The Effect of Plaintext Length on Round Trip Time With Client Server Based Advanced Encryption Standard (AES) Algorithm

Alfian Agusnady¹, Opim Salim Sitompul¹, T Tulus, Berti Sari Sembiring¹, Titin Qowidho¹
¹ Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan – Indonesia
* alfianagusnady@gmail.com

Abstract. The length of the plaintext affects the round trip time, where the longer the plaintext, the longer round trip time. In an attempt of 35 plaintext characters obtained 1.171 ms round trip time. Whereas on an attempt of 113 plaintext characters obtained 2.355 ms round trip time. In Figure 2 can be seen the graph increase of the round trip time. The author concludes that the length of the plaintext affects the round trip time in the client server based AES algorithm. The longer the plaintext, the longer the round trip time process will run.

Keywords : Cryptography, Advanced Encryption Standard (AES).

1. Introduction
The rapid development of technology allows humans to communicate and exchange information/data without being blocked by distance. Along with this, the demands of security for the confidentiality and interchangeable information are also increasing.

The Advanced Encryption Standard (AES) is an algorithm that functions to secure data. The AES algorithm is a block of symmetrical ciphertext that can encrypt (encipher) and decrypt (decipher) information. This algorithm uses 128, 192, and 256 bit cryptographic keys to encrypt and decrypt data on 128 bits blocks. In addition, AES has advantages in security, speed, and algorithm characteristics along with its implementation. AES is symmetric encryption standard recommended by NIST. AES is most effective algorithm to provide security in message transmission [1].

2. Related Research
Kyungtae Kang, et al, apply the Advanced Encryption Standard (AES) method in blocking the code in the background. The AES decryption process uses new analytical models to predict the time and energy needed to solve the problem of the cellphone receiver [2].

Erkay Savas, et al, the research applies the Advanced Encryption Standard (AES) algorithm for there are several different cache-based attack categories; namely, access-driven, trace-pus and time-driven attacks. This method aims to detect attacks, attacks, and minimize the costs of different threats, and optimize attacks.. [3].

Monodeep Kar, et al, the research demonstrate an integrated inductive voltage regulator (IVR) to optimize side-channel-attack (PSCA) attacks from 128-bit Advanced Encryption Standard (AES-128) engines. By applying AES algorithm key-byte can be extracted and inhibits key extraction[4].
3. Proposed Method

3.1. Cryptography
Cryptography is the science or art to maintain the confidentiality of information or messages by encoding them in a form that cannot be understood anymore [5]. Cryptography is a method to maintain data security so that data confidentiality and authenticity can be guaranteed and can improve the security aspects of data or information. Cryptography supports the need for two aspects of information security, namely protection to the confidentiality of information and protection against forgery and alteration of information submitted from the sender to the recipient of the information [6].

3.2. Advanced Encryption Standard Algorithm
The AES algorithm is a symmetric block cipher, as for the sender and receiver using the same key for encryption and decryption. The data block length is set to 128 bits and the key length can be 128, 192, or 256 bits [7].

AES is an example of a symmetric algorithm, it has a key for the sender and receiver, both to encrypt and decrypt text or data. AES is an algorithm for the implementation of hardware and software and works better in hardware [8].

4. Results and Discussion
The research that the author did on analyzing the effect of plaintext length on round trip time with client server based algorithm to provide several plaintext with different characters length. The test can be seen on Figure 1 as the test result can be seen on Table 1.

| No. | Plaintext Description                                                                 | Character Length | Ciphertext                                                                 | Round Trip Time |
|-----|---------------------------------------------------------------------------------------|------------------|---------------------------------------------------------------------------|-----------------|
| 1.  | Morphological process and labeling.                                                    | 35               | :?@÷?©<?£?(ã=f3ãô,Éhœ=÷M9 μn0£ÔÖ1_@*JuÉ9                                    | 1,171 ms        |
| 2.  | In this work we use color and object movement detection.                              | 56               | #2?*÷ú÷ßΛ4z÷e÷ñ a?jWindows Client Java                                      | 1,405 ms        |
| 3.  | After we finished with calibration procedure, next step is detection and              | 90               | {?AVèun&c AcO÷<P?÷h=E70U                                                   | 1,458 ms        |

Figure 1a. Server

Figure 1b. Client
tracking process.

4. As for each process of detecting and tracking, we conduct a search using a reference model in the video frame that we use as input.

5. In the process of detection using several materials such as shape, color, object movement, texture, and edges.

From Figure 1 and Table 1 can be seen that the length of plaintext affect the round trip time. Where the longer the plaintext, the longer the round trip time. On 35 characters plaintext test, the author obtained 1,171 ms round trip time. Whereas on 113 character plaintext test, the author obtained 2,355 ms round trip time. In Figure 2 can be seen the round trip time graph is increasing.

![Figure 2. Round Trip Time Graph](image)

Therefore it can be concluded that the length of plaintext affect the round trip time on client server based AES algorithm. The longer the plaintext then the longer the round trip time process run.

5. Conclusions
This research shows the length of plaintext affect the round trip time. On the testing of 35 characters of plaintext, the author obtained 1,172 ms round trip time. Whereas on testing of 113 characters of plaintext, the author obtained 2,355 ms. In Figure 2 can be seen the round trip time graph increasing. The author concludes that the length of the plaintext affect the round trip time in the client server based AES algorithm. The longer the plaintext, the longer the round trip time process will run.
References

[1] Flevina Jonese D’souza, et al, Advanced Encryption Standard (AES) Security Enhancement Using Hybrid Approach, International Conference on Computing, Communication and Automation (ICCCA 2017).
[2] Kyungtae Kang, et al, Accommodating the Variable Timing of Software AES Decryption on Mobile Receives, IEEE.
[3] Erkay Savas, et al, A Generic Method for the Analysis of a Class of Cache Attacks: A Case Study for AES, The British Computer Society, 2015.
[4] Monodeep Kar, et al, Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator. IEEE, 2018.
[5] Sugiyanto, et al, Pengembangan Algoritma Advanced Encryption Standard Pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere. ULTIMATICS, 2016.
[6] Warkim, et al, Kriptografi Algoritma Advanced Encryption Standard Dan Pengecekan Error Detection Cyclic Redudancy Check, Jurnal FTI UNTAR.
[7] Soufiane Oukili, et al, High Speed Efficient Advanced Encryption Standard Implementation,IEEE, 2017.
[8] Christian C, et al, MarkToLock: An Image Masking Security Application via Insertion of Invisible Watermark Using Steganography and Advanced Encryption Standard (AES)Algorithm, IEEE, 2017.