Application and Manual Encryption Process with The Combination Algorithm of One Time Pad and Vigenere Cipher

Siti Julianita Siregar\textsuperscript{1}, Muhammad Zarlis\textsuperscript{2,}\textsuperscript{*}, Zakarias Situmorang\textsuperscript{3}

\textsuperscript{1,2}Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Padang Bulan Medan-20155, Indonesia.

\textsuperscript{3}Department of Information System, Univesity Katolik Santo Thomas Medan, Indonesia.

E-mail: m.zarlis@usu.ac.id

Abstract. Cryptography is a branch of science which study art or a way to secure an information in order to that information becomes incomprehensible to third parties who does not have the authority. The intention of cryptography also serves as multiple aspects in information security such as confidentiality, data integrity, authentication, and non-repudiation. One of the things that be done to maintain the safety of information, is by encrypting the message to disguise the original message so that third parties will not be able decipher it in the event of an interception. Therefore, in order to secure the information, by encrypting the key using a different key technique is generally done with combining two algorithms which is One Time Pad with random key generator and Vigenere cipher using XOR and XNOR. The encryption process result from One Time Pad algorithm are ciphertext while the Vigenere Cipher algorithm is the XOR cipherkey and XNOR cipherkey.

1. Introduction

As time goes by, the development of how human communicated grows constantly. One of the ways is to communicate using the exchange of messages in the form of texts, documents, images, PDF (Portable Document File) and in any other forms. The message that was sent usually contains crucial information and must be kept private.

The safety of message and information is crucial in communicating. A substantial amount of cyber-crimes searching for security to enter and manipulate. The security of the message and confidentiality is a priority. In order to ensure the security and confidentiality, it is necessary to have a technique to encode the message or information called cryptography. Cryptography is a branch of science which study art or a way to secure an information in order to that information becomes incomprehensible to third parties who does not have the authority. The intention of cryptography also serves as multiple aspects in information security such as confidentiality, data integrity, authentication, and non-repudiation.

To ensure the safety of the message, can be done by encrypting the message to disguise the original message so that third parties will not be able decipher it in the event of an interception. The strength of the cryptography is determined by which key is used. Therefore, in order to achieve the capacity of cryptography to secure the information, generally done by combining
two algorithms which is One Time Pad with random key generator and Vigenere cipher using XOR and XNOR key.

From previous authors such as Zulfidar (2014), Andi Marwan Elhanafi (2014), Yupiyanti (2014), Robbi Rahim, et al (2018), the four previous researchers where more likely to explain how a process of encryption is good with a cryptography algorithm that use a key general only. I have not found that some writing that use a combination of more than only cryptography algorithm use a One Time Pad with generate random key and combined with XOR key and XNOR key for the Vigenere Cipher Algorithm. The use generate random key in the One Time Pad algorithm here is intended to maximize the key used by minimizing the opportunity to use the same key in the next encryption using the One Time Pad algorithm, then the key in encrypted with the Vigenere Cipher using XOR and XNOR keys. The working of XOR and XNOR keys are to change the primary key with a new key by converting ASCII characters to binary then a new key will be obtained using XOR and XNOR in binary form and will be converted back into ASCII characters. After that, adding the plaintext and keys using the modulus system is expected to increase the speed of the encryption process and increase the higher security opportunities.

2. Formulation of Research Question and Objectives
Based on the introduction above, the research question in the One Time Pad algorithm, the key authentication work system at the time of the transaction can only be used once which also can be called the One Time Password, therefore the author feels the need for a development in determining a random key and combined it with another algorithm such as the Vigenere Cipher algorithm using the XOR and XNOR keys which are expected to improve the safety of the plaintext and the key in the encryption process of the message.

The objectives of this research is to improve the safety of the message by combining One Time Pad algorithm with the generate random keys and the Vigenere Cipher algorithm with the XOR and XNOR keys.

3. Methodology
In this research, the author would like to combine the One Time Pad cryptographic algorithm with the Vigenere Cipher. The process of encrypting plaintext with the One Time Pad algorithm using Generate Random Keys, then the key of the One Time Pad algorithm is encrypted using the Vigenere Cipher algorithm with keys using the XOR and XNOR keys. Afterwards, it will produce ciphertext from the encryption as a result of using the One Time Pad algorithm and cipher-key which is the result of encryption using the Vigenere Cipher algorithm.

3.1. Research Design
The research methodology used is as follows:

a. Literature Studies Author collected the information and data reference from books, journal, article and other sources regarding the One Time Pad algorithm and Vigenere Cipher algorithm using the XOR and XNOR keys.

b. Analysis and System Design This phase is used to manage the data that was collected and perform a cryptography analysis from the combination of One Time Pad algorithm and Vigenere Cipher to gain an understanding regarding the algorithm and random key, as well as XOR and XNOR keys, which is then carried out a system design based on the literature that was collected.

c. System Implementation In this phase, implementation in the application design that has been made in the analysis and the draft of the system into a computer program using the language programming Microsoft Visual Studio 2012.
d. System Evaluation After the system implementation phase, an application test is carried out to discover whether the designed system is running as expected and to conduct a research on the data that was going to be evaluated.

3.2. Encryption System Design

The encryption process that was design using One Time Pad algorithm with generate random keys and Vigenere Cipher algorithm using XOR and XNOR keys. The following figures and explanation of the stages of the encryption process:

![Figure 1. Encryption Process with the Combination of One Time Pad and Vigenere Cipher](image)

The following explanation of the stages of the encryption process combination of One Time Pad and Vigenere Cipher:

1. Determine the plaintext by creating a message.
2. Plaintext will be encrypted using the One Time Pad cryptographic algorithm using the Generate Random Keys key.
3. Ciphertext will be obtained from the plaintext encryption of the One Time Pad cryptographic algorithm with the Generate Random Keys key.
4. The key to the One Time Pad algorithm, which is the result of Generate Random Keys, will be used as a plaintext in the Vigenere Cipher algorithm.
5. The plaintext of the Vigenere Cipher algorithm will be encrypted using the XOR and XNOR keys.
6. To determine the XOR and XNOR keys will be done by determining a key from the new Generate Random Keys and will be added to the plaintext of the Vigenere Cipher algorithm.

The results of plaintext encryption from the Vigenere Cipher algorithm will get two ciphers, namely the XOR cipherkey and the XNOR cipherkey.

3.3. Encryption Process Model Design

The encryption model design of the analysis from the combination of the One Time Pad and Vigenere Cipher algorithm, the One Time Pad algorithm with Generate Random Key will be used
to encrypt messages that will later become ciphertext, while the Vigenere Cipher algorithm with XOR and XNOR keys will be used to encrypt the keys of the One Time Pad algorithm that will later become a cipherkey. For more details, you can see from the following Flowchart:

**Figure 2.** Encryption Process Flowchart using One Time Pad

**Figure 3.** Encryption Process Flowchart using Vigenere Cipher

From the figures above we can see that there will be 2 (two) algorithms namely the Vigenere Cipher and the XOR and XNOR algorithms which the function is to encrypt the keys into cipherkeys.
4. Result
The combination of the One Time Pad algorithm with the Generate Random Keys key, then the key that was produced will be encrypted using the Vigenere Cipher algorithm with the XOR and XNOR keys will be applied using the Visual Basic application program. The following text will explain the test results manually and testing using the Visual Basic application.

4.1. Manually Encryption Process of One Time Pad Algorithm and Vigenere Cipher
The encryption process using the One Time Pad algorithm can be seen through the following flowchart diagram:

![Flowchart](image)

Figure 4. One Time Pad Flowchart Algorithm

The examples to be tested as follows:
Plaintext : BELAJAR
Key(Random) : VMRLACF
Plaintext and key (random) will be transform into ASCII then using the formula One Time Pad $C = P + K \mod 26$ to obtain the results such as the table below:

| Plaintext | 1 | 4 | 11 | 0 | 9 | 0 | 17 |
|-----------|---|---|----|---|---|---|----|
| Key       | 21| 12| 17 | 11| 0 | 2 | 5  |
| Results   | 22| 16| 2  | 11| 9 | 2 | 22 |
| Ciphertext| W | Q | C  | L | J | C | W |

Therefore, the ciphertext from the encryption process of the One Time Pad algorithm with Generate Random Keys is **WQCLJCW**.

The following process is to determine the new key to XOR and XNOR using Random Keys which will then converted into binary from to perform the XOR and XNOR processes and
afterwards the results will be encrypted using the Vigenere Cipher algorithm. The following is the flowchart of the algorithm process to determine the XOR key.

**Figure 5. Flowchart Algorithm XOR Key**

Plaintext(Key OTP): **VMRLACF**
XOR Random key: **RNKKJEI**

Therefore, the new value of XOR and XNOR key encrypted using Vigenere Cipher.

Plaintext 01010110 01001101 01010010 01001100 01000001 01000011 01000110
XOR 01010010 01001110 01001011 01001011 01001010 01000101 01001001

| XOR Key 00000100 00000011 00011001 00000111 00001011 00000110 00001111 |

The binary results will be converted into ASCII is XOR Key:

```
J L •
```

The same process will be used to obtain the value of key. The following is the flowchart of the algorithm process to determine the XNOR key.
Figure 6. Flowchart Algorithm XNOR Key

Plaintext(Key OTP): **VMRLACF**
XNOR Random key: **ECNAGLM**
Plaintext 01010110 01001101 01010010 01001100 01000001 01000011 01000110
XNOR R 01010010 01001110 01001011 01001011 01001010 01000101 01001001
The binary results from XNOR key will be converted into ASCII is XOR Key: `îñáöüóó`.

After receiving the results from the XOR and XNOR key, the Vigenere Cipher encryption process using key from XOR and XNOR will take place. The following is the flowchart of Vigenere Cipher encryption process with XOR key:

Figure 7. Algorithm Encryption of Vigenere Cipher XOR Key Flowchart
\[ \text{Plaintext}(\text{KeyOTP}) : \text{VMRLACF} \]
\[ \text{KeyXOR} : \]

\[ \exists \mathcal{L}_\varphi \]

\[ \text{Cipherkey} : 3^*, ?, < . \]
\[ \text{Formula} : \text{Plaintext} + \text{KeyXOR} > 26 \text{so} \]
\[ (\text{Plaintext} + \text{KeyXOR}\text{mod}26) + 65 \]

\[ \text{Or} \]
\[ (\text{Plaintext} + \text{KeyXOR}–26) + 65 \]

**Table 2.** Encryption Process Substitution Table of Vigenere Cipher Using XOR Key.

| Plaintext | 21 | 12 | 17 | 11 | 0 | 2 | 5 |
|-----------|----|----|----|----|---|---|---|
| XOR Key   | -61| -62| -40| -58| -54| -59| -50|
| Result    | 51 | 41 | 42 | 44 | 63 | 60 | 46|
| Cipherkey | 3  | *  | ,  | ?  | i | . |

From the results of the substitution table the Viginere Cipher encryption process with the XOR key will get the XOR cipherkey value of 3^*, ?, i.

Afterwards, the VigenereCipherencryption process will be carried out using the XNOR key. The following is the flowchart of the VigenereCipher encryption process with the XNOR key:
Figure 8. Algorithm Encryption of Vigenere Cipher XOR Key Flowchart.

Plaintext : VMRLACF
KeyXNOR : ïⁿâձüôô.
Cipherkey : căÜâβφβ.

Table 3. Experiment data tsp eil51.

| Plaintext | 21 | 12 | 17 | 11 | 0 | 2 | 5 |
|-----------|----|----|----|----|---|---|---|
| XNOR Key  | 171| 176| 162| 177| 184| 175| 179|
| Result    | 231| 227| 218| 227| 223| 216| 223|
| Cipherkey | C  | Ā  | Ĉ  | Ĉβ| φ | β | β |

From the results of the substitution table the Vigenere Cipher encryption process with the XNOR key will get the XNOR cipherkey value of $c\hat{a}Ü\hat{a}βφβ$.

The final results of the encryption process from the combination of cryptography algorithm of One Time Pad and Vigenere Cipher is the value of XOR cipherkey and XNOR cipherkey.

4.2. Encryption Process Results Using Application
The following are the test results using Visual Basic:

1. Before encrypting the first message, we must first input plain text. Afterwards, press the following Encryption button as shown below

2. Encryption Process Results The encryption process previously described above will be tested using the application and the results are the same as the results using the application as shown below:
5. Discussion
The One Time Pad and VigenereCipher have the same formula in the encryption process and plaintext description. The formula used is:

Encryption: \( C_i = (P_i + K_i) \mod 26 \)

The distinction from both algorithm lies in the keys that was used. The One Time Pad algorithm using generate random keys, while the Vigenere Cipher using keys from XOR and XNOR.

The value of XOR and XNOR will be generated from the XOR and XNOR formulas with keys from the One Time Pad on XOR and XNOR, right with the new random key generate. The results of the XOR and XOR keys are used as a key for the Vigenere Cipher encryption process.

There are a few advantages of the combination of the One Time Pad algorithm with the generate random key and the Vigenere Cipher algorithm with the XOR and XNOR keys:
1. By having different key values in each algorithm, the probability of message interception will decrease
2. The results of encrypting message using Vigenere Cipher algorithm with XOR and XNOR key is dissimilar and distinctive therefore it is safer or harder to breach by cryptanalyst.
Whilst the shortcomings of the One Time Pad algorithm with the generate random key and the Vigenere Cipher algorithm with the XOR and XNOR keys:

1. When plaintext input in the application program, the program is incapable to use spaces and lowercase letters because in the One Time Pad character only 26 characters namely A-Z.
2. In the encryption process the value of the XOR key is very unique and often appears empty or only space.

The encryption process that have been made in the applications can only be run if the XOR Key in the encryption process can be seen or the key is not empty.

6. Conclusions and Suggestion

Based on this research, it can be concluded that The result of manual encryption of the combination of the One Time Pad algorithm with the Vigenere Cipher algorithm is similar and in accordance with applications that have been designed using the Visual Basic program. The results of encrypting messages using the Vigenere Cipher algorithm with the XOR and XNOR keys are not the same because the keys used during the Vigenere Cipher process are different from the XOR key.

The author’s advice that can be given for this research to improve and to develop is by adding the One Time Pad key randomization method using a matrix system.

References

[1] A H M Pardede, Lorena Perbina, Muhammad Zarlis. 2019. Application of Message Security.
[2] Application Using Vigenere Cipher Algorithm Utilizing One Time Pad (OTP) Algorithm as a Key Generator, Journal of Physics : Conference Series1363(2019)012080.
[3] Arif Budiman, Paradise. 2019. Modification of Vigenere Algorithm and One Time Pad Using Rivest Code 6 (RC6) Key Expansion, E Journal Compiler ISSN:225-3839.
[4] Monalisa F S, Garuda Ginting. 2019. Kombinasi Algoritma Exact Matching dan Operasi XOR pada Teks, Jurnal Pelita Informatika Volume 18 Nomor 4 ISSN:2301-9425.
[5] H Mawengkang, I L Sitepu, S Efendi. 2018. Security Analysis in File with Combinations One Time Pad and Vigenere Algorithm, 2nd Nommensen International Conference On Technology and Engineering 420(2018) 012129.
[6] Triandi B, Ekadiansyah, E., Puspasari, R., Iwan, L. T., & Rahmad, F. (2018). Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions, In 2018.
[7] Hutagalung, Wandy Hotmida. 2017. Implementasi Vigenere Cipher Dengan Random Key Method Linear Feedback Shift Register (LFSR) pada Teks, Majalah Ilmiah INTIVolume 12, Nomor 12 ISSN: 2339-210X.
[8] Priyam, Anuja. 2015. Extended Vigenere Using Double Transposition Cipher With One Time Pad Cipher, Intl J Engg Sci Adv Research 2015 June: 1(2):62-65.
[9] Bhardwaj, C., 2012. Modification of Vigenere Cipher by Random Numbers, Punctuation & Mathematical Symbols, Journal of Computer Engineering (IOSRJCE) ISSNNo: 2278-0661.
[10] Anupriya, E. 2011. Encryption Using XOR Based Extended Key For Information Security - A Novel Approach, International Journal on Computer Science And Engineering (IJCSE) ISSN: 0975-3397.
[11] Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi Penerbit Andi: Yogyakarta.
[12] Ariyus, Dony. 2006. Kriptografi Keamanan Data dan Komunikasi Penerbit Graha Ilmu: Yogyakarta.
[13] Munir, Rinaldi. 2006. Pengantar Kriptografi. Bandung