International Journal of Engineering & Technology, 7 (3.4) (2018) 318-320

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Implementation of AES Algorithm for Information Security of Web-Based Application

Janner Simarmata[1], Tonni Limbong[2], Misalina BR Ginting[2], Romanus Damanik[2], Muhammad Irwan Padli Nasution[3], Abdul Halim Hasugian[3], M Mesran[4], Abdul Sani Sembiring[4], Harvei Desmon Hutahaean[5], Insan Taufik[5], Paska Marto Hasugian[5], Hengki Tamando Sihotang[5], Asaziduhu Gea[6], Marlyna Infryanty Hutapea[6], Indra Kelana Jaya[6], Doli Hasibuan[6], Alfonsus Situmorang[6], Jimmy Febrinus Naibaho[6], Junika Napitupulu[6], Sonny Leston Hutabarat[7], Muhammad Ikhsan Setiawan[8], Marzuki Sinambela[9]

[1]Universitas Negeri Medan, Medan-Indonesia
[2]Universitas Katolik Santo Thomas Medan, Medan-Indonesia
[3]Universitas Islam Negeri Sumatera Utara, Medan-Indonesia
[4]STMIK Budi Darma, Medan-Indonesia
[5]STMIK Pelita Nusantara, Medan-Indonesia
[6]Universitas Methodist Indonesia, Medan-Indonesia
[7]Sekolah Tinggi Ilmu Komputer Medan, Medan-Indonesia
[8]Department of Civil Engineering, Narotama University, Surabaya – Indonesia
[9]Badan Meteorologi, Klimatologi dan Geofisika Wilayah 1, Medan - Indonesia
**Corresponding author E-mail: jannersimarmata@unimed.ac.id*

Abstract

This study focused on designing a web-based information security system to secure text and image files using the AES (Advanced Encryption Standard) algorithm to encrypt and decrypt text and image files. This web-based system is designed to help users easily access applications online. The conclusion of this study proves that the AES Algorithm method is a very good algorithm in securing text and image files, and with this web-based information security application, information confidentiality is more awake and in the decryption process, the results of the decryption file contents are not changed at all.

Keywords: *AES Algorithm, Information Security , Encryption, Decrytion*

1. Introduction

Encryption is the process to secure the information to ensure the security of sensitive information. One effort securing information systems that can be done is cryptography. This technique is used to transform data into specific codes, with the purpose of the information stored or transmitted over insecure networks (such as the Internet) cannot be read by anyone except those who are eligible [1]–[4].

Encryption algorithm is the process of scrambling data so that it cannot be read by doing various substitutions and transformations in plaintext (original message) and converting them into ciphertext (random messages). Encryption algorithms are grouped into two general categories: Symmetric-key (also called secret-key) and asymmetric-key encryption (also called public key) [5]–[9].

Advanced Encryption Standard (AES) is a cryptographic algorithm and encryption standard proposed by NIST to replace DES in 2001. Use of the AES algorithm supports a combination of data (128 bits) and a key length of 128 bits (AES 128), 192-bit (AES 192), and 256-bit (AES 256) depending on the length of the key. Things to distinguish from each AES-128 uses 10 rounds, AES-192 with 12 rounds, and AES-256 with 14 rounds.

2. Related Works

2.1 Advanced Encryption Standard (AES)

The AES algorithm is a symmetrical block cipher that can encrypt and decrypt data. As shown in Figure 1, encryption converts data (plain-text) into an incomprehensible form called cipher-text, while decryption converts these ciphers back to plain text [10]. 128, 192, or 256-bit cryptographic keys can be used by the AES algorithm to encrypt and decrypt data in 128-bit blocks.

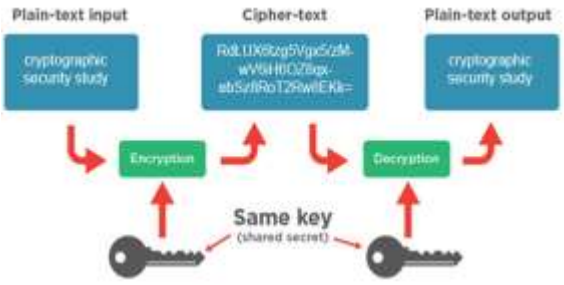


Fig. 1: Symmetric Block Cipher

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The algorithm starts with the key stage Add round followed by nine rounds of four stages and the tenth stage of the three stages that applies to encryption and decryption algorithms [11].

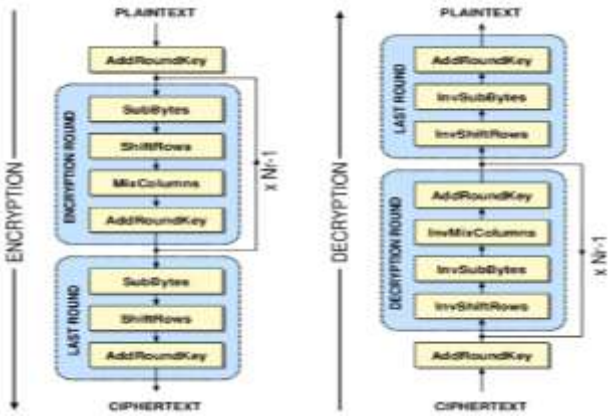


Fig. 2: Design flow of AES Algorithm encryption and decryption process

Table 1: Key length and number of rounds

Algorithm	Key length (Nk Words)	Block size (Nb Words)	Number of rounds (Nr)
AES-128	128 bits	4 words (16 bytes)	10
AES-192	192 bits	4 words (16 bytes)	12
AES-256	256 bits	4 words (16 bytes)	14

Table 1 shows the different keys and number of rounds and associated block sizes [12].

2.2 Modes of Operation of AES Encryption Algorithm (AES Cipher)

There are five modes of operation recommended by NIST that can be used [13]. Each mode of operation has its own parameters which are important to provide the necessary security of the algorithm [14]. The five modes of operation: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR) [13][15].

3. Result and Discussion

In the system implementation phase produces a web-based application to process encryption and decryption of text and image files using the AES algorithm. The key block length used is 128, 196 and 256 in ECB and CBC modes. The main view of the application can be seen in Figure 3.

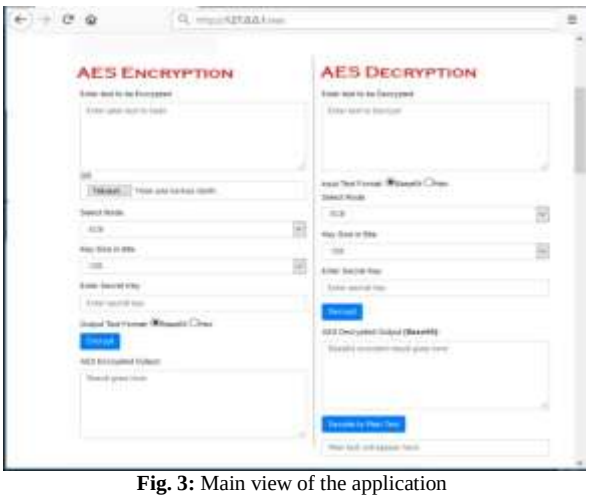


Fig. 3: Main view of the application

The AES algorithm has a 128-bit block size, with a key length of 256, 192 or 128 bits. When a symmetrical cipher mode requires an IV, the length of the IV must be the same as the block cipher size. Therefore, you must always use 128 bit IV (16 bytes) with AES.

For encryption, enter plain text or image files that you want to encrypt. Then select the Electronic Code Book (ECB) mode, while plain text input will be divided into several blocks and each block will be encrypted with the key provided. CBC mode is highly recommended and requires IV to make each message unique. If no IV is entered then by default it will use the Cipher Block Chaining (CBC) mode.

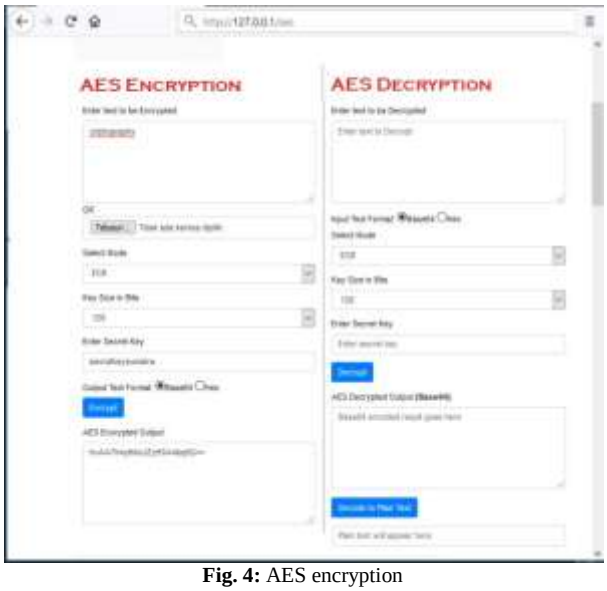


Fig. 4: AES encryption

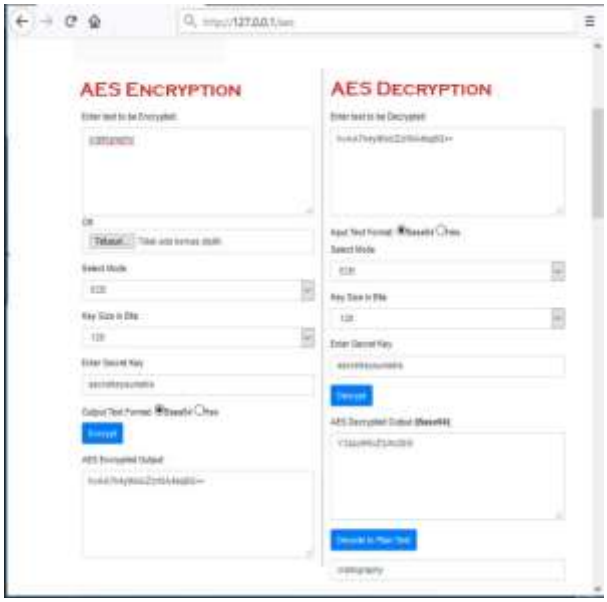


Fig. 5: AES decryption

4. Conclusion

Protecting data from attacks is difficult. One way to secure data from attacks is to use encryption, 0ne of them by using the AES encryption method. Based on the results of the implementation that has been carried out that the application of the AES (Advanced Encryption Standard) algorithm for information security both web-based text and image files runs well. Web-based applications are able and can help users to encrypt and decrypt text and image files.

References

[1] J. Simarmata, "Pengamanan Sistem Komputer," *Andi, Yogyakarta*, 2006.

[2] G. Gunawan *et al.*, "Mobile Application Detection of Road Damage using Canny Algorithm," in *Journal of Physics: Conference Series*, 2018, vol. 1019, no. 1, p. 12035.

[3] R. Rahim *et al.*, "Internet based remote desktop using INDY and socket component," *Int. J. Eng. Technol.*, vol. 7, no. 2.9, pp. 44–47, 2018.

[4] B. Silaban and T. Limbong, "Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction," *Media Inf. Anal. dan Sist.*, vol. 2, no. 2, pp. 14–20, 2017.

[5] G. Singh and S. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 33–38, 2013.

[6] J. Simarmata, "Pengenalan Teknologi Komputer dan Informasi," *Yogyakarta Andi*, 2006.

[7] A. Widarma, "COMBINATION AES, RC4 AND ELGAMAL ALGORITHM IN HYBRID SCHEME FOR DATA SECURITY," *Comput. Eng. Sci. Syst. J.*, vol. 1, no. 1, pp. 1–8, Jan. 2016.

[8] T. Limbong and P. D. P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of Matlab."

[9] R. Rahim *et al.*, "Block Architecture Problem with Depth First Search Solution and Its Application," *J. Phys. Conf. Ser.*, vol. 954, no. 1, 2018.

[10] G. Gunawan *et al.*, "Mobile Application Detection of Road Damage using Canny Algorithm," in *Journal of Physics: Conference Series*, 2018, vol. 1019, no. 1.

[11] M. S. Reddy and M. Y. A. Babu, "Evaluation Of Microblaze and ImplementationOf AES Algorithm using Spartan-3E," *Int. J. Adv. Res. Electr. Electron. Instrum. Energy*, vol. 2, no. 7, pp. 3341–3347, Jan. 1970.

[12] R. Anokye, E. S. Bakar, A. Y. Abare, R. M. Kalong, and A. Muhammad, *The difference in density along the bamboo culms of Gigantochloa scortichinii and Bambusa vulgaris*. 2014.

[13] M. J. Dworkin, "Recommendation for block cipher modes of operation : National Inst of Standards and Technology Gaithersburg Md Computer Security Div," 2007.

[14] D. Blazhevski, "Modes of operation of the aes algorithm," no. Ciit, pp. 212–216, 2013.

[15] A. Altigani, M. Abdelmagid, and B. Barry, "Analyzing the Performance of the Advanced Encryption Standard Block Cipher Modes of Operation: Highlighting the National Institute of Standards and Technology Recommendations," *Indian J. Sci. Technol.*, vol. 9, no. 28, 2016.