MESSAGE SECURITY USING ONE TIME PAD AND AES HYBRID CRYPTOGRAPHY

Thin Thu Thu Tun[1], Ei Ei Myint[2], May Thida Aung[3]

[1,2] Information Technology, Technological University (Monywa), Monywa, Myanmar
[3]Information Technology, Technological University (Meiktila), Myanmar

Abstract

The art and science of concealing data to introduce secrecy in information security is recognized as cryptography. The data may contain confidential information that need to be secured form any third party access. Encryption techniques are required to secure these types of data. In order to obtain more security, hybrid encryption can be used. Hybrid encryption is a process by which combines two or more algorithms together and provides better security than a single encryption can do. The proposed system is designed by combination of two symmetric techniques; one time pad stream cipher and AES block cipher. In the system, the performance measurement of encryption algorithms is conducted in terms of processing time and memory usage. The avalanche effect of AES and proposed OTP-AES algorithms is calculated and analyzed. The OTP-AES algorithm will enhance the message security as compare to original AES algorithm.

Keyword: Hybrid Encryption, OTP-AES, Message Security

1. INTRODUCTION

The ability to protect data is essential to the growth of electronic commerce and data security. Cryptographic techniques are necessary for protecting data. There are three different types of cryptographic algorithms. These are symmetric and asymmetric and hashing. The symmetric algorithms use only one secret key for both encryption and decryption. The asymmetric algorithms have two keys where public key is used for encryption and the private key is used for decryption. The hashing algorithms convert a variable length message to a fixed-length message. Symmetric algorithms include two classes: stream ciphers and block ciphers. The major different between a block cipher and a stream cipher is that a stream cipher encrypts and decrypts one bit or byte of plaintext at a time. On the other hand, a block cipher encrypts and decrypts one block of plaintext at a time. Hybrid encryption is a method of combining one cryptographic approach with the other. It performs to improve the secureness of cryptography and provides more confidentiality of message.

Nishtha Mathura and Rajesh Bansode [1] proposed an extension of a public-key cryptosystem to support a private key cryptosystem which is a combination of AES and Elliptic Curve Encryption (ECC). In this work, an improved AES algorithm was used to encrypt plaintext and ECC algorithm was applied to encrypt the AES key. It is increasing overall security of the system by implementing software based counter measures to prevent possible vulnerabilities posed by the timing side channel attack. Chandra Prakash Dewangan and Shashikant Agrawal [2] proposed a novel approach to enhance AES algorithm. In their algorithm, input plaintext and encryption key had been mapped into various binary codes instead of giving plaintext and encryption key directly to the AES algorithm. The performance of their algorithm is evaluated using avalanche effect due to one bit variation in plaintext and avalanche effect due to one bit variation in encryption key. Experimental results showed that their proposed algorithm exhibit significant high avalanche effect which improves the level of the security.

EmanSalim Ibrahim Harba [3] proposed a method to protect data transferring and to produce a strong system protection by the use of three hybrid encryption techniques: AES, RSA and HMAC. The symmetric AES function was used to encrypt data, asymmetric RSA was used to encrypt AES password and HMAC was used to encrypt the authentication between server and client, or

client and client. As a result, the overall encryption is simple and fast with low computational requirements and provides high system security. Kassim Mohammed Awad, and et al. [4] suggested a model to hybrid cipher for secure multimedia by using AES and RC4 Chain. The system was tested on four selected images, four audio files and four text files with different sizes. The performance of the system was evaluated by histogram, correlation coefficient, Number of Pixel Changing Rate (NPCR) and Unified Averaged Changed Intensity (UACI), execution time and entropy of information.

2. BACKGROUND THEORY

This section describes the AES algorithm and illustrates the AES encryption process. And then, the about of one time pad cipher is presented.

2.1. AES algorithm

AES is a block cipher that operates based on a substitution-permutation network. AES uses data block size of 128-bit and one of the three various key sizes (128,192 or 256 bits). A 128 bit data block is divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a 4×4 matrix called the state. For both encryption decryption functions, AES takes 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys to generate ciphertext or to regain the original plaintext [6].
Each round of encryption process requires the four types of operations. These operations are as follows:

- Substitution Bytes: In this operation, a Substitution-Box is used to perform a byte-by-byte substitution of the block. To substitute a byte, the bytes are interpreted as two hexadecimal digits.
- Shift Rows: In this operation, there is no change in the bytes in the first row of the state. There is a cyclic shift of the second, third, and fourth rows to the left by one, two, and three bytes respectively.
- Mix Columns: In this operation, the bytes in each column are mixed by the multiplication of the state using a fixed matrix of polynomial and new value of the columns is placed.
- Add Round Key: In this operation, a round key is generated by performing various operations on the cipher key, and each byte of the state is combined with the round key using bitwise XOR [1].

Decryption is the reverse process of encryption and using inverse functions: Inverse Substitution Bytes, Inverse Shift Rows and Inverse Mix Columns. Firstly, Add Round Key stage is operated in both encryption and decryption process. Before reaching the finall round, the output of Add Round Key stage goes through Nr-1 rounds where Nr refers to number of rounds based on the key length. During each of those rounds, all of four stages are performed. In the final round, three stages are processed and there is no Mix Columns stage [7]. The encryption process of AES is shown in Figure 1.

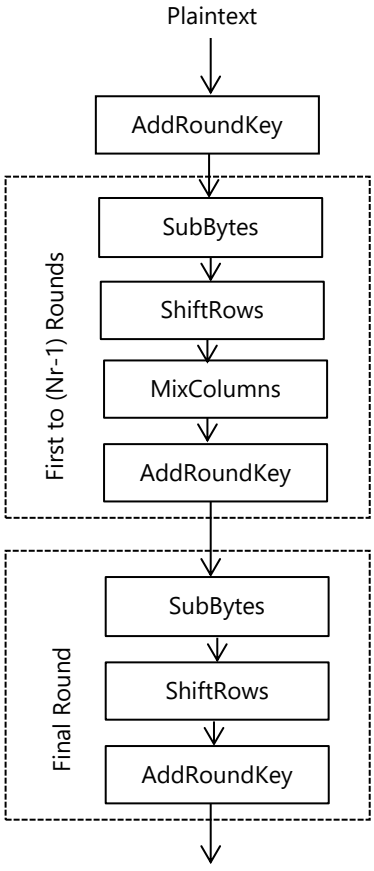

Figure *ss of AES*

2.2. One time pad cipher

In cryptography, one time pad is a technique in which a secret key generated randomly is used only once to encrypt a message that is then decrypted using a matching one time pad and key. It is a stream cipher and it extends the Vigenère cipher so that the key is as long as plaintext. The encryption process and decryption process incude a XOR operation between message and

one time pad key by the use of following equation (1) and (2).

$C = (P \oplus K)$ (1)

$P = (C \oplus K)$ (2)

Where P refers to plaintext characters, K refers to key characters and C refers to ciphertext characters.

Messages encrypted with key based on randomness have the advantage that there is theoretically no way to break the code by analyzing a succession of messages. The main benefit of one time pad cryptography is the generation of random key. If the message which is not a random sequence is combined with one time pad key which is a random sequence, then the result is chipertext which is completely a random sequence. The disadvantage of one time pad is that it can't process when the length of plaintext is larger than the length of key, because the key for this cryptography should be the same length as the plaintext [5].

3. ARCHITECTURE OF THE SYSTEM

In this session, the proposed OTP-AES algorithm, and implementation of the system are presented. And then, the results of performance comparison are also discussed.

3.1. The proposed OTP-AES algorithm

At present, various types of cryptographic algorithms provide high security to message on networks, but these algorithms also have some drawbacks. The concept of the dual encryption can be used to enhance security of message. The proposed OTP-AES algorithm is developed to attain better security by combination of one time pad and AES. Firstly, the plaintext message is encrypted with one time pad technique to produce one time pad ciphertext. After that, this produced ciphertext is encrypted again by the use of AES algorithm, and then the OTP-AES ciphertext is received. In order to get back original message, dual decryption process must be used in the sequence order of AES and one time pad. The block diagram of hybrid encryption using one time pad and AES algorithms can be seen as shown in Figure 2.

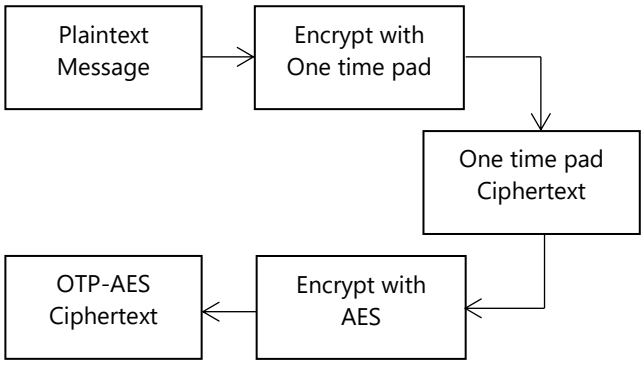

Figure 2.Hybrid Encryption using One time pad and AES

3.2. Implementation of the system

The one time pad and AES hybrid system is implemented using Java programming language. To encrypt the message, the user must type the inputs (message and key) in the respective text boxes with the use of corresponding buttons.

Under OTP-AES encryption process, the message is encrypted with one time pad and the onetime pad ciphertext is obtained. And then, this ciphertext is encrypted again by AES with the use of 128 bit key length. The desired OTP-AES cipxertext is gained as shown in Figure 3.

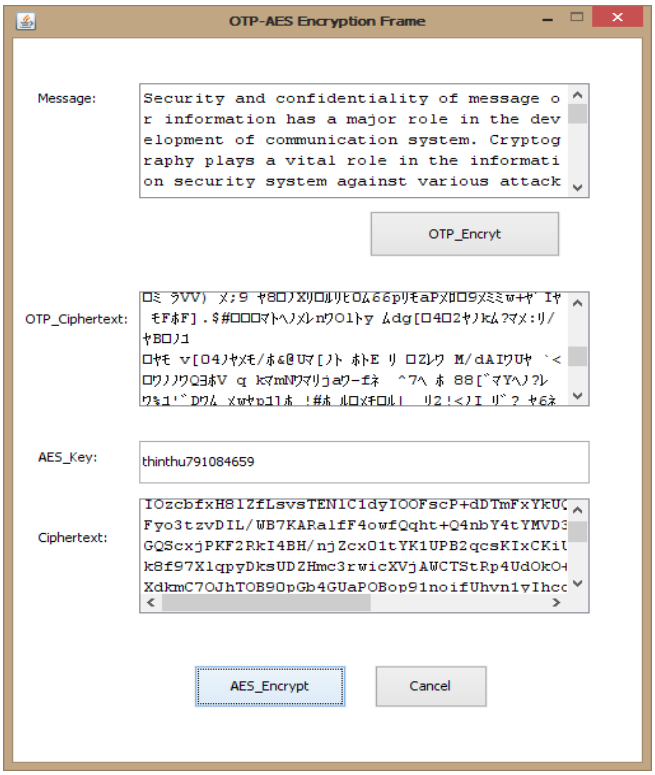

Figure 3. OTP-AES Encryption Process

In OTP-AES decryption process, the ciphertext is decrypted with first by AES using predefined key, and second by one time pad to regain the original message without any changes. This decryption process and the recovered original message can be seen in Figure 4.

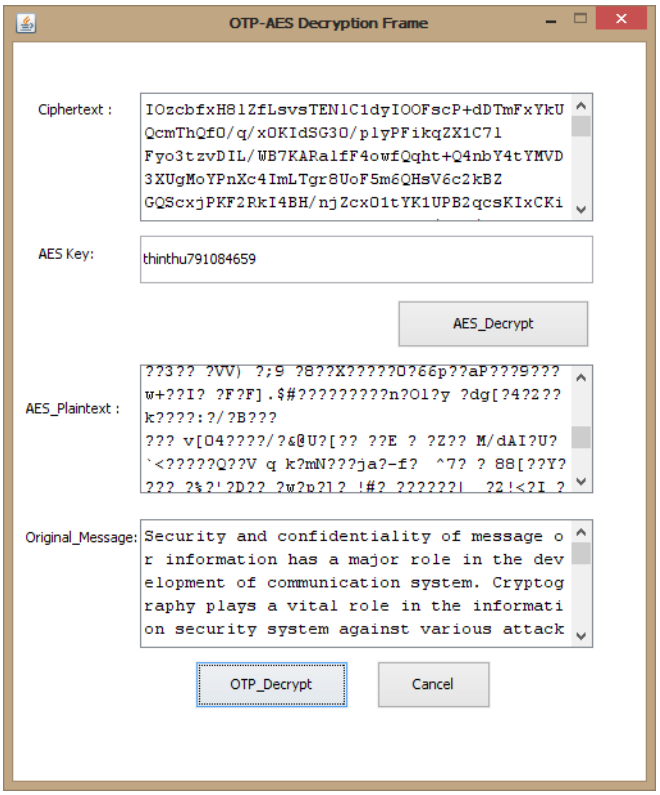

Figure 4. OTP-AES Decryption Process

3.3 Comparison results

In this session, comparison results of one time pad, AES and OTP-AES algorithms are analyzed. The system measures the running time in milliseconds and memory usage in kilobytes.The performance measurement of each algorithm can be seen as shown in Figure 5. From this Figure, comparison results can be viewed by the use of corresponding buttons (Time Graph, Memory Graph). The comparison of running time is illustrated as shown in Figure 6. According to the results, the OTP-AES encryption takes the longest time among these three algorithms because it performs dual encryption process over plaintext. But OTP-AES encryption is faster than the sum of the time of one time pad encryption and AES encryption. Based on the results of research, OTP-AES encryption reduces 10% time consumption over the sum of one time pad and AES.

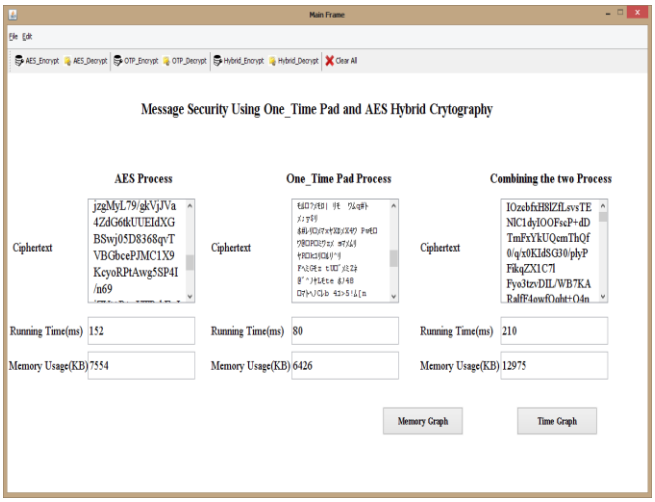

Figure 5. Performance Measurement of Each Algorithm

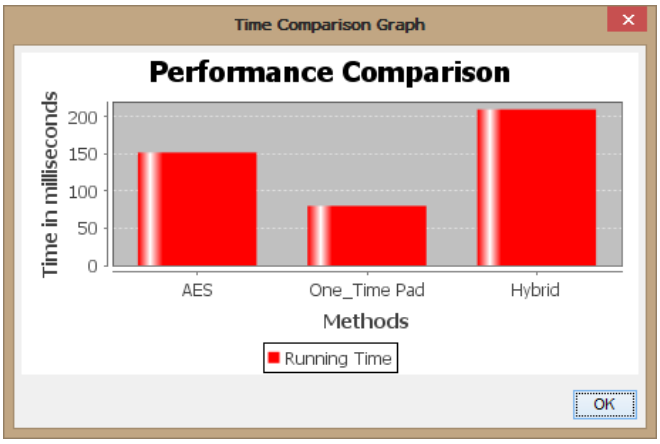

Figure 6. Comparison of Running Time

The comparison of memory usage is represented as shown in Figure 7.

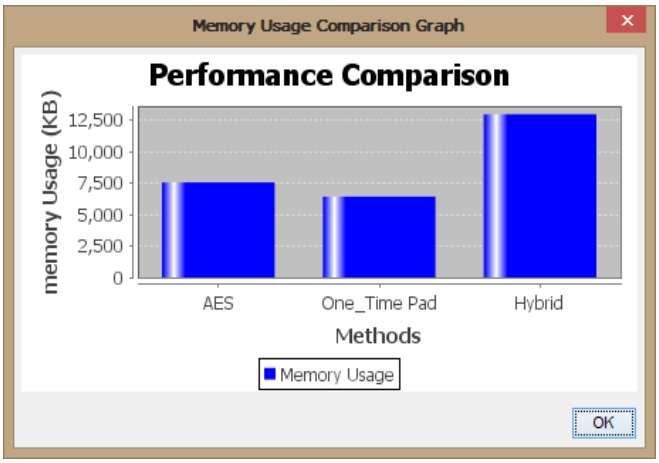

Figure 7. Comparison of Memory Usage

Based on the results from the above Figure, the OTP-AES encryption consumes the highest memory among

these three algorithms. But OTP-AES encryption consumes lower memory than the sum of the usage of one time pad encryption and AES encryption. According to the results of research, OTP-AES encryption reduces 7% memory usage over the sum of other two algorithms.

An enviable property of any encryption algorithm is that a small change in either the plaintext or the key must produce a significant change in the ciphertext. The changing of the plaintext or the key in one bit should produce a change in many bits of the ciphertext. This property is known as the avalanche effect. It is calculated by the following equation 3;

$$\text{Avalanche Effect} = \frac{\text{Number of change bits in ciphertext}}{\text{Number of bits in ciphertext}} \quad (3)$$

For example, the plaintext "Cryptography and Hybrid Encryption" and the key "2597421350987654" are used to calculate the avalanche effect of AES and OTP-AES algorithms. In the result of changing one bit in plaintext and keeping the key constant, AES supports 34% avalanche effect whereas OTP-AES supports 98%. In changing one bit in the key and keeping the plaintext constant, AES has 96% whereas OTP-AES has 98%. In both cases, OTP-AES algorithm provides the higher percentage of avalanche effect than original AES algorithm as shown in Figure 8.

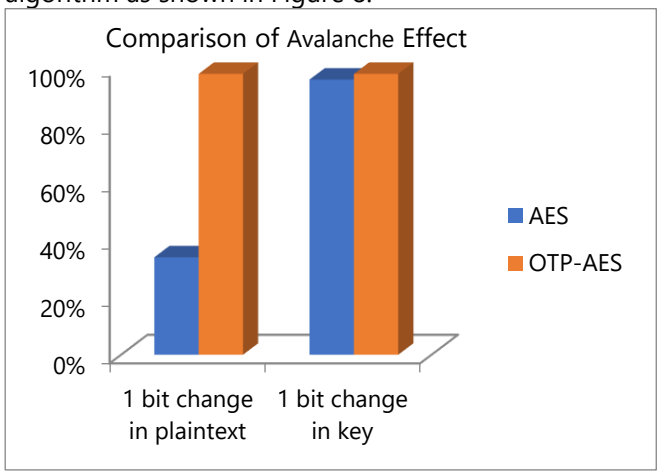

Figure 8. Comparison of Avalanche Effect of AES and OTP-AES

4. CONCLUSION

In this paper, the hybrid cryptography with the combination of one time pad and AES is presented. The system evaluates the performance measurement of one time pad, AES and OTP-AES encryption based on running time and memory usage. And, the avalanche effect of AES and OTP-AES algorithms is also calculated. According to the results, OTP-AES encryption process reduces a slight percentage of both time and memory consumption as compare to the sum of one time pad and AES encryption processes. And also, OTP-AES algorithm leads significant increment in avalanche effect of AES Algorithm. Therefore, the OTP-AES algorithm provides better security of message as compare to original AES algorithm because it has a better avalanche effect and includes one time pad's XOR concept.

5. ACKNOWLEDGEMENT

The author wants to express her thanks to the experts who have contributed towards development of the paper.

REFERENCES

[1] Nishtha Mathura and Rajesh Bansode, "AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection", Seventh International Conference on Communication, Computing and Virtualization, 2016.

[2] Chandra Prakash Dewangan and Shashikant Agrawal, "A Novel Approach to Improve Avalanche Effect of AES Algorithm", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1 (8), 2012.

[3] Eman Salim Ibrahim Harba, "Secure Data Encryption through a Combination of AES, RSA and HMAC", Engineering, Technology & Applied Science Research, Vol. 7 (4), 2017.

[4] Kassim Mohammed Awad, Ali Makki Sagheer, and Ayoob Abdulmunem Abdulhameed, "Hybrid Cipher for Secure Multimedia by using AES and RC4 Chain", Iraqi Journal for Computers and Informatics (IJCI), Vol. 43 (1), 2017.

[5] M G Ristiana, R Marwati and S M Gozali, "Hybrid algorithm of RSA and One Time Pad Cryptography", 2018.

[6] Chaitali Haldankar and Sonia Kuwelkar, "Implementation of AES and Blowfish Algorithm", International Journal of Research in Engineering and Technology (IJRET), Vol. 3 (3), 2014.

[7] Jayeeta Majumder, Sagarjit Das, and Sayak Maity, "SMS Encryption in Android Platform", International Journal of Computer Engineering and Applications (IJCEA), Vol. 9 (5), 2015.