. Engineering, C. Networks, U. The, and G. Of, "SECURED WIRELESS COMMUNICATION USING AES-256," 2015.

[8] A. Singh, P. Agarwal, and M. Chand, "Analysis of Development of Dynamic S-Box Generation," *Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 154–163, 2017.

[9] A. Muhammad Abdullah and A. Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," Eastern Mediterranean University, 2017.

[10] 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.