Enhancement of OTP stream cipher algorithm based on bit separation

Arisman*, Mahyuddin K M Nasution, and Syahril Efendi

Faculty of Computer Science and Information Technology, Universitas Sumatera Utara Medan, Sumatera Utara, Indonesia

*arisman.pili@gmail.com

Abstract. Along with the increasing development of cryptography and computer science, it is appropriate that we try to prepare and improve the ability of cryptographic algorithms to counteract and prevent threats. Generally, this algorithm encrypts the text with combined using key. The original message must be the same length of the key used. Actually in this study, a new method for improve OTP was successfully carried out. First, key will be generated using PRNG algorithm then bits of Plaintext will be separate each into 2 bits then rotating it key using matrix table, further key will be inserted into separated Plaintext and re-separate each it into 1 byte, hereinafter the new Plaintext will be XORed with a rotated key. To produce more advanced cipher.

1. Introduction

We have known that most of studies was discussed about an enhancement this algorithm. At OTP Encryption Enhancement Based on Logical Operations, where plain text and keys was combined using AND operator further the text who has been produced from this calculate will be XORed again with key[1]. In this study the method has been successfully applied to produce stronger ciphers. At Another research, Shannon was implemented successfully autonomous key characters to establish the cipher. At this technique, the Original Text are XORed with autonomous key[2].

There is also a study recommending a hybrid approach to processing OTP using quantum superposition states and the results are supported by a usefullness theoretical, OTP is produced from the best approach in the classical system and has passed statistical test.[3]. An OTP encryption algorithm based on one way hash and conventional block cipher This algorithm patches the shortcomings of conventional block ciphers when implementing a hash algorithm, it is easy to implement and improve on conventional block ciphers[4].

More research about encrypting an image based on OTP with the Chaotic approach, was implemented by Jeyamala and friends. This publication describes an invention algorithm that has the ability to maintain the confidentiality of images based on chaos theory. The test results from this study have been successfully analyzed using appropriate tools and have been compared with other similar algorithms[5]. In this paper, a new method to enhancement OTP using separation of bit has been presented, bits of plaintext will be separate each into 2 bits then rotating it key using 4x2 matrix table, further key will be inserted into separated plain and re-separate each into 1 byte hereinafter the new plaintext will be XORed with a rotated key. The cipher has been expanded from basic algorithm with the result that aggregate of default plaintext is not similar with cipher and more complicated.
2. Material And Method

A. OTP
Modern OTP Stream Cipher is a binary number based algorithm, to produce ciphers XOR process will performance between plain bits of text with a key, further to get the plain text back, the XOR process is carried out between the text cipher and the key so that plain text is retrieved. The OTP algorithm is difficult to solve, especially if the provisions are implemented properly. Starting from using random keys with only one use.

![Fig 1. One Time Pad Scheme](image)

After the Cipher text is sent to the recipient, the last recipient of the encrypted message will be XORed with the duplicated and plaintext key received. Key senders and recipients will automatically be destroyed after use, so that the old key is not reused. With a definition of One Time Pad construction above, we can give the example for encryption and decryption where Plaintext= A and Key= P, ci = pi XOR ki and pi = ci XOR ki.

First, we will Conversion Plaintext and Key to binary as follows:

| Plaintext | Dec | Bin   |
|-----------|-----|-------|
| A         | 065 | 01000001 |

| Key | Dec | Bin   |
|-----|-----|-------|
| P   | 080 | 01010000 |

At Table 3. encryption process each one (plaintext and key) will be XORed to generate a cipher then at Table 4 at decryption process furthermore each one (Cipher and Key) will be XORed to generate a plaintext.

| Plaintext | Dec | Bin   |
|-----------|-----|-------|
| A         | 065 | 01000001 |
| P         | 080 | 01010000 |
| Cipher Binary | 31 | 00010000 |
| Cipher Character | 1 | |

| Plaintext | Dec | Bin   |
|-----------|-----|-------|
| Cipher   | 017 | 00010001 |
| P        | 080 | 01010000 |
| Plain Binary | 065 | 01000001 |
| Plaintext | A   | |

B. Designed OTP Enhancement (Proposed OTP Enhancement)
In this session, enhancement of OTP based on bit separation will be shown. If these bases are applied properly cipher character increase four times than original, surely the length will increase as well however that more complicated and the big deal at the future to overcome vulnerability.

![Fig 2. OTP Enhancement Design (encryption)](image)
We can define a equation from Fig. 2 above as follows:

\[ \epsilon = \{0,1\}^l \]  
\[ Mb = Ps \subseteq Kr = \{ x \mid x \in Ps \text{ or } X \in Kr \} \]  
\[ C = Mb \oplus Kr \]  

Accordingly Figure 2. We can see the scheme explanation of proposed OTP Enhancement at encryption section flow, first key will be generated by the Lfsr algorithm using possible feedback polynomial further we will mix separated plain with rotated matrix key has produced sets of binary numbers=Mb where \( \epsilon = \{0,1\}^l \). Hereafter the encryption process by performing XOR between Mb and Kr, where equation for Mb=Ps \( \subseteq \) Kr = \{ x \mid x \in Ps \text{ or } X \in Kr \}), we have seen that Ps and Kr is substantion from Mb.

Further we can define equation from Fig. 3 above as follows:

\[ \epsilon = \{0,1\}^l \]  
\[ C \oplus Kr = Mb \]  
\[ Mb = (Ps \subseteq Kr = \{ x \mid x \in Ps \text{ or } X \in Kr \}) \]  
\[ P = Tb \]  
\[ Tb = \{Ps \notin Kr\} = \{ x \mid x \notin Ps \text{ or } X \notin Kr \} \]

Accordingly Figure 3. Sets of binary \( \epsilon = \{0,1\}^l \) to obtaining the plain text firstly we should performance XOR between Cipher (C) and rotated matrix key (Kr) to call in Mixed Bits (Mb) where Mb=(Ps \( \subseteq \) Kr = \{ x \mid x \in Ps \text{ or } X \in Kr \}) further we will enable the trim process for Mixed Bits (Mb) by drop out the set of keys with Tb=\{Ps \notin Kr\}={ x \mid x \notin Ps \text{ or } X \notin Kr \}).

C. Enhancement in Practice

a) The encryption flowchart at proposed Enhancement OTP Algorithm as follows:

![Fig 4. OTP Enhancement Flowchart (encryption)](image-url)
This will be applied using the PHP programming language. First, Algorithm will receive plaintext and key input where Plaintext A = 01000001 and Key P = 01010000. Key=P = 01010000 = 8 Bits. Then LFSR will generate with $2^n-1=2^8-1=255$ random key periods, with maximum feedback polynomial $g(x)=x^4+x^3+x^2+x^8$.

![LFSR Key Generated](image)

**Fig 5.** LFSR Key Generated

Further obtain first period from LFSR key generated is 00101000, using it as key and rotate using matrix table as follow:

| LFSR Generate Key | Table 5. Rotating key process | Rotated Key |
|-------------------|--------------------------------|-------------|
| 0(1) 0(2)         | 1(8) 0(1)                     | 1 0 1 0 0 0 0 |
| 1(3) 0(4)         | 1(7) 0(2)                     |
| 1(5) 0(6)         | 0(6) 0(3)                     |
| 0(7) 0(8)         | 0(5) 0(4)                     |

Then was obtained a rotated Key “P” : 1 0 1 0 0 0 0, hereinafter plaintext will be separated into 2 Bits 01 00 00 01

Mix bits into 32 Bits as follow:

0110100000 0010100000 0010100000 + 01

and separate into 4 bytes

01101000 00001010 00000010 10000001

Then, perform XOR process with rotated key as follow:

| 01101000 00001010 00000010 10000001 | 10000001 (Mixed Plaintext and Key) |
|-------------------------------------|-----------------------------------|
| 10100000 10100000 10100000 10100000 | 10100000 (Rotated Key)            |
| 11001000 10101010 10100100 00100001 | XOR                               |
| 200 170 162 033 (Decimal)  | € ! (Cipher)                      |

b) The Decryption flowchart at proposed Enhancement OTP Algorithm as follows:

First, algorithm will requesting the key. If value is True then plaintext will be displayed. Else incorrect plaintext will occur.
Hereinafter explanation Fig. 6 flowchart as follows:

Input key has been generated = 00101000 as shown at Fig 5. If key true algorithm will conversion cipher to binary where cipher = È”e! = 11001000 10101010 10100010 00100001 further key will be rotated again using matrix as shown at Table V. Key rotation results = 10100000 then XORed cipher and rotated key which produces 32 binary bits.

| Cipher   | Rotated Key |
|----------|-------------|
| 11001000 | 10101010    |
| 10100000 | 10100010    |
| 00100001 |             |

XOR

Further performed the key separation/cut out process from the 32 Bits of binary as follow:

01101000 00001010 00000010 10000001 (XORed Result)
01101000000101000000101000001 (32 bits of binary)

Fig 7. Cut Out Useless Keys Process
Cut out useless keys, this will produce 8 bits of Binary, Cut out Result: \textit{01000001} with decimal number 065 with A as plaintext.

3. Result and Discussion
The new cipher has difficult analysis for unauthorized readers as a security application. A new cipher text is highly secret. The adopted message example has been presented which has text length of four times from original characters. So, there is a difficulty to analyze it by the cryptanalyst which requires a long time of processing. further, we can see as follows:

**Table 6. Comparation of original vs enhancement otp**

| Original OTP | Enhancement OTP |
|--------------|-----------------|
| Plaintext    | Key            | Cipher |
| A            | P              | ◄      |
| A            | P              | ◄      |

In Original OTP with Plaintext=A and Key=P it had been produced Cipher=◄, actually it’s not similar with OTP based Bits Separation that Cipher has been generated = ◄! surely the length will increase as well however that more complicated and the big deal at the future to overcome vulnerability. On the Original OTP it will show the length of original characters and cipher was similar as follows:

Plaintext= A = \textit{00100001} 8 Bits
Ciphertext = ◄ = \textit{00011111} 8 Bits

The length of bit was similar

However it’s different when algorithm implemented using OTP base bits separation, length of cipher character is not similar with plaintext character, we can see as follows:

Plaintext = A = \textit{01000001} 8 Bits
Ciphertext = ◄! = \textit{11001000} \textit{10101010} \textit{10100010} \textit{00100001} 8 Bits

Of course it will be hard to guess the plaintext character from the cipher had been produced and give complexity to cryptanalysis to analyze the cipher and get the original message, because we have know that an original OTP have very strong, moreover enhancement OTP based Bit separation surely can give a new strength against the existing algorithm.

4. Conclusion
With the security concerns we have proposed a enhancement scheme similar OTP that is based separation bits. In the proposed Algorithm few additional improvement part as follows, first key will be generated using PRNG algorithm and separate plain, then rotated key, further: insertion key to separated plain. By taking these three issues, we try in this study to achieve a more secure OTP scheme. Actually in this paper, a new method to enhancement OTP stream cipher using separation of bit was cleared to produce more complicated cipher. at future research possible to use a new technique such using another random generator algorithm and logic gate to get more varied ciphers.

REFERENCES
[1] Yaqeen S Mezaal, Dalal A Hammood and Mohammed H Ali 2016 \textit{OTP. Encrp. Enhc. Bases on Logc. Opr}. 109-112.
[2] G Goos, J Hartmanis and J van Leeuwen, 2017 \textit{lecture on data security, Modern Cryptology, in Theory and Practice} vol 3 (Springer).
[3] Gaurav Upadhyay and Manisha J Nene 2016 \textit{Otp. Gen. Using Qntm Superpos. Stat} 16 1886.
[4] Songsheng Tang and Fuqiang Liu 2012 A Otp. Encrp. Algo. Based. On Owh. And Convent. Block. Cipher 12 74.

[5] Jeyamala C, Gopi Ganesh S and Raman G.S 2010 Conf. An Image Encryption Scheme Based on One Time Pads – A Chaotic Approach vol 2 (India:icoc).

[6] Siddesh Gaonkar, 2015 Dsgn of 8 bit, 16 bit and 32 bit LFSR For PN Seq Gnrt using Vhdl 306.