An Implementation of RC4+ Algorithm and Zig-zag Algorithm in a Super Encryption Scheme for Text Security

M A Budiman, Amalia and N I Chayanie
Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia

Email: mandrib@usu.ac.id, amalia@usu.ac.id, noerindachayanie@student.usu.ac.id

Abstract. Cryptography is the art and science of using mathematical methods to preserve message security. There are two types of cryptography, namely classical and modern cryptography. Nowadays, most people would rather use modern cryptography than classical cryptography because it is harder to break than the classical one. One of classical algorithm is the Zig-zag algorithm that uses the transposition technique: the original message is unreadable unless the person has the key to decrypt the message. To improve the security, the Zig-zag Cipher is combined with RC4+ Cipher which is one of the symmetric key algorithms in the form of stream cipher. The two algorithms are combined to make a super-encryption. By combining these two algorithms, the message will be harder to break by a cryptanalyst. The result showed that complexity of the combined algorithm is $\theta(n^2)$, while the complexity of Zig-zag Cipher and RC4+ Cipher are $\theta(n^2)$ and $\theta(n)$, respectively.

1. Introduction
Communication is the process of transferring information from one party to another. One example of communication is sending letters. With more advanced developments, the letter is no longer done by handwriting but by means of electronic messaging. Sending massages electronically via insecure channels may allow unauthorized parties to read the messages. To maintain the messages confidentiality, one solution is to encrypt the messages using cryptographic algorithms. Cryptography is the science and art to preserve messages confidentiality. According to Request for Comments (RFC), cryptography is a mathematical science that deals with transforming data to make the meaning unintelligible (to hide the meaning of the data), to prevent it from unauthorized changes, or to prevent it from unauthorized use. A cryptographic system is a system that can be used to change a message in order to make the message not understood by anyone other than the recipient. This process is called encryption [1]. Two types of cryptography are classical cryptography and modern cryptography. To further improve security, a combination of classical and modern algorithms is performed. Classical cryptographic algorithm to be used for this data encoding process is Zig-zag Cipher and modern algorithm that will be used is RC4+ Cipher.

Zig-zag Cipher is one of the classical cryptography that use transposition techniques that use character permutations, in which the original message unreadable unless the person has the key to decrypt the message [2]. The Zig-zag Cipher algorithm includes an unsafe classical cryptography algorithm. This is evidenced by research that proves that the more difficult algorithm of the Zig-zag...
Cipher algorithm, that is Affine Cipher can already be solved by cryptanalysis [3]. RC4+ Cipher is one type of RC4 algorithm, which uses a variable whose key length is from 1 to 256 bits used to initialize a 256 bit long table. The two algorithms combined are called Super Encryption. By combining these two algorithms, we can get a stronger cipher so it is not easy to break, and also to prevent of using a single cipher only which is comparatively weak [4].

2. Method

One of the key symmetric algorithms in the form of stream cipher is RC4+ cipher algorithm. Undoubtedly, the importance of stream ciphers in computer applications cannot be ignored. Therefore, a standardized model for the stream cipher design is certainly today’s requisite [5]. RC4+ uses a structure like RC4 and adds some operations to amplify the cipher. This structure tries to exploit good points on RC4 then provides some additional features for better security limits [6]. The RC4+ cipher algorithm has two main parts: Key Scheduling Algorithm (KSA) in Table 1 and Pseudo Random Generation Algorithm (PRGA) in Table 2.

Table 1. KSA of RC4+ Cipher [6]

| for i from 0 to 255 |
|---------------------|
| S[i] := i           |
| endfor              |
| j := 0              |
| for i from 0 to 255 |
| j := (j + S[i] + key[i mod keylength]) mod 256 |
| swap values of S[i] and S[j] |
| endfor              |

Table 2. PRGA of RC4+ Cipher [6]

| while |cipherkey| < |plaintext|: |
|-------|---------|-----------------|
| i := i + 1 |
| a := S[i] |
| j := j + a |
| Swap S[i] and S[j] |
| (b := S[j]; S[i] := b; S[j] := a) |
| c := S[i<<5 ⊕ j>>3] + S[j<<5 ⊕ i>>3] |
| output (S[a+b] + S[c⊕0xAA]) ⊕ S[j+b] |
| endwhile |

Where i and j are 8-bit array indexes, S is all possible 256 permutations, << and >> are left and right shift, ⊕ is exclusive OR.

The technique applied to the Zig-zag Cipher algorithm is the technique of transposing the encryption cipher and decrypting the message by altering the order of the letters in the plaintext to the ciphertext in such a way that the contents of the message are not understood except by certain people. How to make Zig-zag Cipher algorithm as powerful as modern algorithm that is by using ASCII characters and then convert it to binary by playing in its bit. Each symbol that appears on the computer screen has a different ASCII code, the length of each ASCII code in binary is 8 bits and there are 28 unique symbols contained in the ASCII table [7].
Zig-zag transpositions can be performed in succession by forming rows or columns arranged in matrix format. If the digit of the key is \( i \), then the position of the transposition message matrix column is read as follows:

\[
(1, i) \ (2, i + 1) \ (3, i) \ (4, i + 1) \ (5, i) \ .... \ (m, n) \ ... \ ...
\]  

After a transposition is processed with a lock on a symmetric encryption cipher, the same key is used for process of decryption. If the digit of the key is \( i \), then the position of the transposition message matrix row is read as follows:

\[
(i, 1) \ (i + 1, 2) \ (i, 3) \ (i + 1, 4) \ (i, 5) \ ... \ (m, n) \ ..........
\]  

The number of digits in the key used in the zig-zag cipher algorithm depends on the number of rows when using row transpositions and depends on the number of columns when using transposition columns [8].

3. Result and Discussion

The result showed that complexity of the combined algorithm is \( \theta(n^2) \), while the complexity of Zig-zag Cipher and RC4+ Cipher are \( \theta(n^2) \) and \( \theta(n) \), respectively. The test results obtained for the .doc file extension are divided into several parts: plaintext text in Figure 1, plaintext symbols in the Figure 2 and the plaintext complex (text, symbols and images) in Figure 3.

![Figure 1. The Length of Text’s Plaintext .doc File Over Time Encryption Process Graph](image1)

![Figure 2. The Length of Symbol’s Plaintext .doc File Text Over Time Encryption Process Graph](image2)
Figure 3. The Length of Complex’s Plaintext .doc File Over Time Encryption Process Graph

The test results obtained for the pdf file extension are also divided into several parts: plaintext text in Figure 4, plaintext symbols in Figure 5 and plaintext complexes (text, symbols and drawings) in Figure 6.

Figure 4. The Length of Text’s Plaintext Pdf File Over Time Encryption Process Graph

Figure 5. The Length of Symbol’s Plaintext Pdf File Over Time Encryption Process Graph
4. Conclusion

The conclusions of an implementation of RC4* Algorithm and Zig-zag Algorithm in Super Encryption Scheme for Text Security are:

- The transposition method of Zig-zag Cipher algorithm used at the time of encryption must be the same as the transposition method used at the time of decryption to obtain the same plaintext result.
- When encrypting more than once using Zig-zag Cipher algorithm and RC4* Cipher algorithm with plaintext and same key will produce different ciphertext. This is due to the addition of capital letters to the remaining Zig-zag Cipher matrix algorithms that have not been filled.
- The result of the decryption process of Zig-zag Cipher algorithm combination and RC4* Cipher algorithm is the same although the encryption obtained is different when encrypting more than once with the same plaintext and key.
- Based on the plaintext length graph of the process time, the plaintext length is proportional to the linear graph. That is, the longer plaintext then the time required to perform the encryption is longer too.
- Based on the complexity value of both algorithm used is Zig-zag Cipher algorithm and RC4* Cipher algorithm obtained by result Θ\( (n^2) \). This complexity sometimes has a faster time so that it’s form a parabolic graph.

References

[1] Churchhouse RF 2002 *Code and Ciphers: Julius Caesar, the Enigma and the Internet* (Cambridge: Cambridge University Press).
[2] Ariyus D 2008 *Pengantar ilmu Kriptografi, Teori, analisis dan Implementasi* (Yogyakarta: Penerbit Andi).
[3] Biryukov A, De Canniere C, Braeken A and Preneel B 2003 A toolbox for cryptanalysis: Linear and affine equivalence algorithms *Eurocrypt* 2656 pp 33-50.
[4] Iswahyudi C, Setyaningsih E and Widyastuti N 2012 Pengamanan kunci enkripsi citra pada algoritma super enkripsi menggunakan metode end of file *Proc. SNAST* 3 pp 278-85.
[5] Alghazzawi DM, Hasan SH and Trigui MS 2013 Stream Ciphers: A Comparative Study of Attacks and Structures *Int. J. Comput. Appl.* 83(1) pp 27-9.
[6] Paul G and Maitra S 2012 *RC4 Stream Cipher and Its Variants* (London: CRC Press Taylor & Francis Group).
[7] Budiman MA and Rachmawati D 2017 On Using Goldbach G0 Codes and Even-Rodeh Codes for Text Compression *IOP Conf. Series: Mater. Sci. Eng.* 1 pp 1-5.
[8] Padmapriya, Ph.D. A. & Mu. Annalakshmi, 2013. Zigzag Ciphers: A Novel Transposition Method. *International Journal of Computer Applications* (0975 – 8887), 8-12. Annalakshmi M and Padmapriya A 2013 Zigzag Ciphers: A Novel Transposition Method *Proc. IJCA* 2 pp 1-4.
8-12.