Comparative analysis of RC4+ algorithm, RC4 NGG algorithm and RC4 GGHN algorithm on image file security

F Akbar¹, H Mawengkang² and S Efendi³

¹Master Program (S2) of Informatics Engineering, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan, Indonesia.
²Department of Mathematics, University Sumatera Utara, Medan, Indonesia.
³Faculty of Computer Science and Information Technology, University of Sumatera Utara, Medan, Indonesia.

¹faridakbarusu@gmail.com,²hmawengkang@yahoo.com,³syahnyata@gmail.com

Abstract. File security is very important in maintaining the confidentiality of the information contained in the file. For that we need a way for information to be kept secrecy, that is with the science of cryptography. Cryptography is one method that disguises data to form encrypted data. In the symmetric RC4 + (Ron Code or Rivest's Cipher) algorithm, it provides secure message security and is an efficient stream cipher. RC4 NGG stream cipher algorithm 3-5 times faster than RC4 algorithm and but still have weakness in KSA randomization. The RC4 GGHN stream cipher algorithm is based on the RC4 algorithm and is relatively more efficient but still has weaknesses. Based on literature review from several research sources, it was stated that RC4+, RC4 NGG, RC4 GGHN are algorithms that are faster and more efficient than RC4 algorithm. Therefore, it is necessary to compare the encryption process with the aim of comparing and knowing which algorithm is better from running time and algorithm complexity. In this research we will perform two tests on each algorithm, image encryption using different key length and same image size and image encryption using the same key length and different image size. The results obtained in this research is RC4 NGG algorithm is the fastest algorithm between the three algorithms that is 13.3% faster than RC4+ and 10.2% faster than RC4 GGHN where the key lengths used in encryption do not affect the processing time and image size used in encryption very affects the processing time.

1. Introduction

RC4 is one type of stream cipher, that processing unit or input data at one time. In this way both encryption and decryption can be performed on variable lengths. This algorithm does not have to wait for a certain number of input data before it is processed, or add additional bytes to encrypt it. The RC4 encryption method is very fast about 10 times faster than the Data Encryption Standard (DES) [1].

In the symmetric RC4 + (Ron Code or Rivest's Cipher) algorithm, it provides secure message security and is an efficient stream cipher [2]. The RC4 + algorithm is a symmetric algorithm used to encrypt and decrypt messages, and use the same key in the encryption-decryption process. The key that is used is key RC4 + key session [3].

There are two new ciphers, named Sheet Bend and Bowline, developed by extending RC4 to 32 bits. This new algorithm is called RC4 (n, m). Then, the NGG name was adopted for
this password after the initials of the designers. Another version of the NGG was introduced and came to be known as GGHN cipher.

In the research of Riad et al. [4] in a journal entitled “Security Evaluation and Encryption Efficiency Analysis of RC4 Stream Cipher for Converged Network Applications”. Declare that RC4 algorithm is very safe and an efficient stream cipher that can be used to secure convergence network.

In the research of Banik & Jha. [5] in a journal entitled “Some Security Results of the RC4 + Stream Cipher”. Declare that the RC4 + stream cipher algorithm can provide maximum resistance to a distinguishing attack if the ground used as a parameter design is made equal to 0x03.

In the research Kircanski et al. [6] in a journal entitled “A new distinguishing and key recovery attack on NGG stream cipher”. Declare that RC4 NGG stream cipher algorithm 3-5 times faster than RC4 algorithm and but still have weakness in KSA randomization.

In the research Kircanski & Youssef [7] in a journal entitled “On the Weak State in GGHN-like Ciphers”. Stating that the RC4 GGHN stream cipher algorithm is based on the RC4 algorithm and relatively more efficient but still has weaknesses.

Based on literature review from several research sources, it was stated that RC4 +, RC4 NGG, RC4 GGHN are algorithms that are faster and more efficient than RC4 algorithm. Therefore, in this research will be done comparison of encryption process and decryption algorithm RC4 + with algorithm which will be compared by writer that is RC4 NGG and RC4 GGHN in image file.

The purpose of doing this comparison analysis is to compare and know which algorithm is better in running time. Based on the explanation above, the writer will do comparison analysis of RC4 + algorithm, RC4 NGG algorithm and RC4 GGHN algorithm on image file security.

2. Study of literature

2.1. RC4+ Algorithm

RC4+ Cipher is one type of RC4 algorithm. Where the RC4 algorithm is one of the symmetric key algorithms in the form of a stream cipher that performs the encryption / decryption process in one byte and uses the same key.

The structure of the RC4+ Cipher algorithm is the same as the RC4 Cipher algorithm. Both algorithms have a Key Scheduling Algorithm (KSA). The KSA of RC4+ Cipher algorithm as follows:

```plaintext
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
```

Figure 1. Key scheduling algorithm (KSA) RC4 +
Unlike RC4 Cipher algorithm, Pseudo Random Generation Algorithm (PRGA) of RC4+ Cipher algorithm is different from RC4 Cipher algorithm. Systematic PRGA RC4+ Cipher algorithm is written as follows:

```
while |cipherkey| < |plaintext|:
    i := i + 1
    a := S[i]
    j := j + a

    Swap S[i] and S[j]  
    (b := S[i]; S[i] := a; S[j] := b; S[j] := a)

    c := S[i]<<<5 (j >> 3] + S[j]<<<5 (i >> 3]

    output (S[i]+b] + S[c⊕0xAA]) (⊕ S[j]+b]
```

**Figure 2.** Pseudo Random Generation Algorithm (PRGA) RC4 +

Figure 2 shows the Pseudo Random Generation Algorithm (PRGA) of the RC4+ Cipher algorithm, where i and j are 8-bit array indexes, S is all possible 256 permutations, << and >> is left and right shift, ⊕ is exclusive OR [8].

### 2.2. NGG and GGHN algorithms

There are two new ciphers, named Sheet Bend and Bowline, developed by extending RC4 to 32 bits. Then proposed a generalization of RC4 in order to extend RC4 to 32/64 bits with a much smaller state size of 232 or 264. This new algorithm is called RC4 (n, m), where N = 2n is the state array size in words, m is the size of the word in bits, n ≤ m. Then, the NGG name was adopted for this password after the initials of the designers. NGG KSA and PRGA update index i, j in the same way as RC4 KSA and PRGA. In the KSA NGG, the S array is initialized to a predetermined random array a. Then, S [i] and S [j] are exchanged and the sum of these two elements (modulo M = 2m) is set to S [i].

```
Input:
    1. Secret key array K[0 . . . N - 1].
    2. Precomputed random array a[0 . . . N - 1].

Output: Scrambled array S[0 . . . N - 1].

Initialization:
    for i = 0, . . . , N - 1 do
        S[0] = a[0];
        j = 0;
end

Scrambling:
    for i = 0, . . . , N - 1 do
        j = (j + S[i] + K[i]) mod N;
        Swap(S[i], S[j]);
        S[i] = (S[i] + S[j]) mod M;
end
```

**Figure 3.** Key Scheduling Algorithm (KSA) NGG
In the PRGA phase, a pseudo-random element is sent to the output and soon after it is modified by the addition (modulo M) of the other two elements of the S array.

\[
\text{Input: Key-dependent scrambled array } S[0 \ldots N - 1]. \\
\text{Output: Pseudo-random keystream bytes } z. \\
\text{Initialization:} \\
i = j = 0; \\
\text{Output Keystream Generation Loop:} \\
i = (i + 1) \mod N; \\
i = (i + S[i]) \mod N; \\
\text{Swap}(S[i], S[j]); \\
\text{Output } z = S[(S[i] + S[j]) \mod M] \mod N; \\
S[i] = ((S[i] + S[j]) \mod M) \mod N; \\
k = (k + S[i]) \mod M; \\
\]

**Figure 4.** Pseudo Random Generation Algorithm (PRGA) NGG

Another version of the NGG was introduced and came to be known as GGHN cipher. In GGHN, in addition to i, j, the third variable k is used to improve the security of the cipher. k is initialized in KSA and depends on the key. The number of loop loops KSA r depends on the parameter n, m.

\[
\text{Input:} \\
1. \text{Secret key array } K[0 \ldots N - 1]. \\
2. \text{Precomputed random array } a[0 \ldots N - 1]. \\
\text{Output:} \\
1. \text{Scrambled array } S[0 \ldots N - 1]. \\
2. \text{Key-dependent secret variable } k. \\
\text{Initialization:} \\
\text{for } i = 0, \ldots, N - 1 \text{ do} \\
\text{if } i = a[i] \text{ then} \\
\text{end} \\
\text{Scrambling:} \\
\text{repeat} \\
\text{for } i = 0, \ldots, N - 1 \text{ do} \\
1. \text{Swap}(S[i], S[j]); \\
S[i] = (S[i] + S[i]) \mod M; \\
k = (k + S[i]) \mod M; \\
\text{end} \\
\text{until } r \text{ iterations}.
\]

**Figure 5.** Key Scheduling Algorithm (KSA) GGHN

In PRGA, k is used to update S as well as to disguise output [9].
3. Finding and Discussion

3.1 Method of collecting data

In this research will be done 2 test:

1. Encrypt the image using different key lengths and same image.
2. Encrypt the image using the same key length and image size differently.

The data used in this research is the key in the form of random string and image with format *.BMP. Research materials are obtained from various sources such as books, journals, proceedings, electronic reading sources, and consultation results with lecturers.

3.2. Test result

In this section comparisons will be made at the time required to complete the process on the RC4+, RC4 NGG, and RC4 GGHN algorithms. Comparison is done on the influence of the key length on the processing time on each algorithm and on the effect of the image size to the processing time on each algorithm.

3.2.1. Comparison of Key Lengths to Process Time

Comparisons were performed on RC4+, RC4 NGG, and RC4 GGHN algorithms. Table 1 shows algorithm time processing with the same sized image 600x600 and different key lengths.

| No. | Key Length | RC4+     | RC4 NGG   | RC4 GGHN |
|-----|------------|----------|-----------|----------|
| 1   | 50         | 77.25 ms | 69.85 ms  | 74.47 ms |
| 2   | 100        | 79.15 ms | 68.89 ms  | 74.62 ms |
| 3   | 150        | 77.30 ms | 69.78 ms  | 75.51 ms |
| 4   | 200        | 75.98 ms | 68.28 ms  | 74.20 ms |
| 5   | 250        | 78.06 ms | 69.09 ms  | 74.16 ms |

Figure 7 shows the comparison of the processing time of each algorithm with the same image input and different key lengths.
Based on table 1 and figure 7 it can be seen that the NGG RC4 algorithm is the fastest algorithm in performing the process time and the different key length does not significantly affect the processing time in each algorithm whether RC4 +, RC4 NGG or RC4 GGHN.

3.2.2. Comparison of Image Size to Process Time
Comparisons were performed on RC4 +, RC4 NGG, and RC4 GGHN algorithms. Table 2 shows the algorithm time process with the same key length that is 250 characters and the image size is different.

| No. | Image Size | RC4+ | RC4 NGG | RC4 GGHN |
|-----|------------|------|---------|----------|
| 1   | 200x200    | 8.29 ms | 7.49 ms | 9.09 ms  |
| 2   | 300x300    | 20.61 ms | 17.08 ms | 18.60 ms |
| 3   | 400x400    | 33.90 ms | 28.55 ms | 32.62 ms |
| 4   | 500x500    | 53.77 ms | 47.09 ms | 51.94 ms |
| 5   | 600x600    | 82.66 ms | 72.45 ms | 80.20 ms |

Figure 8 shows the comparison of the processing time of each algorithm with the same key input and different image sizes.
Based on table 2 and figure 8 it can be seen that the NGG RC4 algorithm is the fastest algorithm in performing different process time and image size greatly affect the processing time in each algorithm be it RC4 +, RC4 NGG or RC4 GGHN.

4. Conclusions
Based on the discussion and analysis that has been done got the conclusion, each algorithm successfully completed the process of image encryption and can be used in image. NGG algorithm can do image encryption faster than other algorithm that is algorithm RC4 + and RC4 GGHN.

1. The key length used in encryption does not significantly affect the processing time of the three algorithms, either RC4 +, NGG or GGHN.
2. The image size used in encryption greatly affects the processing time of the three algorithms be it RC4 +, NGG or GGHN.
3. Based on the results obtained NGG algorithm is the fastest algorithm among the three algorithms is 13.3% faster than RC4 + and 10.2% faster than GGHN.

5. References
[1] Mollin, R.A. 2007. An Introduction to Cryptography. 2nd Ed. Chapman & Hall/CRC: Florida.
[2] Munir, R. 2006. Kriptografi. Penerbit Informatika: Bandung.
[3] Kromodimoeljo, S. 2010. Teoridan Aplikasi Kriptografi. SPK IT Consulting: Jakarta.
[4] Riad, A E D., Elminir H K., Shehata A R., & Ibrahim T R. 2013. Security Evaluation and Encryption Efficiency Analysis of RC4 Stream Cipher for Converged Network Applications. Journal of electrical engineering, VOL. 64
[5] Banik, S., & Jha, S. 2015. Some Security Results of the RC4 + Stream Cipher.Security Comm. Networks 2015.
[6] Kircanski, A., Youssef, A M., & Al-Zaidy, R. 2009. A new distinguishing and key recovery attack on NGG stream cipher. Cryptogr. Commun. (2009).
[7] Kircanski, A., & Youssef, A M. 2012. On the Weak State in GGHN-like Ciphers. 2012 Seventh International Conference on Availability, Reliability and Security.
[8] Paul, G., & Maitra, S. 2012. RC4 Stream Cipher and Its Variants. CRC Press Taylor & Francis Group: London.
[9] Gong, G., Gupta, K.C., Hell, M. & Nawaz, Y., 2005. Towards a general RC4-like key stream generator. Conference on Information Security and Cryptology. 3822: 162–174, New York.: Springer.