

Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process

A Subandi^{1*}, M S Lydia², R W Sembiring³, M Zarlis² and S Efendi²

¹Student of Computer Science, Universitas Sumatera Utara, Medan-Indonesia

²Departement of Computer Science, Universitas Sumatera Utara, Medan-Indonesia

³Politeknik Negeri Medan, Medan-Indonesia

*aminsubandi@yahoo.com

Abstract. Modifications to Vigenere cipher are possible to make in order to be effective and efficient of this algorithm. In this study, we tried to modify Vigenere by exploiting RC6 key expansion to generate new keys used for encryption process, RC6 is a well-known as a modern cryptographic algorithm. If the RC6 Key expansion process will generate the S key as much as $2r+4$, in this research will produce S Key as long as the plaintext length. Then for the encryption process done twice. The results show that the method proposed producing completely different key sequences (not repetitions like Vigenere cipher) can also produce an average avalanche effect of 17 bits of the total 64 bits or about 26,56 %, better than the standard Vigenere which only reached 7.81%, but unfortunately no better than Vigenere with the RC6 key expansion without twice encryption process that reaches 31.25% and of RC6-8/5/b with 35.94%.

1. Introduction

Vigenere cipher was a simple but powerful classic algorithm in its time because the people of that time had not been able to solve this algorithm until it was finally solved by Friedman and Kasiski around 1917 [1]. One of the disadvantages of this algorithm is that if the key length entered by the user is smaller than plaintext, the next key is the repetition of the user key, this will allow for the histogram, Kasiski finds a way to obtain the initial user key length from the histogram.

Modification of Vigenere ciphers is possible to make this algorithm better, but the effectiveness of the modifications performed is not always better than standard Vigenere [1], in the study [1] reviewing some modifications that have been made and concludes that the entropy and Index of coincidence of the proposed modifications do not increase significantly, there is even a subset of the standard vigenere itself.

In 2010 and 2011 studies involving Vigenere ciphers have been performed and managed to obtain a much better avalanche effect than standard vigenere [4][5], but in those studies the combination of many classical and modern algorithms, the study may effective but inefficient, because the impression of simple Vigenere is lost.

In this study, we are interested in modifying Vigenere with the aim of keeping Vigenere simple and secure by exploiting the key expansion of the Rivest Code 6 (RC6) algorithm. RC6 itself is a well-known modern algorithm but has a fairly good security standard and becomes the nearest rival of the Rijndael algorithm which is the winner of the Advanced Encryption Standard (AES) a competition to gain new standards in the



cryptographic fields organized by the National Institute of Standards and Technology (NIST) in 1997 [3]. RC6 has six basic operations such as the integer addition modulo, integer subtraction modulo, XOR operation, integer multiplication modulo and bit rotation both right and left [2]. One of the strengths of RC6 is the key-expansion, the process of combining the initial user key with the initial Skey to generate new S keys used for encryption and decryption process. In this study, we will use and slightly modify the key-expansion of RC6 where as if RC6 produces as many as $2r+4$ pieces of S key, but in this study will produce S key as much as the length of the plaintext, the S Key is then used to perform the Vigenere encryption process twice. Next, will be calculated how the avalanche effect generated from the proposed modification.

2. Theories

2.1. Vigenere Cipher

Vigenere cipher is a classical algorithm and of course a symmetric algorithm. In the process of encryption and decryption using tabula recta, a 26 x 26 matrix containing alphabet letters (Figure 2.1), where ciphertext is the alphabet letter of intersection between the Plaintext alphabet and the alphabet of keys [1] [4] [5] [6] [7] [8] [9].

		-- PLAINTEXT --					
		A	B	C	D	...	Z
K E Y	A	A	B	C	D	...	Z
	B	B	C	D	E	...	A
	C	C	D	E	F	...	B
	D	D	E	F	G	...	C

	Z	Z	A	B	C	...	Y

Figure 1. Vigenere Tabula recta 26 x 26

Mathematically, the process of encryption and decryption can be seen in the following equation:

$$Ci = E(Pi + Ki) \bmod 26 \quad (1)$$

$$Pi = D(Ci - Ki) \bmod 26 \quad (2)$$

Where C is the cipher text generated from the Encryption E process by adding the alphabetic index of Plaintext P with a Key K modulated with 26, and vice versa Plaintext P is generated from the Decryption D process by subtracting the Cipher text C alphabet index with key K and also modulated with 26.

2.2. RC6 Key Expansion

RC6 is the development of the previous algorithm that is RC5. RC6 is a parameterized cipher block algorithm with RC6-w/r/b [3]. The parameter w is the number of bits in each block with the suggested value is 32, the parameter r indicates the number of iterations during the encryption process the suggested value is 20 and b is the key length specified by the user so that RC6 can also be written as RC6-32/20/b.

There are three processes in RC6 that are Key-Expansion process, encryption, and decryption process. Key-expansion process. It functions to combine the K user key with the S key. The key-expansion procedure is as follows:

```

S[0] =  $P_w$ 
for i = 1 to  $2r+3$  do
{ S[i] = S[i-1] +  $Q_w$  }

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[j] + x + y ) <<<3
  y = L[j]
  i = ( i + 1 ) mod  $2r+4$ 
  j = ( j + 1 ) mod c
}

```

P_w and Q_w are constants defined as follows:

$$P_w = \text{Odd}((e - 2) \times 2^w) \quad (3)$$

$$Q_w = \text{Odd}((\phi - 1) \times 2^w) \quad (4)$$

With: $e = 2.718281828459 \dots$ (logarithm basis) and $\phi = 1.6180339887 \dots$ (golden ratio) w value is the number of bits used on each block, $\text{Odd}(x)$ will produce the odd integer value closest to x . This procedure will produce as much as $2r+4$ S keys that will be used to encrypt and decrypt process.

2.3. Avalanche effect

Avalanche effect is one of the ways to determine a cryptographic algorithm whether or not good if a little change occurs, both on plaintext and on the key will cause changes to the resulting ciphertext. The algorithm is said to be good if the value of avalanche effect produced high, the higher the avalanche effect then the algorithm security will be better [4] [5], because it will cause cryptanalyst difficult to do cryptanalysis technique to ciphertext obtained.

Here is the formula to calculate the value of avalanche effect:

$$\text{avalanche effect} = \frac{\text{Number of bit splits}}{\text{Total Number of bits}} \times 100\% \quad (5)$$

3. Methods

In this study, the Vigenere cipher algorithm will be modified by exploiting the RC6 key expansion process to disguise the user key that will be used for the encryption process. Also in this study will perform the encryption process twice. And all operations use 8 bit American Standard Code for Information Interchange (ASCII) characters and implemented using Microsoft Visual Basic 2005 Express Edition.

For the encryption process, first, enter the plaintext and the key, then processed key expansion as in RC6 but with a little change, then the first encryption process to get the first ciphertext, and then performed the same encryption process using the same key until finally got the final cipher text. The same procedures applied to the decryption process to restore plaintext as before.

The flow chart of the method used is illustrated as follows:

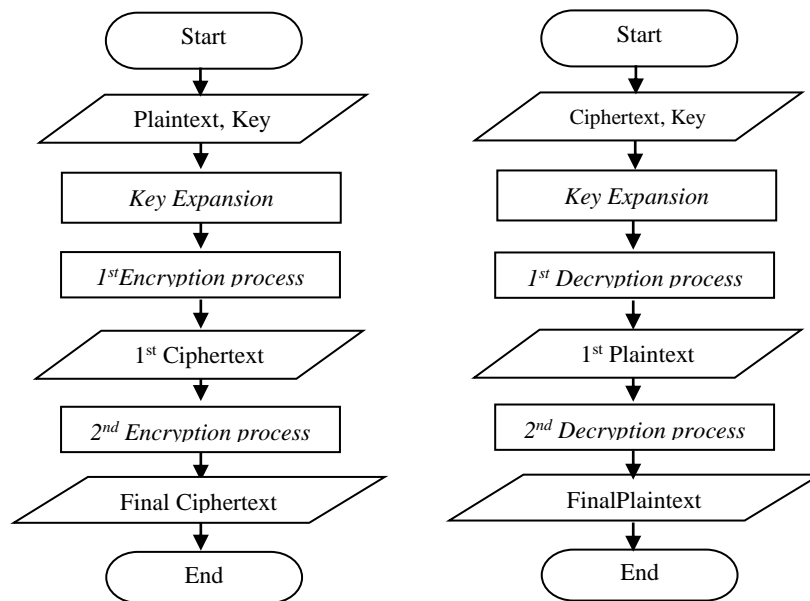


Figure 2. (a) Encryption process (b) Decryption process

Key expansion process in this research is as follows:

```

S[0] = Pw
for i = 1 to m do
{ S[i] = S[i-1] + Qw }
x, y, i, j = 0
for k = 1 to n do
{ S[i] = ( S[i] + x + y ) <<< 3
  x = S[i]
  L[j] = ( L[j] + x + y ) <<< 3
  y = L[j]
  i = ( i + 1 ) mod len(P)
  j = ( j + 1 ) mod c
}

```

Where m is the length of the plaintext minus by one and n is three times the length of the plaintext is done to combine the S key with the User key three times round. Meanwhile, since the encryption in this study uses 8 bit ASCII characters for each variable, the initial value of $P_w=185=b9$ and $Q_w=159=9f$. This key-expansion process will produce the S Key as long as plaintext length to be used for encryption and decryption Vigenere cipher.

Then do the encryption and decryption process Vigenere cipher as follows:

$$Ci = E(Pi + Si) \bmod 256 \quad (6)$$

$$Pi = D(Ci - Si) \bmod 256 \quad (7)$$

4. Result

An example of Implementation with Microsoft Visual Basic 2005 Express Edition can be seen in the following figure:

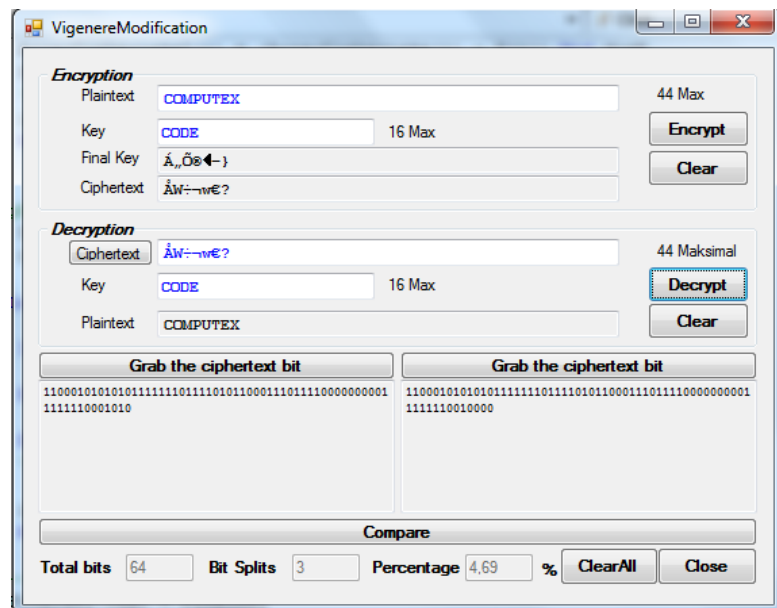


Figure 3.Example of implementation result

To perform the test used plaintext COMPUTER and CODE keys, to calculate the avalanche effect will be made a little change both on plaintext and on the user initial key, the changes in plaintext to **X**OMPUTER, **CO**MMUTER and **CO**MPUTEX while the changes in the key to **CODY**, **K**ODE and **CO**BE.

Furthermore, the comparison of avalanche effect will be done with Vigenere Cipher Standard, Vigenere modification if only exploiting RC6 key-expansion process, RC6-8/5/b that is with RC6 implementation 8 bits of data per-block with 5 times round in encryption process. And compared with Vigenere Modification proposed in this research, that is by exploiting RC6 key-expansion and double encryption process. The average of avalanche effect produced in this research can be seen in the following figure:

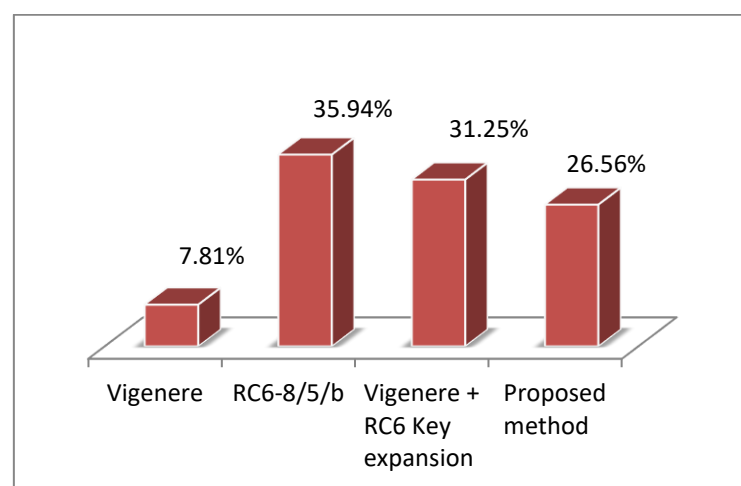


Figure 4. Results comparison of average avalanche effect generated

5. Conclusions

The conclusions of this study are as follows:

- By utilizing such key-expansion processes as in RC6 algorithm, this research succeeded in producing the completely different sequence of keys for the encryption process so it is hoped that the kasiski method will be difficult to guess the number of user's initial keys;
- If the key-expansion process in RC6 produces a key row of $2r+4$, then in this study a key number of plaintext lengths is generated then changes to the number of the plaintext will also result in changes to the key generated;
- The method proposed in this study, from 64 bits, the average avalanche effect is reached 17 bits or about 26,56%, the result is better when compared to standard Vigenere that only reached 5 bits or approximately 7.81% but it is not better than RC6-8/5/b which also the encryption process is much more complicated than the average value of the avalanche effect is reached 23 bits or about 35.94% and even the modification proposed in this study is no better than modifying Vigenere if by only adopting RC6 key-expansions that produce 20 bits or about 31.25%. That means it turns out that the double encryption process does not need to do.

References

- [1] Aliyu A-A M and Olaniyan A 2016 Vigenere Cipher: Trends, Review and Possible Modifications *International Journal of Computer Application* **135**(11): 46-50.
- [2] Fishawy N E And 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.
- [3] Paar C and Pelzl J 2010 *Understanding Cryptography* Springer Verlag Berlin Heidelberg
- [4] Ramanujam S and Karuppiyah M 2011 Designing an algorithm with high Avalanche Effect *International Journal of Computer Science and Network Security(IJCSNS)* **11**(1): 106-111.
- [5] Saeed F and Rashid M 2010 Integrating Classical Encryption with Modern Technique *International Journal of Computer Science and Network Security (IJCSNS)* **10**(5): 280-285.
- [6] Saputra I, Aan M, Hasibuan N A and Rahim R 2017 Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File *International Journal of Engineering Research & Technology (IJERT)* **6**(01): 266-269.
- [7] Singh G and Supriya 2013 Modified Vigenere Encryption Algorithm and its Hybrid Implementation with Base 64 and AES *Institute of Electrical and Electronics Engineers (IEEE)* DOI 10.1109/ADCONS.2013.33: 232-237.
- [8] Sinha N and Bhamidipati K 2014 Improving Security of Vigenere Cipher by Double Columnar Transposition *International Journal of Computer Applications* **100**(14): 6-10.
- [9] Subandi A, Meiyantri R, Sandy C L M and Sembiring R W 2017 Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography with keystream Generator Modification *Advances in Science, Technology and Engineering Systems Journal (ASTESJ)* **2**(5): 1-5.