A Modified RAES Technique for a Secured Information Security

[1]Hussain, H.S, [2]Eden Barua, [3]Nik Zulkarnaen Khidzir, [4]Cheang Kah Wai, [5]Ghazali M. F.

[1]Faculty of Computing and Engineering, Quest International University, Perak, Malaysia
[2]Faculty of Computing and Engineering, Quest International University, Perak, Malaysia
[3] Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, Kelantan, Malaysia
[4]Faculty of Computing and Engineering, Quest International University, Perak, Malaysia
[5]Kulliyyah Muamalat dan Sains Pengurusan, UniSHAMS

Keywords: cipher; encryption; plaintext; RFC; AES; RAES.

Introduction

The word 'Cryptography' according to Stallings (2017), is derived from a Greek word meaning secret writing. In cryptography plain text is transferred to cipher text using encryption techniques, this process is called encryption. And converting cipher text to plain text using decryption techniques, this process is called decryption. There are several conventional cryptographic methods, and because it is possible to crack cipher text. Many cipher techniques have developed but the Rail Fence Cipher (RFC) is the simplest and amusing cryptographic algorithm until now (Nahar & Chakraborty, 2020). RFC is a type of transposition techniques. Meanwhile, there is another technique called Advanced Encryption Standard (AES). The AES algorithm is one of the symmetric key block digits with block sizes varying from 64 to 256 bits (Burr, 2003). Some AES applications continue to struggle for low performance areas such as smart cards and cellular phone-related hardware. Therefore, encryption speed and execution times are two important factors for the real-time use of AES algorithms. The problem with the use of AES is the compromise between the speed of encryption and decryption and execution time where there is more confusion and diffusion. Furthermore, AES is said to use an algebraic structure which is too simple and each block is always encrypted in the same way that making it easy to break (Tillich et al., 2008; Stalling, 2017). Therefore, this paper proposes a new approach called the RAES technique, which results from redesigning the current RFC using two basic phases, first using the AES technique and then using the potential of the RFC technique to protect confidential messages for more secure information security.

Materials and Methods

There are several conventional cryptographic methods, and because it is possible to crack cipher text, that is why it tries to propose RAES techniques written in C++ programming to be more secure to protect information from cipher breaking. Mixing RCF ciphers with AES, it appears that the encryption and decryption of the modified RAES requires the generation of the plaintext elements which are usually single letters are written in a predetermined

sequence into a matrix format which is basically a rectangle that has been decided by the transmitter and receiver in advance, and then it is read off according to another predetermined sequence across the matrix to get the cipher text. Through this RAES technique, not only the strength of the AES technique can be applied but also the RFC technique that uses keywords and salt can also be used making this mixed system perform ciphers that are difficult to break by attackers. Moreover, the strength of the RAES algorithm is in terms of faster execution times and more secure than existing substitution and transposition algorithms. First of all, for RAES encryption, the plain text and initial key is added to the block using an XOR ("exclusive or") cipher, which is a built-in operation of the processor hardware. The plain text used is in the form of a text file where the characters used are between 10 to 50 characters as in (Aaref & Ablhd, 2017; Nahar & Chakraborty, 2020). Then each byte of data is replaced with another, according to a predefined schedule. Next, the 4 × 4 array rows are moved: the bytes in the second row are moved one space to the left, the bytes in the third row are moved two spaces, and the bytes in the fourth row are moved three. The columns are then mixed by using the mathematical operation combines four bytes in each column. Finally, the RFC algorithm is applied from the resulting blocks, and the process is repeated for each round. This results in a cipher text that is radically different from the regular text. For RAES decryption, the same process is performed in reverse (See Figure 1).

Results and Discussion

To get started to run AES at first it should have a plain text. For example, the plain text that used as input to AES is **"MEET ME AT QUEST INTERNATIONAL UNIVERSITY"** to be cipher with the proposed system as output cipher text **"U2FsdGVkX19eUOzxd4RrAxqv2moIDvCDgUSxTtjuVVtOx7sUW6H3JBXlHqMktyJYuwGeX5FaHJI3HkMMxuV8g"**. The result is strong and difficult to break. And same character ciphered to different characters and all the plain text characters quite different from the original text.

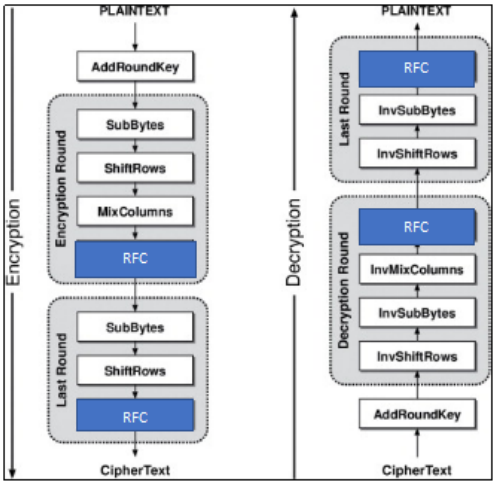

Figure 1 The implementation of RAES technique

The steps of AES that lead to the above results are as following:

At first the plain text "MEET ME AT QUEST INTERNATIONAL UNIVERSITY" pass to AES algorithm where used as follow:

Keyword = **INTRODUCING YOU A NEW TECHNIQUE!**

Salt = **NEW CIPHER RAES TECHNIQUE**

The output of this is: Cipher text =

"U2FsdGVkX19eUOzxd4RrAxqv2moIDvCDgUSxTtjuVVtOx7sUW6H3JBXlHqMktyJYuwGeX5FaHJI3HkMMxuV8g".

Now this cipher text is considered as plain text to RFC algorithm by use the encryption key as follow:

- In RFC algorithm, the order of the alphabets is re-arranged to obtain the cipher text.
- Where the plain text is written downwards and diagonally on successive rails of an imaginary fence.
- When the pointer reaches the bottom rail, it will traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus, the alphabets of the message are written in a zig-zag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

For example, if the message is "U2FsdGVkX19eUOzxd4RrAxqv2moIDvCDgUSxTtjuVVtOx7sUW6H3JBXlHqMktyJYuwGeX5FaHJI3HkMMxuV8g" and key (number of rails) = 3 then cipher is prepared as:

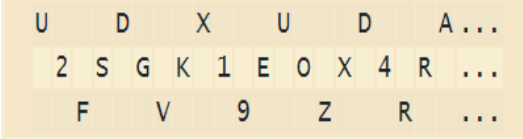

Figure 2. Cipher text in RFC

With the same way it gets the cipher text:

"UDXUDA2DGTVXWJHTUXHHXG2SGK1EOX4RXVMIVDUXTUVO7U63BLQKYYWE5AJ3KMU8FV9ZRQOCSJTSHXMJGFIMV"

From the algorithm implemented above, can be summarized as follows:

Plaintext: MEET ME AT QUEST INTERNATIONAL UNIVERSITY

Ciphertext: UDXUDA2DGTVXWJHTUXHHXG2SGK1EOX

4RXVMIVDUXTUVO7U63BLQKYYWE5AJ3KMU8FV9ZRQOCSJTSHXMJGFIMV

Figure 3 shows the output from the implementation of the RAES Technique.

Figure 3. Output from the program using RAES technique

Meanwhile, the decryption function requires the use of the inverse of the whole process from beginning to end due to the symmetric technique.

Table 1 shows the time taken with the use of the RAES Technique based on key types.

Table 1 Show time taken based on key types.

Keys	Time Taken
RAES 128	0.18
RAES 192	0.38
RAES 256	0.40

When using the RAES Technique to encrypt plain text similar to that used above, for key 128 (RAES 128) the time taken is 0.18 seconds. While for RAES 192 (key is equivalent to 192) recorded a time of 0.38 seconds and 0.40 seconds recorded for RAES 256. It shows a longer time taken if encrypting the same plain text for RAES 256 compared to RAES 192 and RAES 128.

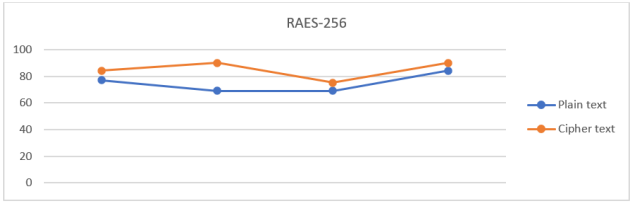

Figure 4. Diffusion and confusion level from RAES-256 technique

Meanwhile, Figure 4 shows the observation for two values, namely plain text and cipher text after being converted to an ASCII numeric values. Thus, the results of RAES-256 (for key 256) levels of diffusion and confusion proved to be higher when the graph above shows a significant difference between the lines representing plain text and cipher text.

Conclusion

In conclusion, it was found that originally, the cipher text generated by the RFC algorithm was prone to be easily decomposed using force, thorough search, search by frequency and many other methods as it had no diffusion and confusion in the generating algorithm. Similarly, to AES itself, it still has its shortcomings such as speed is still slow especially AES256 but with a combination of RFC and modified AES known as RAES technique, adds a high percentage of confusion and diffusion in algorithms that generate a strong and difficult to crack ciphers.

References

Aaref, A. M. & Ablhd, A. Z. (2017). A New Cryptography Method Based on Hill and Rail Fence Algorithms. Diyala Journal of Engineering Sciences, 10(1), 39-47.

Burr, W.E. (2003). Selecting the advanced encryption standard. IEEE Security and Privacy 1(2), 43–52.

Nahar, K., & Chakraborty, P. (2020). Improved Approach of Rail Fence for Enhancing Security.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice, Global Edition. Pearson. p. 177. ISBN 978-1292158587. ACM Woodstock conference

Tillich, S., Feldhofer, M., Popp, T. & Großsch¨adl, J. (2008). Area, delay, and power characteristics of standard-cell implementations of the AES S-Box. Journal of Signal Processing Systems 50(2), 251–261.