JURNAL EMACS
[Engineering, MAthematics and Computer Science] Vol.4 No.2 May 2022: 73-77
e-ISSN: 2686-2573
DOI: 10.21512/emacsjournal.v4i2.8273

Encrypted Short Message Service Design Using Combination of Modified Advanced Encryption Standard (AES) and Vigenere Cipher Algorithm

Christopher[1*], Abel Gunawan[2], Sheila Prima[3]

[1,2,3] Computer Science Department, School of Computer Science,

Bina Nusantara University,
Jakarta, Indonesia 11530
christopher013@binus.ac.id; abel.gunawan@binus.ac.id;
sheila.octarini@binus.ac.id

*Correspondence: christopher013@binus.ac.id

Abstract *– Despite the popularity of social media and Internet-based messaging services, Short Message Service (SMS) is still widely used by a lot of people worldwide. However, in this modern era, Short Message Service (SMS) is not a secure way of sending and receive text messages. Anyone with the right privilleges can easily read all the messages sent using SMS service. Therefore, appropriate cryptographic algorithms should be applied to ensure confidentiality of the message content. In this paper, a modified AES with Vigenere Cipher Algorithm will be used to encrypt the text message, hence greatly increasing the security of the sent messages. Avalanche Effect is chosen as a metric for measuring performance of the proposed algorithm and its implementation. The proposed algorithm shows high Avalanche Effect compared to standard AES algorithm.*

Keywords: *Secure Messaging; Advanced Encryption Standard; Vigenere*

I. INTRODUCTION

Thanks to the development of internet technology, it is now possible for people to establish a communication with practically anyone around the globe in just a fraction of a second using their smartphone. The most recent research conducted by Ericsson & the Radicati Group shows that in 2021, more than 80 percent of the world populations have at least one smartphone on their possesion [4].

However, in this era of smartphone, many people still use *Short Message Service* (SMS) to send and receive text messages. Dating back to 1984, SMS was invented by a German engineer by the name of Friedhelm Hillebrand along with a colleague named Bernard Ghillebaert [9]. SMS made it possible to send and receive text messages using the existing GSM network.

According to a study from the Pew Research Center, those in the United States who communicate using *Short Message Service* (SMS) send and receive on average more than 40 messages every day [9]. That means millions of text messages are sent through Short Message Service (SMS) every single day despite the rise of social media and Internet-based messaging services.

While the numbers seem facinating to some extent, this may raise some security concerns. One of the biggest concerns is that, by design, SMS has no encrpytion at all, meaning that someone with enough privilleges can easily read all the text messages sent over the network.

This research attempts to solve the problem by proposing an encryption method that will encrypt the text messages before it is sent over the network. The method is designed to be fully compatible with existing SMS service with minimal configuration required on both the sender and recipient side.

1.1 Related Works

There has already been some approaches on designing an encrpytion method for Short Message Service (SMS). M. Agoyi and D. Seral [5] had already completed a similiar study using RSA ELGamal and the Elliptic curve encryption algorithm. However, it is later proven that it is very time consuming to use an asymmetric method for the encryption process. On the other hand, based on a study conducted by Rayarikar, R., & Upadhyay [7] AES encryption alone is not considered secure enough for this purpose. Later, Neetesh Saxena and Narendra S. Chaudhari [6] explored the possibility of using digital signature algorithms such as DSA, RSA, and ECDSA. By using the ECDSA algorithm, the results turned out to be satisfactory. However, it was mentioned that the algorithm was merely

simulated and implemented using a Java Virtual Machine as implementations of ECDSA is not always feasible on low powered devices such as a smartphone.

In the end, a combination of modified AES and Vigenere Cipher algorithm was chosen. As shown in this study [3], a modified Vigenere Cipher alone is strong enough against common attacks, such as pattern prediction and brute force attack. Hence a combination with AES will result in much better security while still not being too resource heavy and maintaining a reasonable process time.

1.2 SMS Architecture

Figure 1 below describes the Short Message Service (SMS) architecture commonly used today.

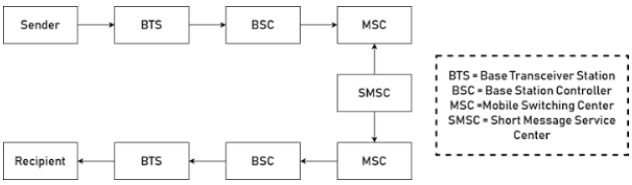

Figure 1. Short Message Service (SMS) architecture

It can be seen from Figure 1 that a text message must go through various destinations before it reaches its target recipient. First, a cellular tower called BTS will receive the message and forward it to Base Station Controller (BSC). In turn, BSC will forward the messages through Mobile Switching Center (MSC) where it is passed to Short Message Service Center (SMSC). SMSC has the responsibility of checking whether the recipeint has cellular signal or not. This can be done by using Home Location Register (HLR) protocol. In the case the recipient mobile phone is out of reach, SMSC will keep the message indefinitely until the network has been restored. Finally, SMSC will forward the messages to the Mobile Switching Center (MSC) of the designated recipient, and the above process is repeated in reverse order before the text message reaches the recipient.

1.3 AES Algorithm

Founded in 2001, the Advanced Encryption Standard (AES) algorithm is the successor of the now outdated DES algorithm. AES is an iterated cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen [1]. The algorithm is commonly referred to as AES-128, AES-192, or AES-256, with the number after the hyphen represents its key length. Unlike its predecessor, AES supports many combinations of data and key length, namely 128, 192, and 256 bits.

During the encryption-decryption process, the AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver the final ciphertext or to retrieve the original plaintext [3]. AES does not have a Feistel structure in which half of the data block is used to modify the other half of the data block and then the halves are swapped [8].

AES has four different stages which consist of one permutation stage and three substitution stages, namely: Substitute bytes, which uses S-box to perform byte-by-byte substitution; Shift rows, which is a simple permutation; Mix columns, which is done over an arithmetic Galois Field; Add round key, a simple bitwise XOR of the current block with a portion of the expanded key [8].

1.4 Modified Vigenere Algorithm

Vigenere encryption algorithm was developed by Blaise De Vigenere in 1583 [2]. It uses the defined square matrix, termed as a tabula recta, a Vigenère square, or a Vigenère table, along with a custom key to encrypt the plaintext message. It is a poly-alphabetic cipher in which a given letter or symbol in a plaintext will not always be enciphered by the same ciphertext letter or symbol. By far, the Vigenere cipher is the best-known poly-alphabetic substitution cipher [2].

The normal Vigenere square matrix is based on twenty-six capital letters, followed by cycles changing the order, composed of a 26 × 26 square matrix. In this system, Ci (Cipher text) is obtained as the sum of Pi (Plain text) and Ki (Key) modulo 26.

However, by following the ASCII 7-bit standard that is currently used in SMS, the proposed Vigenere formula is then altered by using modulo 128 instead of 26. Hence the formula becomes as follows:

- For Encryption:

$$Ci = (Pi + Ki) \bmod 128$$

- For Decryption:

$$Pi = (Ci + Ki) \bmod 128$$

II. METHOD

The proposed message encryption and decryption process can be seen on Figure 2 below.

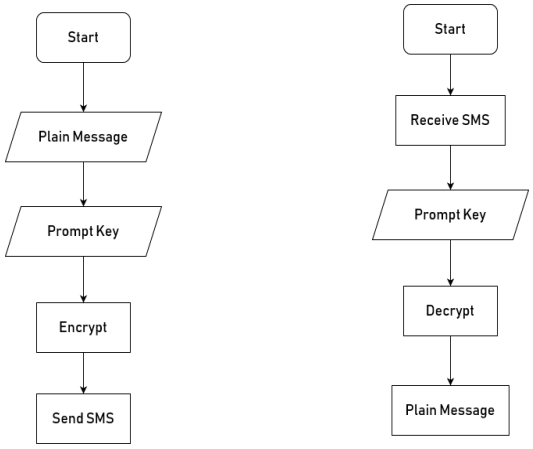

Figure 2. SMS encryption and decryption process

It can be seen from Figure 2 that the messages will be encrypted before being sent over to the SMS service. Similarly, the received messages will be decrypted locally on the client side first before being passed to the recipient. This implies that there are no plain text messages sent over the SMS network. Furthermore, a key is always required to encrypt and decrypt the messsage, adding an additional layer of security to both client sides.

Figure 3 and Figure 4 below further illustrate the proposed encryption and decryption algorithm (i.e. combination of modified RSA and Vigenere algorithm).

Figure 3. Proposed Encryption process using combination of AES and Vigenere Algorithm

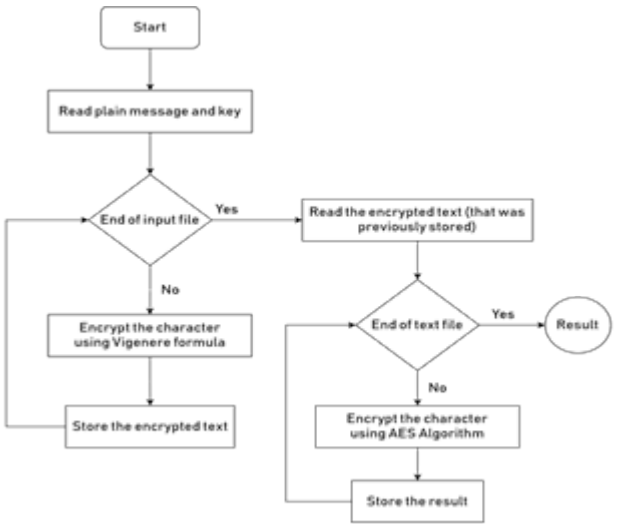

Figure 4. Proposed Decryption process using combination of AES and Vigenere Algorithm

As described from the above figure, the encryption process steps are as follow:

- Input original message
- Prompt for encryption key
- Encrypt the message using Vigenere cipher
- Encrypt the results generated on step (3) using AES algorithm
- Send the message using SMS service

Whereas the decryption process steps can be listed as below:

- Receive encrypted message
- Prompt for encryption key
- Decrypt the message using AES algorithm
- Decrypt the results generated on step (3) using Vigenere cipher
- Display the received message to the recipient

III. RESULTS AND DISCUSSION

Presented below are test results of the proposed algorithm. The tests were performed using "NUSANTARA" as the input message and "binusian20212022" as the key. The tests were mainly focused on calculating their Avalanche Effects by using two different approaches as the changes will be made at the beginning and the end of the text.

Avalanche Effects can be calculated by using the following formula.

$$\frac{\sum bits\ changed}{\sum number\ of\ bits\ on\ ciphertext} \times 100\% \quad (1)$$

Case 1: Changes made at the end of the text

Using the regular AES-128 algorithm, the text "NUSANTARA" can be encrypted into "6cf9fd8546e8a9fdc402bffa28127b10". Altering the last character of the text from an "A" to a "B" changes the encryption result to "4e281e54f8359588464dee3f420ea6fd". Converting both results to binary causes 92 bits to be flipped from the original results. Therefore, the calculated Avalanche Effect based on equation 1 is 71.87%. The results are summarized on the Table 1 below for convenience.

Table 1. Regular AES-128 Algorithm with changes made at the end of the text

	Regular AES Algorithm
Text	NUSANTARA
Key	binusian20212022
Encrypted Text	6cf9fd8546e8a9fdc402bffa28127b10
Modified Text	NUSANTARB
Modified Encrypted Text	4e281e54f8359588464dee3f420ea6fd
Number of bits flipped	92
Avalanche Effect	71.87%

Using the combination of AES-128 and Vigenere algorithm, the text "NUSANTARA" can be encrypted into "9dy5q2dizgpw8ykw86f2ekyj74yj xqf5". Altering the last character of the text from an "A" to a "B" changes the encryption result to "u9w2633rkrqn7fkyivin9qfpxrgdqvbn". Converting both results to binary yields 102 bit flips between the results. Therefore, the calculated Avalanche Effect is 79.68% as shown in Table 2 below.

Table 2. Proposed algorithm with changes made at the end of the text

	Regular AES Algorithm
Text	NUSANTARA
Key	binusian20212022
Encrypted Text	9dy5q2dizgpw8ykw86f2ekyj74yjxqf5
Modified Text	NUSANTARB
Modified Encrypted Text	u9w2633rkrqn7fkyivin9qfpxrgdqvbn
Number of bits flipped	102
Avalanche Effect	79.68%

Case 2: Changes made at the beginning of the text

Using regular AES-128 algorithm, the text "NUSANTARA" is encrypted into 6cf9fd8546e8a9fdc402bffa28127b10 from the previous case. Altering the first character of the text from an "N" to an "H" changes the encryption result to "422bbf631298a13a41 3c8ee0c279f727". Converting both results to binary yields 78 bit flips between the results. Therefore, the calculated Avalanche Effect is 60.93%. The results are summarized on the Table 3 below.

Table 3. Regular AES-128 Algorithm with changes made at the beginning of the text

	Regular AES Algorithm
Text	NUSANTARA
Key	binusian20212022
Encrypted Text	6cf9fd8546e8a9fdc402bffa28127b10
Modified Text	HUSANTARA
Modified Encrypted Text	422bbf631298a13a413c8ee0c279f727
Number of bits flipped	78
Avalanche Effect	60.93%

Using the combination of AES-128 and Vigenere algorithm, text "NUSANTARA" is encrypted into "9dy5q2dizgpw8ykw86f2ekyj74yjxqf5" like before. Altering the last character of the text from an "N" to an "H" changes the encryption result to "2e4q7z4b8ar7u6kffq4wz5wuxpb6jhzk". Converting both results to binary yields 98 bit flips between the results. Therefore, the calculated Avalanche Effect is 76.56% as shown in Table 4 below.

Table 4. Proposed algorithm with changes made at the beginning of the text

	Regular AES Algorithm
Text	NUSANTARA
Key	binusian20212022
Encrypted Text	9dy5q2dizgpw8ykw86f2ekyj74yjxqf5
Modified Text	HUSANTARA
Modified Encrypted Text	2e4q7z4b8ar7u6kffq4wz5wuxpb6jhzk
Number of bits flipped	98
Avalanche Effect	76.56%

Comparing the two cases, it can easily be seen that the proposed algorithm has a higher Avalanche Effect than the regular AES algorithm. This difference is illustrated in Figure 5 below.

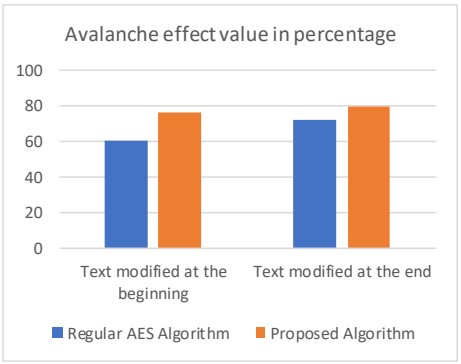

Figure 5. Avalanche Effect differences between two algorithms on both cases

Figure 5 above also further implies that the proposed algorithm has a lower difference in Avalanche Effect values between cases compared to the standard AES algorithm. A higher Avalanche Effect means the proposed algorithm provides a somewhat higher level of security compared to the regular AES algorithm. Hence a text message encrypted using the proposed algorithm is less likely to be cracked compared only being encrypted using a standard AES algorithm or, even worse, not encrypted at all.

IV. CONCLUSION

The use of AES and Vigenare encryption provide great security improvement on sending and receiving text messages compared to without any encryption. These two algorithms combined have managed to provide a greater security, evident in the increase of the Avalanche Effect compared to using only a regular AES algorithm, while still maintaining a low complexity. However, there are still a number of possible future studies that can be done. For instance, it may be possible for this algorithm to be implemented on another type of insecure messaging service such as Multimedia Messaging Service (MMS). Additionally, there may be a way to further increase the Avalanche Effect without much negative side effects.

REFERENCES

[1] Advanced Eneryption Standard (AES), Federal Information Processing Standards Publication 197, November 2001.

[2] Brian Carter and Tanja Magoc, "Introduction to Classical Ciphers and Cryptanalysis", 2007

[3] Gurjeevan Singh, Ashwani Singla and K S Sandha, "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System", International Journal of Multidisciplinary Research, Vol.1 Issue 4, pp. 143-151, August 2011.

[4] How Many Smartphones Are In The World? (2022). Bankmycell. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[5] M. Agoyi and D. Seral, "SMS Security: An Asymmetric Encryption Approach," 2010 6th International Conference on Wireless and Mobile Communications, 2010, pp. 448-452, doi: 10.1109/ICWMC.2010.87.

[6] N. Saxena and N. S. Chaudhari, "Secure encryption with digital signature approach for Short Message Service," 2012 World Congress on Information and Communication Technologies, 2012, pp. 803-806, doi: 10.1109/WICT.2012.6409184.

[7] Rayarikar, R., & Upadhyay, S. (2012). SMS Encryption using AES Algorithm on Android. International Journal of Computer Applications, 50(19).

[8] William Stallings. (2010). NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication. *Cryptologia* 34:3, pages 225-235.

[9] What is SMS and How is it Different from Text Messages? (2020). TextMagic. https://www.textmagic.com/blog/what-is-sms-and-how-is-it-different-from-text-messages/