Analysis of *RC6-Lite* Implementation for Data Encryption

Amin Subandi[1*], Maya Silvi Lydia[1] and Rahmat Widia Sembiring[2]
[1]*Faculty Computer and Information Technology, Universitas Sumatera Utara, Medan - Indonesia*
[2]*Politeknik Negeri Medan, Medan – Indonesia*

Keywords: Cryptography, RC6, RC6-Lite, Implementation, Encryption.

Abstract: *RC6* is a simple modern cryptographic algorithm but can provide sufficient security for data encryption and decryption, *RC6* is a parameterized algorithm with *RC6-w / r / b*, where the suggested *w* values are 16, 32 and 64 and *r* values (rotation of encryption processing) is 20, while *b* is the user-specified key length. In this study, the authors are interested to implement with the *Microsoft Visual Basic 2005 Express Edition* programming language and to determine the effectiveness of *RC6* with the lowest parameters of the suggested *RC6 8/5 / b*, and we call it with *RC6-Lite*. From the result of the research, it can be concluded that for the change in plaintext, the average value of avalanche effect produced is 26.49% and for the changes made on the key, the average value of avalanche effect produced better that can reach 52.38%. And this is of course still better than the classic Playfair and Vigenere cipher algorithms which each have only avalanche effect of 10.9% and 3.1% (Saeed & Rashid, 2010).

1 INTRODUCTION

One of the techniques for securing data that can be used is cryptographic techniques, cryptography is the science and art to maintain the confidentiality and security of information on a data using mathematical techniques that are poured into the form of algorithms.

Cryptography is only considered as a security of electronic data communications, whereas since 2000 B.C. (Paar, 2010) where electronic data communication has not existed, this cryptography science has been applied.

In the days of ancient Rome, it was told that Julius Caesar sent a secret message to a General on the battlefield, so that to secure the information in the message from the others during the delivery process, the message was randomized so that only the General was aware of the information in the message (Ariyus, 2008).

From its time, cryptography is divided into modern and classical cryptographic algorithms. Classical cryptography works in alphabet mode while modern cryptography works in bit mode. While the key, the cryptographic algorithm is divided into key symmetric cryptography algorithms and asymmetric keys. The symmetric key encrypts and decrypts a message with the same key while the asymmetric uses a different key in the encryption and decryption process.

Rivest Code 6 (RC6) is a modern block cipher cryptography algorithm which is the closest rival algorithm of the Rijndael algorithm, Rijndael is the winning algorithm of the new Advanced Encryption Standard (AES) algorithm search competition held by the National Institute of Standards and Technology (NIST) this is held to look for new algorithms to replace the DES algorithm. RC6 filed by Ronald Linn Rivest et al of RSA Security Inc. In 1998. Famously simple but has a pretty good security. The algorithm is simple because in this algorithm contains six basic primitive operations such as addition, subtraction, *XOR*, multiplication and shifting bit either right or left (Fishawy & Zaid 2007).

This algorithm has three processes, the process of key expansion, encryption and the decryption process. The key expansion process is the process to generating *S-box* keys with user keys, while encryption is the process of encoding messages with *S-box* keys that have been generated from the key expansion process, as well as the decryption process.

The RC6 algorithm is a parameterized code block algorithm with the parameter RC6-w / r / b where *w* is the size of the word block, *r* is the number of encryption rotations whereas *b* is the key length specified by the user. The suggested *w* values are 16, 32 and 64. The standard RC6 filed on NIST has RC6-

Subandi, A., Lydia, M. and Sembiring, R.
Analysis of RC6-Lite Implementation for Data Encryption.
DOI: 10.5220/0010037500420047
In *Proceedings of the 3rd International Conference of Computer, Environment, Agriculture, Social Science, Health Science, Engineering and Technology (ICEST 2018)*, pages 42-47
ISBN: 978-989-758-496-1

32 / 20 / b parameters, each block having 32 bits and encrypting 20 rounds. For the maximum quality of safety parameters RC6 32/20/16 is recommended (Ahmed et al, 2007) In the encryption process this algorithm does it on every four plaintext blocks if in the last phase of the encryption process is not sufficient then padding bits on plaintext to four the last plaintext block is fulfilled.

Much research has been done in implementing this RC6 algorithm, and with the above parameters, this algorithm is able to provide enough security. However, for cryptanalysis against RC6 this is best attacked by *X2* (Terada & Ueda, 2009), and to overcome this, Terada & Ueda (2009) do research by modifying RC6 to RC6T, where they add *T ( )* function, a simple additional swap on each round.

In this study, the authors are interested to analyze and implement the RC6 algorithm on text data with the lowest parameter and the author call it as RC6-Lite is RC6 with a variant of parameter RC6-8 / 5 / b. Thus, RC6-Lite will encrypt the characters (8 bits) and 4 characters (32 bits) of processing not per four characters (32 bits) per block and 16 characters (128 bits) per process as in the standard RC6, 5 times the encryption process rotation is not 20 times. With the RC6-Lite parameter how is its effectiveness ?, to measure its effectiveness, the author will calculate the value of avalanche effect generated from this RC6-Lite algorithm.

2 METHODS

2.1 Key Expansion Procedure

This procedure is used for generating internal keys based on the secret key *K* to populate the *S* table, the number of *S* variables is 2 (*r* + 2). In populating the *S* table, RC6 uses two magical constants *Pw* and *Qw*.

$$Pw = Odd((e - 2) \times 2^w) \quad (1)$$

$$Qw = Odd((\emptyset - 1) \times 2^w) \quad (2)$$

Where :

w = 16, 32 and 64

e = 2.718281828459 ... (logarithmic base) and

$\emptyset$ = 1.6180339887... (golden ratio)

the *Odd(x)* function will produce the odd integer closest to *x*.

Pada penelitian ini, nilai *w* = 8, sehingga nilai konstanta *Pw = 185 = b9* dan *Qw = 159 = 9f*

The key expansion procedure can be seen in the following pseudocode:

```
S[0] = Pw
for i = 1 to (2r+3) do
{ S[i] = S[i-1] + Qw }
x, y, i, j = 0
for k = 1 to (3 x (2r+4)) do
{ S[i] = (S[i] + x + y) <<< 3
  x = S[i]
  L[j] = (L[i] + x + y) <<< 3
  y = L[j]
  i = (i+1) mod (2r+4)
  j = (j+10 mod c
}
```

From the pseudocode above, in this study with the value of *r* = 5, it will generate as many as 14 pieces of the key *S*. In the standard RC6, the above process will produce *S* key of 44 pieces. While *c* is the number of keys entered by the user. This *S* key will be used for the encryption and decryption process, where the first two keys will be used for the initial whitening process, and the last two keys are used for the final whitening process and the rest is used for encryption of r times.

2.2 Encryption and Decryption Procedure

RC6-Lite algorithm in this research will break the block data of 32 bit into 4 pieces of 8 bit block, then this algorithm work with 4 8-bit registers of *A, B, C* and *D*. In the process will be obtained *(A, B, C, D) = (B, C, D, A)* which means that the value located on the right side comes from the register on the left side. The encryption and decryption process of the RC6 algorithm begins and ends with a whitening process that aims to disguise the first and last iteration of the encryption and decryption process, and in the process requires 14 subkeys that have been generated in the key expansion process and named with *S [0]* to *S [13]* each of which is 8-bit in length. In each iteration in the encryption process used 2 (two) subkeys. The sub-keys in the first iteration use *S [2]* and *S [3]*, the next iteration uses sub-advanced subkeys.

For the encryption process can be clearly seen in the following figure:

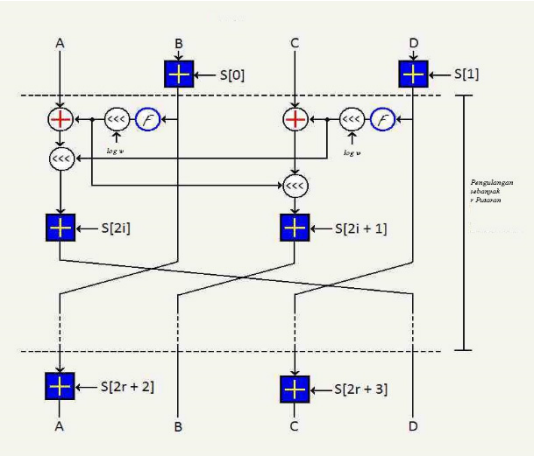

Figure 1: Encryption Scheme of RC6.

Pseudocode for encryption process can be seen as follows:

```
B = B + S[ 0 ]
D = D + S[ 1 ]
for i = 1 to r do
{ t = ( B x ( 2B + 1 ) )<<< 5
  u = ( D x ( 2D + 1 ) )<<< 5
  A = (( A ⊕t )<<< u )+ S[ 2i ]
  C = (( C ⊕u )<<< t )+ S[ 2i + 1 ]
  (A, B, C, D) = (B, C, D, A)
}
A = A + S[ 42 ]
C = C + S[ 43 ]
```

Pseudocode for decryption process is described below:

```
C = C - S[ 43 ]
A = A - S[ 42 ]

for i = r downto 1 do
{ (A, B, C, D) = (D, A, B, C)
  u = ( D x ( 2D + 1 ) )<<< 5
  t = ( B x ( 2B + 1 ) )<<< 5
  C = ((C - S[ 2i + 1 ] )>>> t ) ⊕u
  A = ((A - S[ 2i ] ) >>> u ) ⊕t
}

D = D - S[ 1 ]
B = B - S[ 0 ]
```

2.3 System Scheme

In implementing this RC6-Lite algorithm, the authors use *Microsoft Visual Basic 2005 Express Edition*, with the system scheme to be created can be seen in the following figure:

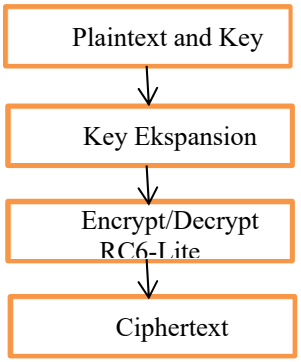

Figure 2: System scheme in this research.

Plaintext and user-keys entered by the user, then performed the process of key expansion to generate the *S-Key*, then do the encryption or decryption process with RC6 Lite to generate ciphertexts.

2.4 Comparison of Avalanche Effect

Avalanche effect is one of the ways to measure the effectiveness of an algorithm, avalanche effect is the bit changes that occur when plaintext or key changes, it will produce different ciphertext bits, the greater the level of its avalanche effect, the more difficult for the cryptanalyst to do the attack.

The algorithm is good if the avalanche effect value is 45 to 60%, to calculate the avalanche effect value using the following formula:

$$avalanche\ effect = \frac{No.\ of\ bit\ spilts}{total\ of\ bits}\ x\ 100 \quad (3)$$

In this research will be adding and subtraction of characters both on plaintext and key, and also replacement of one character either plaintext or key.

3 RESULT AND DISCUSSIONS

As the research data, plaintext and key used are as follows:

Plaintext : `THE KEY IS UNDER THE TABLE`
Key : `THE KEY`

Based on the application that the authors created using the RC6-Lite algorithm, the resulting ciphertext is as follows:

Ciphertext : ™¢‹ FäƒÇ«<+Þ‰Ì.Æ¯ÕÔbZä> Ú&£l

Viewed from the resulting ciphertext, it appears that the length of the ciphertext is longer than plaintext, this is due to the addition of padding made to plaintext which is not a multiple of 4 (RC6-Lite encrypts every 4 characters), padding in this study is done by adding the character " * " On plaintext. More details can be seen in the following figure:

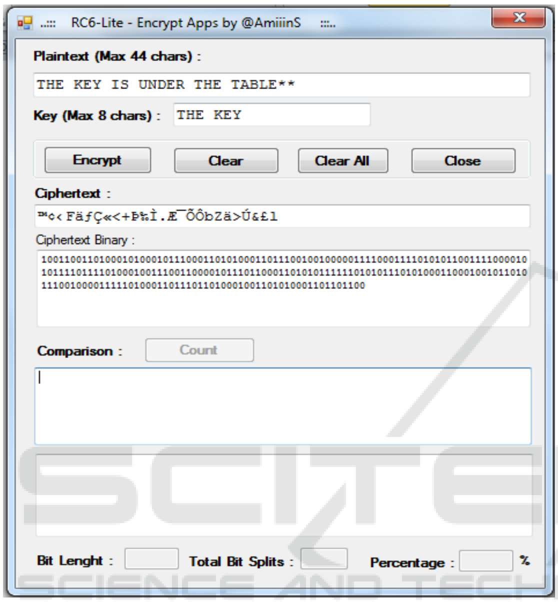

Figure 3: Encryption Application.

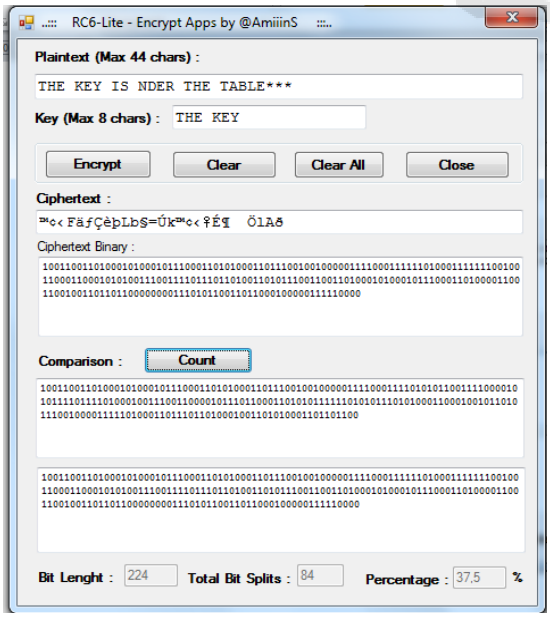

Figure 4: Comparison experiment.

The first test made a change to plaintext, that is by removing the character "U" and still with the same Key, the test results as shown there are images and described as follows:

The first test:

Key : THE KEY
Plaintext1 : THE KEY IS UNDER THE TABLE
Bit Ciphertext1 :
1001100110100010100010111000110101000110111001001000001111000111101010
1100111100001010111101111010001001110011000010111011000110101011111101
0101110101000110001001011010111001000011111010001101110110100010011010
10001101101100
Plaintext2 : THE KEY IS NDER THE TABLE
Bit Ciphertext2 :
1001100110100010100010111000110101000110111001001000001111000111111010
0011111111001001100011000101010011100111011101101001101011100110011010
0010100010111000110100001100110010011011011000000001110101100110110001
00000111110000

The resulting bit length is 224 bits, with the number of bits split is 84 bits thus the avalanche effect percentage is 37.5%.

The second test:

Key : THE KEY
Plaintext1 : THE KEY IS UNDER THE TABLE
Bit Ciphertext1 :
1001100110100010100010111000110101000110111001001000001111000111101010
1100111100001010111101111010001001110011000010111011000110101011111101
0101110101000110001001011010111001000011111010001101110110100010011010
10001101101100
Plaintext2 : THE KEY ISS UNDER THE TABLE
Bit Ciphertext2 :
1001100110100010100010111000110101000110111001001000001111000111110100
1111101111110101111000010000011100011011000000101111101101111010111110010010110101111111000101000100110010
0011111111001100010001001100111100110000101111111

The resulting bit length is 224 bits, with the number of bits split is 78 bits thus the avalanche effect percentage is 34.82%.

The third test :

Key : THE KEY
Plaintext1 : THE KEY IS UNDER THE TABLE
Bit Ciphertext1 :
10011001101000101000101110001101010
00110111001001000001111000111101010
11001111000010101111011110100010011
10011000010111011000110101011111101
01011101010001100010010110101110010
00011111010001101110110100010011010
10001101101100
Plaintext2 : THE REY IS UNDER THE TABLE
Bit Ciphertext2 :
10011001101000101000101110001101110
00101101100101011111100101110101010
11001111000010101111011110100010011
10011000010111011000110101011111101
01011101010001100010010110101110010
00011111010001101110110100010011010
10001101101100

The resulting bit length is 224 bits, with the number of bits split is 16 bits thus the avalanche effect percentage is 7.14%.

The fourth test:

Key1 : THE KEY
Key2 : THE EY
Plaintext1 : THE KEY IS UNDER THE TABLE
Bit Ciphertext1 :
10011001101000101000101110001101010
00110111001001000001111000111101010
11001111000010101111011110100010011
10011000010111011000110101011111101
01011101010001100010010110101110010
00011111010001101110110100010011010
10001101101100
Bit Ciphertext2 :
00000101101001010100000100010010111
01001100101100011101001011100011110
00010100100100001101010101011111000
10001100001101000101111100011111110
10101100101000010111000101101000011
00010010111100110111000011111000001
11000111000100

The resulting bit length is 224 bits, with the number of bits split is 119 bits thus the avalanche effect percentage is 53.12%.

The fifth test:

Key1 : THE KEY
Key2 : THE KEYS
Plaintext1 : THE KEY IS UNDER THE TABLE
Bit Ciphertext1 :
10011001101000101000101110001101010
00110111001001000001111000111101010
11001111000010101111011110100010011
10011000010111011000110101011111101
01011101010001100010010110101110010
00011111010001101110110100010011010
10001101101100
Bit Ciphertext2 :
11101000101011100011101111100110011
11001101111111101011100011110011001
10001100011010011000000011100011101
10011010110110010010011010010101011
01100111010100011111101010001101000
10010100001101000100010000010000001
01101110101111

The resulting bit length is 224 bits, with the number of bits split is 110 bits thus the avalanche effect percentage is 49,11%.

The sixth test:

Key1 : THE KEY
Key2 : THE REY
Plaintext : THE KEY IS UNDER THE TABLE
Bit Ciphertext1 :
10011001101000101000101110001101010
00110111001001000001111000111101010
11001111000010101111011110100010011
10011000010111011000110101011111101
01011101010001100010010110101110010
00011111010001101110110100010011010
10001101101100
Bit Ciphertext2 :
11001010111001000001111110010011011
01100001110010001111000000101000001
00011001111001010011110101111001110
00011100110000000001110011100101000
00111100000101110010011001011010111
10010000000100110011001011100000100
10110010111101

The resulting bit length is 224 bits, with the number of bits split is 123 bits thus the avalanche effect percentage is 54.91%.

To prove that the application in this study can restore plaintext as before, the simulation can be seen in the following figure:

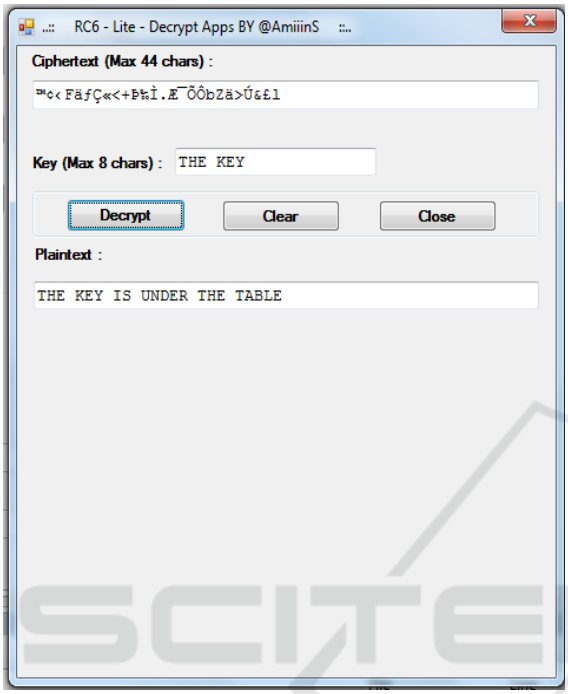

Figure 5: Decryption application.

4 CONCLUSIONS

From the result of research can be concluded that:

- Implementation done in this research using *Microsoft Visual Basic 2005 Express edition* application can encrypt and decrypt the data, provided that the key entered by the user is equal.
- For changes to plaintext, such as deletion, addition and replacement of one character, the average avalanche effect yielded 26.49%, this result is even smaller than the resulting of 54.6% DES in the Saeed & Rashid (2010) research and lost thinner than Blowfish 28.71% in Ramanujam & Karuppiah (2011) research, this may be caused by RC6 algorithm to block each process, so the effect that occurs only on the block of each process, in RC6-Lite only do the process of encryption and decryption at 32 bits each, and RC6 encrypts every 128 bits. Nevertheless, RC6-Lite is still better than the 7.8% SDES algorithm and from the classical Playfair cryptography of 10.9% and Vigenere 3.1% (Saeed & Rashid, 2010).
- For changes to the Key, such as deletion, addition, and replacement of one character, the results show that the resulting avalanche effect reaches an average value of 52.38%, this proves that the key expansion process in this RC6-Lite can play an important role in encryption and decryption on this algorithm.

REFERENCES

Ahmed. H.E.H., Kalash, H.M. & Farag Allah, O.S., 2007. *Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images*. Institute of Electrical and Electronics Engineers (IEEE), DOI 10.1109/ICEE.2007.4287293.

Ariyus, D. 2008. *Pengantar Ilmu Kriptografi, Teori Analisis dan Implementasi.* Penerbit ANDI: Yogyakarta.

Fishawy, N. E. & Zaid, O. M. A. 2007. *Quality of Encryption Measurement of Bitmap Images with RC6, MRC6 and Rijndael Block cipher algorithm*. International Journal of Network Security, 5(3): 241-251.

Paar, C & Pelzl, J. 2010. *Understanding Cryptography*. Springer: Verlag Berlin Heidelberg.

Ramanujam, S. & Karuppiah, M. 2011. *Designing an algorithm with high Avalanche Effect*. International Journal of Computer Science and Network Security (IJCSNS). 11(1): 106-111.

Saeed, F. & Rashid, M. 2010. *Integrating Classical Encryption with Modern Technique.* International Journal of Computer Science and Network Security (IJCSNS). 10(5): 280-285.

Terada, R. & Ueda, E. T. 2009. *A New Version of RC6 algorithm, stronger against X^2 cryptanalysis.* Conference in Research and Practice in Information Technology (CRPIT). Vol.98.